ОТЧЕТ ФАТФ

Противодействие использованию программ-вымогателей

Март 2023

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является независимой межправительственной организацией, разрабатывающей и популяризирующей свои принципы для защиты всемирной финансовой системы от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ являются общепризнанными международными стандартами по противодействию отмыванию денег и финансированию терроризма (ПОД/ФТ).

Дополнительную информацию о ФАТФ можно найти на **www.fatf-gafi.org**

Данный документ и/или любая включённая в него карта подготовлены без предубеждения и ущемления статуса никакой территории или ее суверенитета, международных границ и разграничительных линий, а также названий территорий, городов или областей.

Неофициальный перевод выполнен МУМЦФМ

Ссылка для цитирования:

FATF (2023), *Countering Ransomware Financing,* FATF, Paris,
http://www.fatf-gafi.org/publications/Methodsandtrends/countering-ransomware-financing.html

Содержание

Список сокращений **2**

Краткий обзор **3**

Введение **7**

Основная тема и предмет исследования 7
Цели и структура 9
Методология 9

ЧАСТЬ I: ФИНАНСОВЫЕ ПОТОКИ, СВЯЗАННЫЕ С АТАКАМИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ 11

Объём финансовых потоков **11**

Характеристики и географические тенденции **14**

Распространённые методы и тенденции **17**

ЧАСТЬ II: СЛОЖНОСТИ И ПЕРЕДОВАЯ ПРАКТИКА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЮ ДОХОДОВ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ 24

Нормативно-правовая база **24**

Атаки с использованием программ-вымогателей как предикатное преступление для ОД 24
Применение превентивных мер в соответствующих секторах 25

Выявление и информирование **26**

Охват обязательствами, касающимися направления СПО 26
Меры по повышению эффективности выявления подозрительных операций 29
Сообщения от потерпевших 32
Другие источники информации для выявления атак с использованием программ-вымогателей 34

Стратегии проведения финансовых расследований **37**

Оперативное реагирование и работа с потерпевшими для получения информации 38
Механизмы и методы расследований 39
Возврат активов 44

Знания и навыки **45**

Политика и взаимодействие на национальном уровне **47**

Национальная оценка и стратегия 47
Сотрудничество и взаимодействие на национальном уровне 49
Сотрудничество и руководства для частного сектора 51

Международное сотрудничество **54**

Затруднения, обусловленные использованием виртуальных активов 56
Необходимость быстрого и оперативного сотрудничества 57
Важность многостороннего взаимодействия 59

Заключение **61**

См. также:

Противодействие финансированию программ-вымогателей: потенциальные индикаторы риска

Этот перечень возможных индикаторов риска дополняет отчёт ФАТФ *«Противодействие финансированию программ-вымогателей»* и может помочь субъектам государственного и частного сектора в выявлении подозрительных операций, связанных с атаками с использованием программ-вымогателей.

https://www.fatf-gafi.org/content/fatfgafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

Список сокращений

КПА	Криптовалюты, обеспечивающие повышенную степень анонимности
ПОД/ФТ	Противодействие отмыванию денег и финансированию терроризма
ГРКИ	Группы реагирования на компьютерные инциденты
ДФ	Децентрализованные финансы
УНФПП	Установленные нефинансовые предприятия и профессии
ПФР	Подразделение финансовой разведки
IP	Протокол межсетевого взаимодействия
ПО	Правоохранительные органы
ОД	Отмывание денег
ВБС	Внебиржевая сделка
ГЧП	Государственно-частное партнёрство
RaaS	Программа-вымогатель как услуга
СПО	Сообщения о подозрительных операциях
КГВА	Контактная группа по виртуальным активам
ПУВА	Провайдер услуг в сфере виртуальных активов
VPN	Виртуальная частная сеть

Краткий обзор

Мировой объём финансовых потоков, связанных с атаками с использованием программ-вымогателей, значительно вырос в последние годы. По оценкам представителей отрасли, объём финансирования таких атак увеличился в четыре раза в 2020 и 2021 годах по сравнению с 2019 годом. Новые технологии повысили прибыльность таких атак и вероятность их успешного осуществления. К ним относится нацеливание атак на крупные и дорогостоящие компании, а также предложение программ-вымогателей как услуги (ransomware as service), когда преступники, занимающиеся разработкой программ-вымогателей, продают удобные для использования пакеты программного обеспечения своим «партнерам» по криминальному бизнесу. Последствия атак с использованием программ-вымогателей могут быть катастрофическими и представлять угрозу для национальной безопасности, включая повреждение и выведение из строя объектов критической инфраструктуры и сервисов.

Целью данного исследования ФАТФ является повышение уровня понимания во всём мире финансовых потоков, связанных с использованием программ-вымогателей, и определение передовой практики для борьбы с этой угрозой. В отчёте также приведён перечень потенциальных индикаторов риска, который поможет государственным органам и субъектам частного сектора выявлять такие финансовые потоки. Выводы данного отчёта основываются на опыте и экспертных знаниях представителей государственного и частного сектора, в том числе на информации и примерах, предоставленных более чем 40 делегациями, входящими в глобальную сеть ФАТФ.

Атаки с использованием программ-вымогателей являются одной из форм вымогательства и, согласно требованиям Стандартов ФАТФ, за такие деяния должна быть установлена уголовная ответственность, и они должны быть квалифицированы как предикатные преступления для отмывания денег. В отчёте отмечается, что выплата выкупа и последующее отмывание доходов от атак с использованием программ-вымогателей, практически всегда осуществляется в виртуальных активах. Преступники, совершающие атаки с использованием программ-вымогателей пользуются международным характером виртуальных активов, что помогает им осуществлять почти мгновенные крупные трансграничные операции часто без участия традиционных финансовых учреждений, в которых реализуются меры и программы по противодействию отмыванию денег и финансированию терроризма (ПОД/ФТ). Кроме того, преступники запутывают следы своих операций, используя в процессе отмывания доходов технологии, методы и токены, повышающие уровень анонимности, такие как повышающие степень анонимности криптовалюты и «смесители» (миксеры).

Практически исключительное использование виртуальных активов в процессе отмывания доходов от атак с применением программ-вымогателей ещё раз подчёркивает важность ускоренной реализации требований Рекомендации 15 ФАТФ, согласно которой юрисдикции должны установить меры для снижения рисков, связанных с виртуальными активами, а также осуществлять регулирование сектора ПУВА. Эти действия являются чрезвычайно важными для недопущения того, чтобы преступники для легализации доходов от своей преступной деятельности получали легкий и простой доступ к ПУВА, находящимся в юрисдикциях, в которых имеются слабые или совсем не имеется никаких мер контроля в сфере ПОД/ФТ.

В отчёте также отмечается, что сведения о совершаемых атаках с использованием программ-вымогателей не предоставляются в должной мере. Это может быть обусловлено трудностями в выявлении таких случаев представителями частного сектора, негативным влиянием на деловую активность потерпевших или страхом мести со

стороны преступников в случае если потерпевший сообщит о совершённой атаке. Это частично объясняет недостаточный опыт расследования случаев отмывания доходов, полученных в результате атак, осуществляемых с использованием программ-вымогателей. В этой связи юрисдикциям необходимо провести дополнительную работу по увеличению и повышению качества источников для выявления и информирования о таких атаках. Представителям государственных органов также следует осуществлять оперативный сбор ключевой информации и обладать необходимыми инструментами и навыками для эффективного отслеживания и возврата виртуальных активов.

Атаки с использованием программ-вымогателей затрагивают широкий спектр областей, и поэтому в расследованиях могут принимать участие другие субъекты, не входящие в традиционную систему ПОД/ФТ, такие как ведомства, отвечающие за кибербезопасность и защиту данных. Поэтому для эффективного пресечения атак с использованием программ-вымогателей и последующего отмывания доходов требуется применение междисциплинарного подхода. По причине присущего децентрализованного и транснационального характера виртуальных активов создание новых и использование существующих механизмов международного сотрудничества является первоочередным условием для успешного противодействия легализации доходов от атак с использованием программ-вымогателей.

Для усиления мер глобального реагирования на атаки с применением программ-вымогателей и связанного с этим отмывания денег, ФАТФ предлагает юрисдикциям реализовать следующие меры.

Предлагаемые меры

Информация, собранная в рамках проведения данного исследования, включала некоторые практические примеры мер, которые страны могут предпринять для наращивания своих возможностей по борьбе с незаконными финансовыми потоками, связанными с использованием программ-вымогателей. В данном разделе обобщена такая передовая практика, а также содержатся предложения о том, как юрисдикции могли бы более эффективно пресекать случаи отмывания доходов, полученных в результате атак с использованием программ-вымогателей.

Реализация соответствующих Стандартов ФАТФ, в том числе касающихся ПУВА, и повышение эффективности выявления атак с использованием программ-вымогателей

- Юрисдикциям следует в ускоренном порядке обеспечить соблюдение требований соответствующих Стандартов ФАТФ, касающихся сектора ПУВА, путём реализации положений Рекомендации 15 (включая так называемое «дорожное правило»[1]) в максимально сжатые сроки. Это обеспечит выполнение провайдерами услуг виртуальных активов необходимых обязательств в сфере ПОД/ФТ, касающихся сбора критически важной финансовой информации и направления сообщений о подозрительных операциях.
- Юрисдикциям следует обеспечить, чтобы за атаки с использованием программ-вымогателей была установлена уголовная ответственность и чтобы такие дея-

[1] «Дорожное правило» является ключевой мерой ПОД/ФТ, согласно которой ПУВА обязаны получать, хранить и обмениваться информацией об отправителях и получателях переводов виртуальных активов. Это позволяет финансовым учреждениям и ПУВА осуществлять проверку на предмет нахождения участников операций в санкционных списках и выявлять подозрительные операции.

ния квалифицировались как предикатные преступления для отмывания денег (например, как один из видов вымогательства) в соответствии с Рекомендацией 3 ФАТФ.

- Юрисдикциям следует повысить эффективность выявления случаев атак с использованием программ-вымогателей путём:
  - Оказания содействия регулируемым субъектам в выявлении случаев осуществления атак с использованием программ-вымогателей и связанного с этим отмывания денег, а также в направлении сообщений о подозрительных операциях. Для этого следует, в том числе, информировать соответствующих подотчётных субъектов о тенденциях, настораживающих признаках (аналогичных тем, которые приведены в документе *«Противодействие использованию программ-вымогателей: потенциальные признаки риска»*[2]) и предоставлять руководства по выявлению таких случаев.
  - Стимулирования и поощрения потерпевших добровольно сообщать о случаях атак, например, путём повышения информированности о доступной поддержке и ресурсах или путём создания защищённых и безопасных каналов связи для сообщения о таких случаях.
- Юрисдикциям также следует рассмотреть возможность установления каналов связи с нетрадиционными субъектами, на которых могут не распространяться требования ПОД/ФТ (такими как компании по кибербезопасности и компании по реагированию на инциденты) с целью расширения спектра источников информации для выявления случаев атак с использованием программ-вымогателей.

Содействие проведению финансовых расследований и реализации мер по возврату активов

- Компетентным органам следует использовать и адаптировать, при необходимости, традиционные правоохранительные методы, а также конкретные методы применительно к виртуальным активам для проведения расследований случаев отмывания доходов от атак с использованием программ-вымогателей. Сотрудникам компетентных органов необходимо обладать специализированными навыками и знаниями, требуемыми для проведения успешных финансовых расследований по делам, связанным с атаками с использованием программ-вымогателей. Это включает разработку, предоставление доступа и обучение использованию инструментов мониторинга и анализа блокчейна.
- Юрисдикциям следует обеспечить, чтобы сотрудники правоохранительных органов постоянно обладали необходимыми возможностями и полномочиями для оперативного и эффективного наложения ареста и конфискации активов, особенно виртуальных активов. Юрисдикциям также следует обеспечить наличие специальных механизмов для надлежащего управления арестованными виртуальными активами.

[2] Документ доступен по адресу: https://www.fatf-gafi.org/content/fatfgafi/en/publications/Methodsandtrends/countering-ransomware-financing.html

Применение междисциплинарного подхода для борьбы с атаками с использованием программ-вымогателей

- В рамках проведения своих национальных оценок рисков юрисдикциям следует обеспечить выявление и оценку рисков ОД, представляемых атаками с использованием программ-вымогателей. Принимая во внимание децентрализованный характер виртуальных активов и наличие преступных группировок, специализирующихся на использовании программ-вымогателей, это также касается юрисдикций, в которых имеются секторы виртуальных активов, но атаки с использованием программ-вымогателей в настоящее не представляют внутреннюю угрозу. Такое выявление и анализ рисков может оказаться полезным в разработке национальных стратегий кибербезопасности, поскольку это позволит получить комплексную национальную картину рисков, исходящих от использования программ-вымогателей.
- Юрисдикциям следует разработать механизмы взаимодействия между соответствующими компетентными органами, начиная от правоохранительных органов, органов, отвечающих за ПОД/ФТ, и органов, занимающихся борьбой с киберпреступностью, и заканчивая нетрадиционными партнёрами, такими как ведомства, занимающиеся вопросами кибербезопасности и защиты данных. Эта способствует обмену информацией и оперативными данными, а также обеспечивает механизм для взаимного обмена различными техническими знаниями и опытом.

Поддержка партнёрских отношений с частным сектором

- Юрисдикциям следует определить и создать механизмы для поддержки сотрудничества между государственным и частным сектором. Юрисдикциям следует рассмотреть возможность включения ПУВА и других нетрадиционных партнёров в такие механизмы сотрудничества. Это позволит создать полезные площадки для повышения информированности и обмена опытом и идеями, а также будет способствовать достижению целей правоохранительных органов.

Развитие и совершенствование международного сотрудничества

- Юрисдикциям следует создать и активно участвовать в двусторонних, региональных и многосторонних механизмах сотрудничества, например, используя сотрудников отделения связи и устанавливая контактных лиц, доступных в круглосуточном режиме, для содействия оперативному международному сотрудничеству и обмену информацией. Это будет способствовать эффективному и быстрому отслеживанию трансграничного перемещения денежных средств и эффективному возврату активов, а также поможет государственным органам успешно ликвидировать транснациональные сети, занимающиеся проведением атак с использованием программ-вымогателей и отмыванием доходов от этой преступной деятельности.

Введение

Основная тема и предмет исследования

1. Программа-вымогатель - это один из видов вредоносного программного обеспечения, разрабатываемого и/или используемого преступниками для блокирования доступа к данным, системам или сетям, с требованием оплаты за восстановление доступа. Распространённые методы атак с использованием программ-вымогателей включают в себя шифрование данных, эксфильтрацию данных (т.е. несанкционированное копирование, передача или получение данных) и прерывание операций жертв атаки. При осуществлении таких атак часто используется сразу несколько методов, в том числе возможные угрозы опубликовать данные жертвы[3].

2. Количество и масштаб атак с использованием программ-вымогателей значительно возросли в последние годы[4]. Атаки с использованием программ-вымогателей осуществляются, главным образом, для получения незаконной прибыли. Увеличение числа таких атак привело к росту преступных доходов от их осуществления, а также к увеличению объёмов связанного с этим отмывания денег. По оценкам представителей отрасли, объём финансирования таких атак увеличился в четыре раза в 2020 и 2021 годах по сравнению с 2019 годом[5]. Хотя согласно последним отраслевым данным, в 2022 году наблюдалась тенденция к снижению количества оплат за восстановление доступа (возможно, по причине отказа жертв атак выплачивать деньги), стоимость виртуальных активов, полученных в качестве выкупа преступниками, совершающими атаки с использованием программ-вымогателей, остаётся значительно более высокой, нежели в период до 2019 года[6]. При этом реальное количество совершаемых атак с использованием программ-вымогателей и понесённых в связи с этим убытков, вероятно, является значительно более высоким, поскольку потерпевшие не всегда сообщают о таких атаках.

3. Атаки с использованием программ-вымогателей наносят существенный ущерб и приводят к нарушению деятельности правительств, государственных учреждений, коммерческих предприятий и граждан. В некоторых случаях такие атаки серьёзно влияют на сферу здравоохранения и представляют угрозу для национальной безопасности, вынуждая, в том числе, прерывать и останавливать работу объектов критической инфраструктуры и сервисов. Такие атаки также приводят к нарушению конфиденциальности и сохранности чувствительных данных[7]. Преступники, совершающие атаки с использованием программ-вымогателей, разработали способы и методы для увеличения прибыльности своих атак и повышения вероятности их успешного проведения. В результате этого, угроза, исходящая от незаконных финансовых потоков, связанных с применением программ-вымогателей, вероятно, будет продолжать возрастать.

---

[3] ФБР, “Scams and Safety: Ransomware” («Мошенничество и безопасность: программы-вымогатели») (дата обращения: сентябрь 2022 года), документ доступен по адресу: www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; Австралийский центр кибербезопасности, “Ransomware” («Программы-вымогатели») (дата обращения: сентябрь 2022 года), документ доступен по адресу: www.cyber.gov.au/ransomware.

[4] Европейское агентство по сетевой и информационной безопасности (ENISA), «Threat Landscape 2022» («Обзор киберугроз в мире в 2022 году») (октябрь 2022 года), документ доступен по адресу: www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[5] Компания «Chainalysis», “Chainalysis Crypto Crime Report 2022” (Доклад компании «Chainalysis» о криптопреступности от 2022 года), (февраль 2022 года), документ доступен по адресу: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

[6] Компания «Chainalysis», “Ransomware Revenue Down As More Victims Refuse to Pay” («Доходы от атак с использованием программ-вымогателей снижаются, поскольку всё большее количество жертв отказывается платить»), (январь 2023 года), документ доступен по адресу: https://blog.chainalysis.com/reports/crypto-ransomware-revenue-downas-victims-refuse-to-pay/

[7] Например, атаки на больницы ставят под угрозу лечение пациентов, а атаки на отделы и управления полиции негативно влияют на обеспечение безопасности.

4. При совершении атак с использованием программ-вымогателей преступники практически всегда требуют оплату за восстановление доступа в виртуальных активах. Потерпевшие или третьи лица, действующие от имени потерпевших, часто используют ПУВА[8] для совершения оплаты. Преступники, совершающие атаки с использованием программ-вымогателей, также используют ПУВА для отмывания незаконно полученных средств и для обмена своих преступных доходов на фиатную валюту, которую можно легко обменять на товары и услуги и является более стабильным средством накопления.

5. В 2018 году ФАТФ внесла изменения в свои Рекомендации для охвата требованиями сектор виртуальных активов и ПУВА. После этого ФАТФ выпустила различные руководства для оказания содействия юрисдикциям и субъектам частного сектора в осуществлении мониторинга и снижении рисков в этом секторе, включая настораживающие признаки ОД и ФТ[9]. Хотя в указанных руководствах иногда затрагивалась тематика применения программ-вымогателей, настоящий отчёт является первым документом ФАТФ, конкретно посвящённым рассмотрению тенденций и методов отмывания денег, связанных с осуществлением атак с использованием программ-вымогателей.

6. В период президентства Сингапура ФАТФ использует накопленный опыт в проведении финансовых расследований в отношении виртуальных активов для выявления трудностей и обмена передовой практикой в целях противодействия использованию программ-вымогателей и связанному с этим отмыванию денег. В данном отчёте акцент сделан на рассмотрении того, как выявлять платежи за восстановление доступа в результате совершения атак с использованием программ-вымогателей и сообщать о таких случаях; как пресекать, выявлять и расследовать финансовые потоки, связанные с использованием программ-вымогателей; и как осуществляется отмывание таких незаконных доходов. При этом в настоящем отчёте не рассматривается проблематика использования программ-вымогателей в целях финансирования терроризма, поскольку в сведениях и примерах, предоставленных для подготовки отчёта, отсутствовала информация о существенном или заметном применении программ-вымогателей в этих целях.

7. Поскольку атаки с использованием программ-вымогателей являются одной из форм вымогательства, в Рекомендациях ФАТФ содержатся требования, согласно которым все юрисдикции должны ввести уголовную ответственность за отмывание доходов от совершения атак с применением программ-вымогателей (Рекомендация 3). Согласно требованиям ФАТФ, юрисдикции также должны выявлять и оценивать существующие в их странах риски ОД и принимать меры для снижения этих рисков (Рекомендации 1 – 2); обеспечить, чтобы субъекты частного сектора, включая ПУВА, применяли надлежащие превентивные меры, такие как направление сообщений о подозрительных операциях (Рекомендации 9 – 23); обеспечить, чтобы правоохранительные органы проводили расследо-

[8] Провайдер услуг в сфере виртуальных активов означает любое физическое или юридическое лицо, которое не охвачено Рекомендациями ФАТФ, и осуществляет в качестве предпринимательской деятельности один или несколько из следующих видов деятельности или операций для или от имени другого физического или юридического лица: обмен между виртуальными активами и фиатными валютами; обмен между одной или более формами виртуальных активов; перевод виртуальных активов; хранение и/или администрирование виртуальных активов или инструментов, позволяющих осуществлять контроль над виртуальными активами; участие в и предоставление финансовых услуг, связанных с предложением выпускающего лица и/или с продажей виртуальных активов.

[9] См.: ФАТФ (июнь 2022 г.), *Обновлённый целевой обзор выполнения Рекомендаций ФАТФ, касающихся виртуальных активов и провайдеров услуг в сфере виртуальных активов;* (сентябрь 2020 г.), *Настораживающие признаки, касающиеся виртуальных активов;* и (август 2019 г.) *Конфиденциальное руководство ФАТФ по финансовым расследованиям в отношении виртуальных активов.*

вания, отслеживали и осуществляли конфискацию преступных доходов (Рекомендации 4, 29 – 31); и осуществлять международное сотрудничество для расследования и судебного преследования за ОД и предикатные преступления, а также в целях конфискации и возврата связанных с этим преступных доходов (Рекомендации 36 – 40).

8. Хотя использование программ-вымогателей является одним из видов киберпреступлений, информация, содержащаяся в данном отчёте, затрагивает, главным образом, применение программ-вымогателей и может или не может касаться других видов киберпреступлений, таких как использование вредоносного программного обеспечения, осуществление фишинговых атак по электронной почте или получение несанкционированного доступа к финансовой информации и ее продажа.

Цели и структура

9. В Части I отчета рассматривается то, как преступники, совершающие атаки с использованием программ-вымогателей, получают, отмывают и обналичивают свои незаконные доходы. Целью данного документа является повышение уровня осведомлённости и понимания масштабов глобальной угрозы, связанной с применением программ-вымогателей, способов осуществления платежей за восстановление доступа или связанных с этим платежей, а также методов того, как доходы, связанные с атаками с использованием программ-вымогателей, оказываются в руках киберпреступников.

10. В Части II отчёта рассматриваются трудности, а также передовая практика, касающаяся выявления, расследования и пресечения финансовых потоков, связанных с атаками с использованием программ-вымогателей.

11. Данный отчёт предназначен для оказания содействия **оперативным органам** в получении высококачественных оперативных финансовых данных, проведении финансовых расследований и выявлении, отслеживании и аресте незаконных доходов. **Национальные регулирующие органы** и **органы, отвечающие за выработку политики,** могут использовать информацию, содержащуюся в данном отчёте, для выявления уязвимостей и снижения рисков. Эта информация также поможет **финансовым учреждениям, ПУВА и установленным нефинансовым предприятиям и профессиям (УНФПП)** в разработке и реализации мер контроля в целях выявления, информирования и недопущения незаконного перемещения доходов от атак с использованием программ-вымогателей.

Методология

12. Соруководителями данного проекта являлись эксперты из Израиля и Соединённых Штатов Америки. Кроме того, представители следующих юрисдикций и организаций внесли вклад в проведённую работу в составе проектной группы: Австралия, Канада, Европейская комиссия, Франция, Германия, Япония, Люксембург, Мексика, Филиппины, Сингапур, ЮАР, Испания, Швейцария, Турция, Великобритания, Азиатско-Тихоокеанская группа по борьбе с отмыванием денег и Группа «Эгмонт».

13. Информация и выводы, содержащиеся в данном отчёте, основаны на:

- Анализе существующей литературы и материалов из открытых источников, посвящённых этой проблематике.
- Информации о восприятии юрисдикциями рисков, а также на информации о национальных законах, полномочиях, проблемах, передовой практике и примерах дел, касающихся использования программ-вымогателей, которая была запрошена у членов глобальной сети ФАТФ, насчитывающей свыше 200 юрисдикций. В общей сложности проектная группа получила данные от более чем 40 делегаций.
- Обсуждениях, состоявшихся в рамках Контактной группы ФАТФ по виртуальным активам (КГВА)[10].
- Целевом взаимодействии с представителями частного сектора через КГВА.

[10] В июне 2019 года Рабочая группа ФАТФ по разработке политики согласилась создать Контактную группу по виртуальным активам для доведения требований ФАТФ до частного сектора и для обеспечения оперативной разработки представителями отрасли надлежащих технологических решений с целью реализации этих требований.

ЧАСТЬ I: ФИНАНСОВЫЕ ПОТОКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Объём финансовых потоков

14. Во всём мире значительно возросло количество атак с использованием программ-вымогателей и объем связанных с ними финансовых потоков. В последние годы многие юрисдикции отмечают увеличение частоты атак с использованием программ-вымогателей от десяти до нескольких сотен процентов, в зависимости от конкретных юрисдикций. Кроме того, в различных юрисдикциях зафиксировано соответствующее увеличение количества сообщений от потерпевших и рост числа сообщений о подозрительных операциях (СПО), связанных с использованием программ-вымогателей. Так, в рамках одной юрисдикции в СПО, отправленных за первые 6 месяцев 2021 года, фигурировали операции, связанные с использованием программ-вымогателей, на общую сумму эквивалентную 590 миллионам долларов США (552 миллионам евро). Это на 42% больше по сравнению с 2020 годом, когда аналогичная сумма составляла 416 миллионов долларов США (389 миллионов евро)[11]. В последних ежегодных отчётах правоохранительных организаций отмечается существенный рост масштабов деятельности, связанной с использованием программ-вымогателей[12]. Кроме того, по мнению представителей отрасли, наблюдается аналогичный рост числа подобных атак и разновидностей активно применяемых программ-вымогателей. По некоторым оценкам, количество атак, совершённых с использованием программ-вымогателей в 2021 году, составило примерно 623,3 миллиона, что более чем в два раза превосходит 304,6 миллиона атак, совершённых в 2020 году[13]. Аналогичным образом, с 2019 года в два раза увеличилось предполагаемое количество разновидностей активно используемых программ-вымогателей[14].

15. Следует отметить, что некоторые юрисдикции сообщили о небольшом количестве атак с использованием программ-вымогателей, совершаемых на их территории. Однако информация, собранная для подготовки данного отчёта, показывает, что количество сообщений об этих атаках по-прежнему меньше количества самих атак, хотя в некоторых юрисдикциях наблюдается увеличение числа СПО, а также сообщений, поступающих от потерпевших. Поэтому точную оценку количества таких случаев, а также сумм, уплаченных в качестве выкупа, дать затруднительно. Примеры, предоставленные для включения в данный отчёт, показывают, что атаки с использованием программ-вымогателей могут представлять риск как для развитых, так и для развивающихся юрисдикций, независимо от региона.

---

[11] Агентство по борьбе с финансовыми преступлениями США (FINCEN), "Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021" («Тенденции совершения атак с использованием программ-вымогателей по данным, поступившим в соответствии с Законом о банковской тайне в период с января 2021 года по июнь 2021 года» от июня 2021г.), документ доступен по адресу: www.fincen.gov/sites/default/files/2021-10/Financial Trend Analysis Ransomware 508 FINAL.pdf

[12] ФБР, "Internet Crime Report 2021" («Доклад о преступности в Интернете от 2021 года»), (дата обращения: 1 декабря 2022 года), документ доступен по адресу: www.ic3.gov/Home/AnnualReports; ЕВРОПОЛ, "Internet Organised Crime Threat Assessment (IOCTA) 2021" («Оценка угрозы организованной преступности в Интернете от 2021 года»), (дата обращения: 1 декабря 2022 года), документ доступен по адресу: www.europol.europa.eu/publications-events/main-reports/iocta-report

[13] Компания «SonicWall», "2022 SonicWall Cyber Threat Report" (Доклад компании «SonicWall» о киберугрозах от 2022 года), документ доступен по адресу: www.infopointsecurity.de/media/2022-sonicwall-cyber-threat-report.pdf

[14] Компания «Chainalysis», "Chainalysis Crypto Crime Report 2022" (Доклад компании «Chainalysis» о криптопреступности от 2022 года), (февраль 2022 года), документ доступен по адресу: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.

16. Несколько юрисдикций отметили, что увеличение числа атак с использованием программ-вымогателей и объемов соответствующих финансовых потоков может быть связано с разработкой преступниками методов повышения эффективности и прибыльности своих атак, таких как **«охота на крупную дичь», «программа-вымогатель как услуга» и двойное/ тройное/ многократное вымогательство,** (см. Вставку 1).

Вставка 1: Развитие методов совершения атак с использованием программ-вымогателей

Тактика **«охоты на крупную дичь» (big game hunting)** – преступники выбирают в качестве цели крупные организации, компании, имеющие большую стоимость, или известных лиц, которые, по их мнению, с большей вероятностью заплатят выкуп для скорейшего возобновления своей деятельности, а также во избежание привлечения внимания общественности. Кроме того, вымогатели выбирают в качестве своих жертв организации, работающие в сфере логистических цепочек с поставкой «точно в срок» (just-in-time), которые с большей вероятностью сильнее пострадают от простоя. От этих преступников страдают и объекты критической инфраструктуры, и организации, хранящие чувствительную или ценную информацию. Злоумышленники полагают, что такие организации в большей степени склонны заплатить выкуп, чем другие жертвы.

Программа-вымогатель как услуга (RaaS) – незаконная бизнес-модель, в рамках которой преступники за плату и/или процент от выкупа предлагают «партнерам» наборы программ-вымогателей в сети «Dark Web» или берут на себя выполнение некоторых элементов атаки, таких как распространение вредоносных программ, осуществление исходного взлома сети жертвы, кража данных или ведение переговоров о выкупе. Преступники также могут покупать украденные учётные данные для получения доступа к системе жертвы и её эксплуатации, что позволяет распространять программы-вымогатели. Кроме того, преступники могут получать закрытую информацию об отдельных отраслях в конкретных юрисдикциях для выбора целей и обеспечения максимальной эффективности своих атак. Модель RaaS снижает расходы на проведение атак и требования к уровню технических знаний преступников, упрощает выход на этот «рынок» и позволяет менее подкованным в техническом отношении преступникам осуществлять атаки с использованием программ-вымогателей.

Двойное вымогательство (double-extortion) - тактика, в рамках которой вымогатели сначала крадут данные своих жертв и потом зашифровывают их, после чего угрожают опубликовать украденные данные, если их требование о выкупе не будет выполнено. Такая угроза опубликования данных является дополнением к угрозам, касающимся взломанной системы. Эта тактика может оказать дополнительное давление на жертв, вынуждая их согласиться на требование о выплате выкупа, даже если они в состоянии самостоятельно восстановить работу системы.

Тройное вымогательство (triple-extortion) - тактика, в рамках которой вымогатели требуют деньги не только от первой жертвы, но также и от другой жертвы, которая может пострадать в результате раскрытия данных, похищенных у первой жертвы, таких как закрытые данные о состоянии здоровья, персональные данные, учётные данные счетов, и данные, являющиеся интеллектуальной собственностью.

Многократное вымогательство (multiple-extortion) - тактика, в рамках которой используется более двух методов вымогательства. В её основе лежит метод двойного вымогательства, включающий шифрование и кражу данных, а также тактика оказания дополнительного давления, например, посредством организации DDoS-атак (отказ в обслуживании), общения с клиентами жертвы, продажи ценных бумаг жертвы без покрытия, или нарушения функционирования инфраструктурных систем.

17. Согласно открытой информации, более половины всех известных атак с использованием программ-вымогателей были осуществлены в отношении субъектов правительственного/государственного сектора, сектора здравоохранения и сектора производства промышленных товаров и услуг.[15,16] Это частично обусловлено тактикой «охоты на крупную дичь», что объясняет крупные выплаты выкупа, а также общее увеличение платежей, осуществляемых жертвами атак с использованием программ-вымогателей. В последние годы целями преступников, совершающих атаки с применением программ-вымогателей, также стали организации энергетического сектора, финансовые учреждения, предприятия связи и образовательные учреждения. Хотя преступники, использующие тактику «охоты на крупную дичь», могут выбирать в качестве целей своих атак в основном большие компании и корпорации, средние и малые организации и отрасли также часто становятся жертвами таких атак с использованием программ-вымогателей. В действительности, такие атаки, по-прежнему, нацелены на средние и малые предприятия. В случае вымогательства выкупа у таких небольших компаний и предприятий соотношение прибыль-риск может оказаться более стабильным по сравнению с резонансными атаками, осуществляемыми в отношении крупных организаций. Во второй половине 2020 года почти 55% от всех атак были совершены в отношении компаний, в которых работают менее 100 человек, а примерно 75% атак были осуществлены в отношении компаний, доходы которых не превышали 50 миллионов долларов США (47 миллионов евро).

18. Суммы выкупа колеблются от нескольких сотен долларов или евро в виртуальных активах в случае мелких атак, совершаемых в отношении физических лиц, до миллиона долларов или евро в виртуальных активах если жертвами атак становятся крупные корпорации или организации, связанные с объектами критической инфраструктуры либо хранящие чувствительную или ценную информацию. Опыт юрисдикций показывает, что размер выкупа, требуемый преступниками, также увеличился в последние годы. В 2021 году средний размер выплаченного выкупа составил примерно 800 000 долларов США (748 000 евро) в виртуальных активах, что почти в пять раз больше чем в 2020 году. Такое увеличение, вероятно, связано с использованием тактики «охоты на крупную дичь», как было отмечено выше. А в отдельных случаях размер требуемого выкупа достигал десятков миллионов долларов или евро в виртуальных активах. Например, по сообщениям прессы, в 2021 году расположенная в США страховая компания подверглась атаке с использованием вредоносного ПО Phoenix CryptoLocker (считается, что после программ Conti и DarkSide это третья по прибыльности программа-вымогатель, используе-

[15] Компания «Sophos», "The State of Ransomware in State and Local Government" («Атаки с использованием программ-вымогателей в отношении государственных и местных правительственных организаций» от сентября 2022 г.), документ доступен по адресу: https://assets.sophos.com/X24WTUEQ/at/rbjqpp5wwm6v5h3wj9v3733/sophos-stateof-ransomware-government-2022-wp.pdf.

[16] Компания «Digital Shadows», "Ransomware: Analyzing The Data From 2020" («Программы-вымогатели: анализ данных за 2020 год» от января 2021г.), документ доступен по адресу: www.digitalshadows.com/blog-and-research/ransomware-analyzing-the-data-from2020/.

мая в рамках модели RaaS). Сообщалось, что эта страховая компания выплатила 40 миллионов долларов США (37 миллионов евро) в качестве выкупа в обмен на восстановление контроля над своей сетью[19].

Характеристики и географические тенденции

19. В целом, атаки с использованием программ-вымогателей - международное явление, отчасти по причине международного характера киберпреступности и виртуальных активов. При этом информация, полученная от членов глобальной сети ФАТФ, примеры дел, а также данные из отраслевых источников указывают на определённые характеристики и географические тенденции, касающиеся атак с использованием программ-вымогателей. В частности, большое количество преступных сетей, совершающих атаки с использованием программ-вымогателей, связано с юрисдикциями, в которых присутствуют повышенные риски ОД (см. Вставку 2). Во многих случаях преступники, совершающие атаки с использованием программ-вымогателей, размещают или обналичивают свои доходы в этих юрисдикциях. В других случаях атаки с использованием программ-вымогателей совершались с территории этих юрисдикций или спонсировались этими юрисдикциями[20].

Вставка 2: Юрисдикции, характеризующиеся повышенными рисками отмывания денег

Следует отметить, что не существует общепризнанного определения или методики установления того факта, что юрисдикция характеризуется повышенным риском ОД/ФТ. Тем не менее, информация о характерных для конкретной страны рисках и других факторах риска может быть полезна для определения потенциальных рисков ОД/ФТ. Примеры наличия признаков повышенного риска:

(a) страны или географические регионы, которые, согласно данным надежных источников, осуществляют финансирование или оказывают содействие террористической деятельности, или на территории которых действуют организации, включённые в списки террористических;

(b) страны, которые, согласно данным надежных источников, характеризуются значительным уровнем организованной преступности, коррупции или иной преступной деятельности, включая производство и транзит наркотиков, торговлю людьми, контрабанду, и незаконную организацию и проведение азартных игр;

(c) страны, в отношении которых международными организациями, такими как ООН, введены санкции, эмбарго или аналогичные меры; и

(d) страны, которые, согласно данным надежных источников, характеризуются слабым режимом государственного управления, обеспечения правопорядка и ре-

[19] Мехротра, Картикай и Уильям Тертон, "CNA Financial Paid $40 Million in Ransom After March Cyberattack" («Компания CNA Financial заплатила выкуп в размере 40 миллионов долларов после кибератаки, совершённой в марте», агентство «Блумберг», 20 мая 2021 года (дата обращения: 1 декабря 2022 г), документ доступен по адресу: www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-inransom-after-march-cyberattack

[20] См. Письмо-предупреждение (AA22-187A) Агентства по кибербезопасности и защите инфраструктуры США (июль 2022г.), документ доступен по адресу: www.cisa.gov/uscert/ncas/alerts/aa22-187a.

гулирования, включая страны, указанные в заявлениях ФАТФ в качестве стран со слабым режимом ПОД/ФТ, особенно по отношению к ПУВА. ПУВА и другие подотчетные субъекты должны обращать особое внимание на деловые отношения и операции с этими странами.

Источник: ФАТФ (2021г.) Обновлённое руководство по применению риск-ориентированного подхода: виртуальные активы и ПУВА, пункт 154

20. Количество атак, совершаемых с использованием программ-вымогателей, зависит от географического положения. В отраслевых докладах от 2022 года указано, что регион Ближнего Востока и Африки был в наименьшей степени подвержен атакам с применением программ-вымогателей (4%), далее - Латинская Америка (6%), Азиатско-Тихоокеанский регион (10%), Европа (28%), и Северная Америка (52%)[21]. Такое отличие в количестве атак влияет на то, как регионы воспринимают грозящие им риски от атак с использованием программ-вымогателей. Информация, предоставленная членами глобальной сети ФАТФ, указывает на то, что юрисдикции, сталкивающиеся с растущим количеством случаев «охоты на крупную дичь» и выплатой больших выкупов потерпевшими, с большей вероятностью оценивают риски ОД, связанные с атаками с использованием программ-вымогателей, как высокие.

21. Многие крупные группировки, совершающие атаки с применением программ-вымогателей, используют так называемую «партнёрскую модель» RaaS (программа-вымогатель как услуга). В рамках этой модели они берут на себя выполнение некоторых элементов атаки в обмен на оплату и/или процент от выкупа. В таких случаях преступники часто находятся в разных географически удалённых друг от друга регионах, вследствие чего могут возникнуть трудности в установлении личности и местонахождения участников таких атак. Например, как видно из материалов дела, касающегося использования вредоносной программы EMOTET (см. ниже), преступники могут сотрудничать при осуществлении атак или использовать общую инфраструктуру, действуя при этом с территории разных юрисдикций. Такая неоднородность состава преступной группы, действующей в разных юрисдикциях, может дополнительно затруднить отслеживание денежных потоков, связанных с ключевыми фигурантами.

Вставка 3. Дело EMOTET[1]

Использование вредоносной программы EMOTET - один из самых значительных случаев массового совершения атак с помощью программ-вымогателей за последние годы. Эта программа была впервые выявлена как «банковский троян»[2] в 2014 году, а впоследствии превратилась в ключевой инструмент для совершения других атак с применением вредоносных программ и программ-вымогателей. На момент ликвидации преступной сети в январе 2021 года с помощью программы EMOTET в мире осуществлялось до 70% атак с использованием программ-вымогателей, включая такие программы как RYUK и DoppelPaymer, которые нанесли значительный

[21] Компания «Group-IB», "Ransomware Uncovered Report. Group-IB" («Доклад о выявленных программах-вымогателях» от мая 2022 г.), документ доступен по адресу: https://spiresolutions.com/wpcontent/uploads/2021/07/ransomware_uncovered_2020.pdf.

экономический ущерб коммерческим предприятиям в Великобритании. Ликвидация этой преступной сети стала результатом тесного сотрудничества и взаимодействия правоохранительных органов Канады, Франции, Германии, Литвы, Нидерландов, Украины, Великобритании и США при координации международных усилий со стороны Европола и Евроюста. Благодаря совместной работе правоохранительные органы стран смогли найти и проанализировать информацию, позволяющую установить связь между реквизитами для совершения платежа и регистрационными данными преступников, использовавших программу EMOTET. Это дело стало яркой иллюстрацией размаха и характера киберпреступности и продемонстрировало ключевую роль международного сотрудничества в борьбе с этой угрозой.

Источник: Великобритания

Примечания:

[1] См. также пресс-релиз Европола по делу EMOTET, документ доступен на сайте: www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99smost-dangerous-malware-emotet-disrupted-through-global-action

[2] Банковский троян – это вредоносная программа, используемая злоумышленниками для хищения учетных данных клиентов финансовых учреждений или получения доступа к их финансовой информации.

22. Отмывание преступных доходов в виде выкупа, полученного в результате атак с применением программ-вымогателей, также носит транснациональный характер с учётом трансграничного характера виртуальных активов, которые почти всегда используются для осуществления таких платежей. Пользователи виртуальных активов могут осуществлять пиринговые операции, т.е. проводить операции напрямую друг с другом, используя только свои закрытые ключи и подключение к Интернет, независимо от географических границ и без участия учреждений, на которые распространяются обязательства в сфере ПОД/ФТ. Преступники, включая преступников, использующих программы-вымогатели, имеющие доступ в Интернет, могут использовать эти характеристики виртуальных активов для проведения крупномасштабных и практически мгновенных трансграничных операций без участия традиционных финансовых посредников, у которых реализованы программы в сфере ПОД/ФТ. Кроме того, у преступников есть возможность получить доступ к ПУВА в любой юрисдикции со слабыми или вовсе отсутствующими мерами контроля в целях ПОД/ФТ, услугами которых они могут воспользоваться для конвертации своих незаконных доходов в фиатную валюту.

Вставка 4: Что такое виртуальные активы?

Виртуальные активы являются средством цифрового выражения стоимости, которое может торговаться или переводиться цифровым образом и может быть использовано для целей платежей или инвестиций. Виртуальные активы не включают в себя средства цифрового выражения фиатных валют, ценных бумаг и других финансовых активов, уже охваченных требованиями в других разделах Рекомендаций ФАТФ.

Наиболее широко используемые виртуальные активы являются средством обмена, записи о выпуске или владении которыми обеспечиваются с помощью технологии распределённого реестра, основанной на криптографии, такой как блокчейн. Как отмечено ниже, многие популярные виртуальные активы функционируют на открытых блокчейнах, где информация об операциях, осуществляемых под псевдонимами, доступна для просмотра.

Источник: ФАТФ

Распространённые методы и тенденции

23. Проведение успешных расследований атак, совершаемых с помощью программ-вымогателей, требует хорошего понимания способов и технологий, используемых для легализации преступных доходов. Поскольку потерпевшие часто не сообщают о таких атаках, в данном отчёте собрана информация из различных открытых источников, а также обобщён накопленный юрисдикциями опыт, чтобы лучше понять, как осуществляется оплата выкупа и как выкуп получают, отмывают и в некоторых случаях обменивают на фиатную валюту.

24. Множество традиционных финансовых учреждений, а также ПУВА участвуют в финансовых потоках, связанных с атаками с использованием программ-вымогателей. Другие третьи стороны, такие как компании по кибербезопасности и компании по реагированию на инциденты, также могут быть задействованы в ответных мерах на атаки, совершаемые с помощью программ-вымогателей, в том числе в процессе выплаты выкупа от имени потерпевших.

25. Хотя виртуальные активы выступают в качестве основного средства и метода оплаты выкупа при совершении атак с использованием программ-вымогателей, в финансовые потоки, связанные с такими атаками, вовлечено множество традиционных финансовых учреждений, а также ПУВА и дополнительные третьи стороны.

Таблица 1: Виды секторов, которые могут быть вовлечены в финансовые потоки, связанные с атаками с использованием программ-вымогателей

Финансовые учреждения	Финансовые учреждения, как правило, выступают в качестве посредников, которых используют жертвы вышеупомянутых атак (или третьи лица, выступающие от имени жертв) для перевода денежных средств провайдерам услуг в сфере виртуальных активов в целях приобретения виртуальных активов.
ПУВА	Жертвы атак (или третьи лица, выступающие от имени жертв) используют ПУВА для приобретения и перевода виртуальных активов определённого типа и на определённую сумму, которые указаны преступниками в требовании о выплате выкупа.
Страховые компании	Страховые компании могут осуществлять покрытие и иногда выплату выкупа в рамках кибербезопасности.
Компании по реагированию на инциденты	Компании по реагированию на инциденты, с которыми связываются жертвы атак с использованием программ-вымогателей, нередко ведут переговоры с преступниками о выплате выкупа. В рамках своих услуг такие компании могут приобретать виртуальные активы у ПУВА с целью выплаты выкупа и переводить эти активы преступникам от имени жертв.
Компании по кибербезопасности	Компании, отвечающие за обеспечение сохранности и защиты данных, систем, сетей и подключённых устройств клиентов от любого несанкционированного или незаконного доступа.

Вставка 5: Типичные финансовые потоки, связанные с выплатой выкупа в результате совершения атак с использованием программ-вымогателей

После получения требования о выплате выкупа жертва или третья сторона, действующая от имени жертвы, как правило, переводят денежные средства (с помощью банковского перевода, автоматической клиринговой системы или банковской карты) провайдеру услуг в сфере виртуальных активов для приобретения и перевода виртуальных активов определённого вида и на определённую сумму, которые указаны преступниками, совершившими атаку.

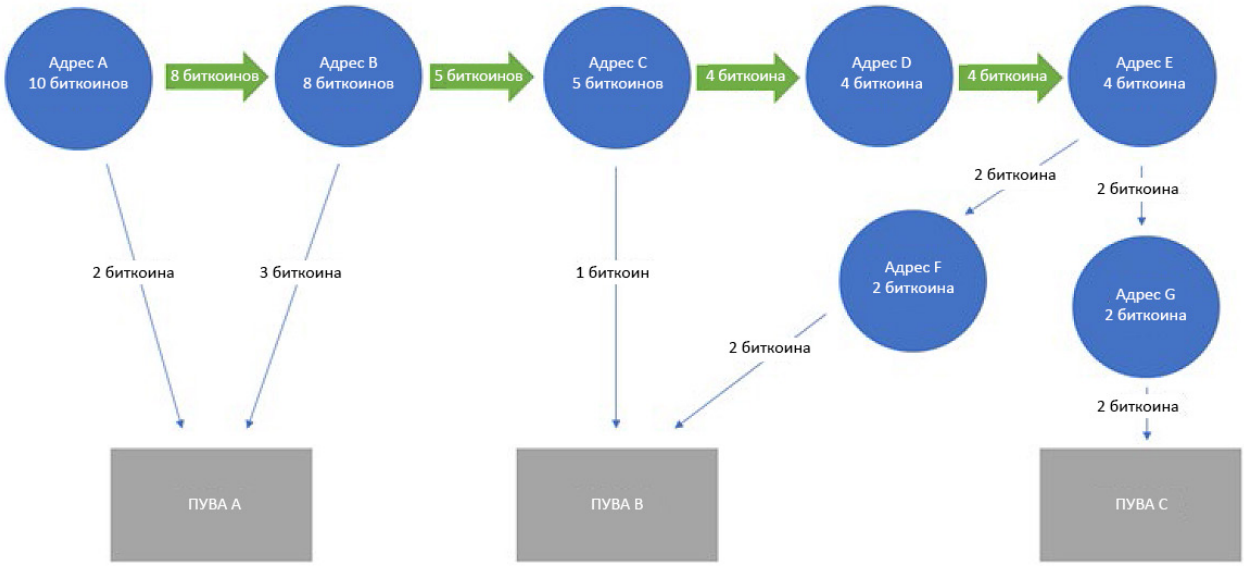
Затем жертва или третья сторона осуществляют выплату выкупа часто с кошелька, открытого на сайте ПУВА, на адрес кошелька виртуальных активов преступника. Обычно это - автономный кошелёк (программно-аппаратные средства, позволяющие пользователям размещать, хранить и переводить виртуальные активы без участия сторонних лиц, таких как ПУВА; это также называется некастодиальный кошелёк), контролируемый совершившим атаку преступником или «денежным мулом», или кошелёк, открытый на сайте ПУВА, находящегося за пределами юрисдикции, в которой была совершена атака, и, как правило, не сотрудничающего с правоохранительными органами или ПФР.

После этого преступники, совершающие атаки с использованием программ-вымогателей, часто используют разные методы для запутывания следов (более подробно эти методы описаны ниже). И, наконец, преступники, совершающие атаки с использованием программ-вымогателей, нередко пользуются услугами ПУВА, находящихся за пределами юрисдикций, в которых они проживают, для обмена полученных виртуальных активов на фиатную валюту. При этом киберпреступники могут также хранить активы в автономных кошельках или использовать виртуальные активы для оплаты услуг сторонних лиц, участвовавших в осуществлении атак.

26. Для отмывания доходов от своей противозаконной деятельности преступники, совершающие атаки с использованием программ-вымогателей, применяют технологии, методы и токены, повышающие уровень анонимности, включая один или несколько методов, описанных ниже. Преступники, совершающие атаки с использованием программ-вымогателей, могут не использовать каждый раз одни и те же элементы или один и тот же порядок действий в процессе легализации своих доходов.

- Преступники, совершающие атаки с использованием программ-вымогателей, часто требуют, чтобы их жертвы выплачивали выкуп виртуальными активами, переводя их на адреса кошельков, контролируемых преступниками. При этом хакеры часто используют **разные адреса кошельков** для получения незаконных доходов от каждой осуществлённой атаки.
- После получения выкупа преступники могут использовать несколько промежуточных адресов для последовательного перевода виртуальных активов с одного адреса кошелька на другие адреса путём осуществления серии операций на небольшие суммы. При этом средства часто переводятся на адрес кошельков, открытых на сайтах нескольких разных ПУВА. Такая схема операций называется **«пилинг-цепь» (peel chain)** и применяется не только исключительно для запутывания следов перемещения виртуальных активов[22]. Такие схемы могут также использоваться преступниками для отмывания крупных сумм виртуальных активов путём проведения серии небольших операций с целью снижения возможностей отследить их перемещение. В частности, след виртуальных активов может быть запутан и сокрыт, если такие операции осуществляются с большой скоростью и частотой.

Рисунок 1: Пример «пилинг-цепи»



- Преступники, совершающие атаки с использованием программ-вымогателей, также часто отмывают виртуальные активы, используя для этого **«миксеры» или «тумблеры»** (например, миксер Wasabi), которые предусматривают разные методы сокрытия связи между адресом кошелька отправителя виртуальных активов и адресом кошелька получателя виртуальных активов.

[22] «Пилинг-цепи» часто наблюдаются на практике и могут возникать естественным путём в зависимости от устройства кошельков виртуальных валют.

Преступники используют такие «миксеры»/«тумблеры» в качестве альтернативного способа или в дополнение к схеме перемещения виртуальных активов путём «пилинг-цепи». В некоторых случаях киберпреступники используют технологию CoinJoin для осуществления операций, при которой несколько отправителей и получателей средств объединяют свои платежи в единую общую транзакцию. Для этого часто требуется специальный сервис, такой как JoinMarket, который сводит заинтересованных пользователей и помогает формировать такие транзакции.

- Кроме того, преступники, совершающие атаки с использованием программ-вымогателей, также применяют **криптовалюты, обеспечивающие повышенную степень анонимности (КПА, которые также называются «анонимные монеты»),** хотя большинство злоумышленников требуют выплачивать выкуп в биткоинах. Опыт юрисдикций и отраслевые отчёты показывают, что криптовалюты, обеспечивающие повышенную степень анонимности, используются для оплаты выкупа преступникам, поскольку они могут обеспечить сокрытие кошельков отправителей и получателей. Например, при использовании КПА может применяться сочетание технологий, направленных на повышение степени анонимности, таких как миксеры (mixers), кольцевые подписи (ring signatures), скрытые адреса (stealth addresses) и кольцевые конфиденциальные транзакции (ring confidential transactions). Такие технологии могут обеспечивать маскировку кошельков отправителей и получателей. Все большее число преступников, совершающих атаки с использованием программ-вымогателей, требуют оплачивать выкуп исключительно в криптовалюте Монеро (Monero), хотя наиболее часто используемым виртуальным активом для оплаты выкупа в результате атак с использованием программ-вымогателей является биткоин (он используется в 99% случаев)[23]. Некоторые юрисдикции сталкивались со случаями, когда хакеры требовали заплатить выкуп как в биткоинах, так и в Монеро. Однако в случае выплаты выкупа в биткоинах преступники, как правило, требуют дополнительную оплату в размере от 10 до 20 процентов от суммы выкупа, поскольку такие операции проще отследить, и преступники несут дополнительные расходы на использование технологий, обеспечивающих повышенную степень анонимности (технология «миксеры»). Применение таких технологий затрудняет государственным органам возможность отследить или привязать операции к конкретным лицам.

- Несколько юрисдикций также отметили, что киберпреступники часто переводят полученный выкуп из биткоинов в другие виды виртуальных активов через ПУВА или DeFi протоколы[24,25]. Такой метод часто называется **«chain-hopping» («прыжки между сетями»)** и означает переход от одного вида виртуальных активов в другой блокчейн, как правило, в быстрой последовательности с целью избежать попыток отследить такие перемещения.

[23] Компания «Coveware», Доклад за третий квартал (ноябрь 2019 г.), документ доступен по адресу: www.coveware.com/blog/q3-ransomware-marketplace-report.

[24] Термин «децентрализованные финансы (DeFi)» используется, когда децентрализованные или распределённые приложения на блокчейне со смарт-контрактом предлагают финансовые услуги, аналогичные тем, которые предоставляются провайдерами услуг в сфере виртуальных активов. Лицо, использующее приложение DeFi (т.е. программное обеспечение), не является ПУВА, поскольку Стандарты ФАТФ не применяются к соответствующему ПО или технологии. Однако создатели, владельцы, операторы или некоторые другие лица, которые осуществляют контроль над деятельностью, связанной с системой DeFi, или оказывают на нее существенное влияние, могут подпадать под определение понятия «ПУВА», сформулированное ФАТФ, в тех случаях, когда они оказывают услуги в качестве ПУВА или активно содействуют предоставлению таких услуг.

[25] Помимо их использования с целью отмывания денег, полученных в результате оплаты выкупа, DeFi протоколы сами по себе, особенно «межсетевые мосты» (cross-chain bridges), все более часто становятся целью киберпреступников, которые пытаются воспользоваться пробелами в системах безопасности и похитить виртуальные активы.

Одна юрисдикция сообщила, что преступники всё чаще используют DeFi протоколы для перевода виртуальных активов в так называемые стейблкоины[26], применяя метод «chain-hopping», перед окончательным обменом средств на фиатную валюту. Такие DeFi платформы являются привлекательными для преступников, поскольку на многих из этих платформ не реализуются меры контроля в целях ПОД/ФТ, даже несмотря на то, что на них могут распространяться обязательства в сфере ПОД/ФТ, в зависимости от конкретных обстоятельств и особенностей их бизнес-моделей. Одна юрисдикция сообщила о том, что обнаружила постоянное незаконное использование DeFi платформ и миксеров, причём в некоторых случаях они использовались много раз подряд в процессе отмывания преступных доходов.

- В процессе отмывания незаконных доходов преступники часто используют услуги централизованных ПУВА, включая внебиржевых трейдеров, для обналичивая своих доходов. Преступники, совершающие атаки с использованием программ-вымогателей, часто переводят виртуальные активы провайдерам услуг в сфере виртуальных активов, которые находятся в представляющих высокий риск юрисдикциях или не реализуют меры контроля в целях ПОД/ФТ, для их перевода в фиатную валюту. Преступники, находящиеся в представляющих высокий риск юрисдикциях, могут использовать местных централизованных ПУВА для этих целей, как, например, в случаях внесенных США в списки криптобирж «Suex»[27], «Chatex»[28], «Garantex»[29] и «Bitzlato Limited» (см. Вставку 6 ниже)[30]. Несколько юрисдикций сообщили о наличии большого количества обменников по обналичиванию виртуальных активов, сосредоточенных в центральных районах городов. В некоторых случаях преступники, входящие в разные группировки, используют одних и тех же ПУВА для получения или отмывания своих виртуальных активов.
- В случаях когда в совершении преступлений задействовано несколько разных субъектов, преступники вынуждены оплачивать услуги своих «партнёров» по криминальному бизнесу, а также платить владельцам инфраструктурных объектов, которые используются для совершения атак. Операторы инфраструктуры, использующейся в преступных целях, всё чаще соглашаются принимать оплату в виртуальных активах, и преступники, совершающие атаки с использованием программ-вымогателей, нередко осуществляют такие платежи, используя доходы от своих атак. Во многих случаях компании, занимающиеся блокчейн-анализом, отмечали прямой перевод выкупа на адрес кошельков виртуальных активов, принадлежащих операторам сервисных систем, предоставляющих преступникам «инфраструктуру как услугу».

---

[26] Примечание, касающееся терминологии: ФАТФ считает, что понятие «стейблкоин» не относится к правовой или технической категории, но является, главным образом, маркетинговым понятием, которое используют те, кто продвигает такие валюты. В связи с тем, что ФАТФ не согласна с употреблением этого названия, в данном отчёте используется термин «так называемые стейблкоины».

[27] См. пресс-релиз Министерства финансов США, документ доступен по адресу: https://home.treasury.gov/news/pressreleases/jy0364

[28] См. пресс-релиз Министерства финансов США, документ доступен по адресу: https://home.treasury.gov/news/pressreleases/jy0471

[29] См. пресс-релиз Министерства финансов США, документ доступен по адресу: https://home.treasury.gov/news/pressreleases/jy0701

[30] См. пресс-релиз Министерства юстиции США, документ доступен по адресу: www.justice.gov/opa/pr/founder-and-majority-owner-cryptocurrency-exchangecharged-processing-over-700-million

Вставка 6: Криптобиржа «Bitzlato Limited»[1]

В январе 2023 года в результате международной операции было установлено, что биржа виртуальных активов «Bitzlato Limited» (значительный объём деятельности которой осуществляется в России) сыграла очень важную роль в отмывании конвертируемой виртуальной валюты (CVC). Указанная операция проводилась под руководством властей Франции и США при поддержке Европола, и в ней также приняли участие представители государственных органов Бельгии, Кипра, Португалии, Испании и Нидерландов. Криптобиржа «Bitzlato» подозревалась в оказании содействия проведению различных незаконных транзакций, в том числе преступникам, совершающим атаки с использованием программ-вымогателей. В их числе фигурирует связанная с Россией хакерская группировка Conti, которая использует модель «программа-вымогатель как услуга». По утверждению Министерства юстиции США, криптобиржа «Bitzlato» получила более 15 миллионов долларов в качестве дохода от атак с использованием программ-вымогателей. Одновременно с этим американское ПФР (Сеть по борьбе с финансовыми преступлениями) издало постановление, в котором указано, что криптобиржа «Bitzlato» «вызывает серьёзную озабоченность в связи с отмыванием денег».

В результате проведённых расследований криптобиржа была ликвидирована, а также был наложен арест на цифровую инфраструктуру и преступные активы на сумму 18 миллионов евро, хранившиеся в криптокошельках во Франции. Кроме того, расследование привело к аресту ключевых руководителей этой криптобиржи в разных юрисдикциях.

В своей рекламе криптобиржа «Bitzlato» позиционировала себя как платформа с минимальными требованиями по идентификации пользователей. По причине такой ограниченной процедуры идентификации клиентов криптобиржа «Bitzlato» предположительно стала чрезвычайно привлекательным местом для размещения преступных доходов и средств, предназначенных для использования в преступной деятельности.

Источник: Франция и США

[1] См. также пресс-релиз Национальной жандармерии Франции, документ доступен по адресу: www.gendarmerie.interieur.gouv.fr/gendinfo/enquetes/2023/demantelement-dune-plateforme-de-cryptomonnaies-servant-au-blanchiment; а также пресс-релиз Европола, документ доступен по адресу: www.europol.europa.eu/mediapress/newsroom/news/bitzlato-senior-management-arrested

27. Некоторые юрисдикции также отметили, что хакеры-вымогатели используют «денежных мулов», имеющих открытые у ПУВА счета, для перевода доходов в фиатную валюту с помощью «офф-рэмпов» (off-ramps), т.е. сервисов/платформ, позволяющих обменивать виртуальные активы на фиатную валюту (это также иногда называется «обналичиванием»). Такие счета могут быть открыты с помощью украденных или поддельных документов, удостоверяющих личность, а также могут являться вполне законными счетами, которые принадлежат третьим лицам. «Денежные мулы» являются, как правило, сторонними лицами, которых задействуют на последнем этапе процесса отмывания денег. «Денежные мулы» отвечают за часть от общего объёма средств в процессе их отмывания. Отсутствие прямой связи между «денежными мулами» и преступной группировкой, а также осуществляемые ими операции на мелкие суммы может затруднить их выявление.

Вставка 7: Пример вербовки «денежных мулов»

Преступники, совершающие атаки с использованием программ-вымогателей, вербуют **«денежных мулов»** и предоставляют им устройства мобильной связи. В большинстве случаев такие «денежные мулы» не пользуются Интернетом и слабо в нём разбираются. После этого у провайдеров услуг анонимной электронной почты, находящихся за пределами юрисдикции, создаются учётные записи электронной почты. Это делается с тем, чтобы затруднить установление личности пользователей таких учётных записей. Затем «денежные мулы» с помощью устройств мобильной связи, предоставленных им «куратором» из числа преступников, связываются с финансовыми учреждениями или ПУВА для прохождения регистрации и открывают у них счета. После успешного приёма на обслуживание «денежные мулы» возвращают указанные устройства мобильной связи «куратору». Затем «кураторы» используют эти устройства мобильной связи для осуществления онлайн транзакций в Интернете от имени «денежных мулов». В некоторых случаях преступники пользуются сервисами виртуальных частных сетей (VPN), которые обеспечивают анонимность IP-адреса используемого устройства. В результате реальное географическое местонахождение преступника, осуществляющего транзакции, остаётся сокрытым.

Источник: ЮАР

ЧАСТЬ II: СЛОЖНОСТИ И ПЕРЕДОВАЯ ПРАКТИКА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЮ ДОХОДОВ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Нормативно-правовая база

28. Прочная нормативно-правовая база служит фундаментом, позволяющим компетентным органам разрабатывать эффективную политику, направленную на снижение рисков, связанных с совершением атак с использованием программ-вымогателей. В данном разделе рассматривается актуальность Стандартов ФАТФ применительно к: (i) криминализации атак с использованием программ-вымогателей в качестве предикатного преступления для ОД; и (ii) реализации превентивных мер в соответствующих регулируемых секторах.

Атаки с использованием программ-вымогателей как предикатное преступление для ОД

29. В большинстве юрисдикций отсутствует специальное уголовное законодательство, касающееся атак с использованием программ-вымогателей. Тем не менее, это в целом не мешает юрисдикциям осуществлять уголовное преследование за совершение таких атак как за предикатное преступление[31].

30. Информация, полученная от участников проекта, указывает на то, что юрисдикции, как правило, осуществляют уголовное преследование за атаки с использованием программ-вымогателей, предъявляя обвинения в вымогательстве, или более часто квалифицируют такие атаки как компьютерные преступления, а именно повреждение данных, проникновение или повреждение компьютерных программ и систем. В соответствии с Рекомендаций 3 ФАТФ юрисдикции должны установить уголовную ответственность за отмывание доходов от преступлений, связанных с вымогательством. Состав таких преступлений как вымогательство удобен тем, что вымогательство является уголовно наказуемым деянием независимо от используемых технологий. А это означает, что атаки с использованием программ-вымогателей, независимо от форм и методов их осуществления, подпадают под понятие вымогательство. Тем юрисдикциям, которые применяют статьи, касающиеся вымогательства, для уголовного преследования за совершение атак с использованием программ-вымогателей, следует обеспечить, чтобы их законодательство позволяло компетентным органам эффективно расследовать и возвращать незаконно полученные виртуальные активы (см. раздел 6).

31. В отличие от вымогательства, компьютерные преступления не вошли в минимальный перечень предикатных преступлений, определённый ФАТФ[32]. Однако, похоже, что это не мешает осуществлять на практике преследование за отмывание доходов от совершения атак с использованием программ-вымогателей. Анализ выборки юрисдикций показывает, что страны, которые используют статьи уголовного законодательства, касающиеся компьютерных преступлений, для преследования за совершение атак с применением программ-вымогателей, относят такие атаки к предикатным преступлениям (либо путём включения их

[31] Большинство юрисдикций сообщило, что они не ввели уголовную ответственность за выплату потерпевшими выкупа злоумышленникам, совершающим атаки с использованием программ-вымогателей. При этом в некоторых юрисдикциях настоятельно не рекомендуют потерпевшим выплачивать выкуп преступникам.

[32] См. перечень установленных категорий преступлений в Глоссарии к Рекомендациям ФАТФ.

в перечень предикатных преступлений, либо в рамках подхода, согласно которому все преступления являются предикатными для ОД). В ходе данного исследования ни одна из юрисдикций не сообщила о проблемах, связанных с уголовным преследованием за отмывание доходов от атак, совершённых с использованием программ-вымогателей. Тем не менее, юрисдикциям следует обеспечить, чтобы выбранная ими статья для предъявления обвинения в совершении предикатного преступления не ограничивала их возможности осуществлять уголовное преследование за отмывание доходов от атак с использованием программ-вымогателей.

Применение превентивных мер в соответствующих секторах

32. Согласно Стандартам ФАТФ, юрисдикции должны реализовывать меры для предупреждения отмывания денег, и такие меры должны применяться, в том числе, финансовыми учреждениями, установленными нефинансовыми предприятиями и профессиями (УНФПП) и провайдерами услуг в сфере виртуальных активов (ПУВА). Реализация этих мер обеспечивает то, что указанные субъекты понимают и снижают свои риски ОД; применяют надлежащие меры контроля, включая идентификацию своих клиентов; и выявляют и сообщают о подозрительных операциях в соответствии с требованиями Рекомендаций 9 – 23 ФАТФ.

33. С учетом связи между применением программ-вымогателей и виртуальными активами, изменения и дополнения, внесённые в Стандарты ФАТФ в 2018 году для распространения этих мер на ПУВА, стали важным шагом в укреплении глобального режима ПОД/ФТ в целях снижения рисков, исходящих от атак с использованием программ-вымогателей. Однако, по состоянию на январь 2023 года[33], из 86 юрисдикций, прошедших оценку на соответствие пересмотренным Стандартам (т.е. Рекомендации 15), 63 юрисдикции (73%) получили рейтинг «частичное соответствие» или «несоответствие» по этим требованиям[34]. И только одна из 86 юрисдикций получила рейтинг «полное соответствие» по результатам взаимной оценки.

34. Учитывая число юрисдикций, прошедших оценку на соответствие пересмотренной Рекомендации 15, указанные цифры с большой вероятностью отражают положение дел во всех остальных юрисдикциях-членах глобальной сети ФАТФ. Эта оценка также подтверждается результатами опроса ФАТФ, проведённого в марте 2022 года, согласно которому в 2022 году менее чем половина респондентов имели режим лицензирования или регистрации виртуальных активов и ПУВА. Таким образом, у большинства юрисдикций, вероятно, имеются пробелы и недостатки в выполнении провайдерами услуг в сфере виртуальных активов обязательств в сфере ПОД/ФТ, в том числе в части, касающейся идентификации клиентов и направления сообщений о подозрительных операциях. Принимая во внимание трансграничный характер виртуальных активов, важно, чтобы юрисдикции-члены глобальной сети ФАТФ ускоренными темпами обеспечили выполнение требований Рекомендации 15 (в том числе, требования, касающиеся так называемого «дорожного правила»).

---

[33] См. сводные рейтинги по результатам взаимных оценок, документ доступен по адресу: www.fatfgafi.org/en/publications/Mutualevaluations/Assessment-ratings.html. Обращаем ваше внимание на то, что не все юрисдикции прошли оценку на соответствие Рекомендации 15 с использованием пересмотренной Методологии.

[34] Этот анализ основан на отчётах о взаимной оценке и отчётах о прогрессе юрисдикций, которые прошли оценку на соответствие Рекомендации 15 с использованием пересмотренной Методологии.

Предлагаемые меры

- Юрисдикциям следует в ускоренном порядке обеспечить соблюдение требований соответствующих Стандартов ФАТФ, касающихся сектора ПУВА, путём реализации положений Рекомендации 15 (включая так называемое «дорожное правило») в максимально сжатые сроки. Это обеспечит выполнение провайдерами услуг в сфере виртуальных активов необходимых обязательств в сфере ПОД/ФТ, касающихся сбора критически важной финансовой информации и направления сообщений о подозрительных операциях.
- Юрисдикциям следует обеспечить, чтобы за атаки с использованием программ-вымогателей была установлена уголовная ответственность и чтобы такие деяния квалифицировались как предикатные преступления для отмывания денег (например, как один из видов вымогательства) в соответствии с Рекомендацией 3 ФАТФ.

Выявление и информирование

35. По причине нахождения преступников, совершающих атаки с использованием программ-вымогателей, в разных географических регионах, а также ввиду широкого спектра методов, применяемых ими для легализации преступных доходов, и текущих особенностей осуществления атак с использованием программ-вымогателей (о чём говорилось в Части I выше), трудно оценить масштаб финансовых потоков, связанных с этим явлением. В большинстве юрисдикций власти по-прежнему получают сообщения не обо всех совершаемых атаках с использованием программ-вымогателей, что затрудняет получение полной картины финансовых доходов и финансовых потоков, связанных с применением программ-вымогателей.

36. Эффективное выявление и информирование о таких случаях является основой для проведения успешных финансовых расследований (см. раздел 6 ниже). На основании опыта юрисдикций и предоставленных примеров дел можно выделить два основных источника для выявления финансовых потоков, связанных с проведением атак с использованием программ-вымогателей, а именно сообщения о подозрительных операциях (СПО) и сообщения, поступающие от потерпевших. В данном разделе рассматриваются трудности и передовая практика, касающаяся охвата требованиями о направлении СПО; выявления подозрительных операций; стимулирования потерпевших сообщать об атаках; и других источников информации для выявления таких атак.

Охват обязательствами, касающимися направления СПО

37. Компетентные органы широко используют СПО для выявления атак, совершаемых с применением программ-вымогателей, а также в качестве источника информации в ходе проведения расследований. На сегодняшний день подавляющее большинство СПО, касающихся выплат выкупа в результате осуществления атак с использованием программ-вымогателей, поступает от ПУВА и банков.

38. В качестве дополнительных потенциальных источников информации для выявления незаконных доходов, получаемых в результате совершения атак с применением программ-вымогателей, небольшое число юрисдикций указали на секторы, на которые, как правило, не распространяются обязательства в сфере ПОД/ФТ. Стимулирование или введение требований для участников таких нетрадиционных сек-

торов направлять сообщения о подозрительных операциях может оказаться полезным, особенно, когда субъекты этих секторов напрямую участвуют в реагировании на атаки с применением программ-вымогателей от имени своих клиентов.

39. Например, участники более широкого сектора страхования, в частности, учреждения, занимающиеся страхованием от кибервымогательства и киберрисков, могут располагать информацией, непосредственно касающейся атак с применением программ-вымогателей, в случаях, когда застрахованные от киберрисков клиенты обращаются к ним с требованием о выплате страхового возмещения. Такие субъекты не подпадают под сформулированное ФАТФ определение «финансовых учреждений», которое охватывает только андеррайтинг и размещение полисов страхования жизни и иных страховых полисов, связанных с инвестициями. Однако в результате взаимодействия с представителями этого сектора для стимулирования или введения требований о направлении сообщений, некоторые юрисдикции увидели в этом некоторый начальный положительный сдвиг в части увеличения количества сообщений о совершаемых атаках с использованием программ-вымогателей и выплате выкупа.

Вставка 8: Целевая информационно-разъяснительная работа в секторе страхования для повышения количества направляемых сообщений об атаках с использованием программ-вымогателей

Во Франции на субъекты сектора страхования, отличного от страхования жизни, распространяются требования в сфере ПОД/ФТ. В 2021 году в этом секторе была проведена информационно-разъяснительная работа в рамках специально созданных рабочих групп, в состав которых вошли представители государственного и частного сектора. Целью этих рабочих групп явилось изучение возможности страхования от киберрисков, а также повышение устойчивости компаний к кибератакам. Главным результатом работы, проведённой этими рабочими группами, стало опубликование отчёта[1], в котором, помимо всего прочего, содержится обзор эволюции рисков ОД, связанных с атаками с применением программ-вымогателей, а также обязательств в сфере ПОД/ФТ и передовой практики, касающейся выплаты выкупа и последующего страхового возмещения.

После этого Управление по пруденциальному надзору и разрешению споров Франции провело анализ страховых компаний, в том числе в ходе выездных надзорных проверок. По результатам этого анализа Управление напомнило регулируемым субъектам об их обязательствах в сфере ПОД/ФТ при оказании таких услуг, в том числе о необходимости мониторинга и получения соответствующей финансовой информации (особенно для отслеживания платежей).

С того времени Управление разведки и противодействия подпольным финансовым схемам (TRACFIN) Франции отмечает рост количества направляемых СПО, касающихся выплаты выкупа в результате атак с использованием программ-вымогателей, с 19 сообщений в 2019 году и 28 сообщений в 2020 году до 66 сообщений, полученных в 2021 году. Такое увеличение числа сообщений в 2021 году было частично достигнуто за счёт одной страховой компании, однако, общее количество сообщений является пока недостаточным для того, чтобы делать какие-либо выводы или заключения.

Источник: Франция

[1] Документ доступен на французском языке по адресу: www.banque-france.fr/sites/default/files/rapport_45_f.pdf

40. Компании по реагированию на инциденты также имеют доступ к актуальной информации, касающейся совершения атак с использованием программ-вымогателей и выплаты выкупа. Например, компании по цифровой криминалистике и реагированию на инциденты, а также юридические фирмы помогают потерпевшим реагировать на атаки, совершаемые с использованием программ-вымогателей. Они могут содействовать организации выплаты выкупа киберпреступникам путем обсуждения размера выкупа, обмена фиатной валюты клиентов на виртуальные активы и перевода средств на счета, контролируемые преступниками. Стимулирование или введение требований для субъектов этого сектора о направлении соответствующих сообщений позволяет своевременно выявлять и информировать о совершении атак с применением программ-вымогателей, особенно с учётом того, что клиенты, вероятно, в первую очередь сообщают об атаках этим субъектам (иногда даже раньше, чем обратятся в правоохранительные органы). В зависимости от бизнес-моделей и предоставляемых услуг эти компании могут подпадать под определение ПУВА (и соответственно на них могут распространяться требования в сфере ПОД/ФТ и обязательства о направлении СПО), если они осуществляют в качестве предпринимательской деятельности для или от имени другого физического или юридического лица обмен виртуальных активов на другие виртуальные активы или фиатную валюту; перевод виртуальных активов; или хранение или администрирование виртуальных активов.

Вставка 9: Регулирование деятельности компаний по цифровой криминалистике и реагированию на инциденты (ЦКРИ)

Компании по ЦКРИ, а также компании по страхованию от киберрисков в ходе оказания услуг могут оказывать содействие потерпевшим в результате атак с использованием программ-вымогателей, способствуя выплате выкупа. В 2020 и 2021 годах Сеть по борьбе с финансовыми преступлениями – FinCEN (ПФР США) разъяснила в своих информационных письмах[1], касающихся атак с использованием программ-вымогателей, что, в зависимости от фактов и обстоятельств, такая деятельность может квалифицироваться как перевод денег. Субъекты, осуществляющие операции по переводу денежных средств, обязаны зарегистрироваться в качестве провайдеров денежных услуг, и на них распространяются обязательства в сфере ПОД/ФТ. В этих информационных письмах также содержатся данные о настораживающих признаках и признаках выплаты выкупа и других платежей, связанных с атаками с применением программ-вымогателей. Такая информация приводится для сведения компаний по ЦКРИ и компаний по страхованию от киберрисков с тем, чтобы помочь им в выявлении подозрительной деятельности и в направлении сообщений о подозрительной деятельности (СПД).

За первые шесть месяцев 2021 года от компаний по ЦКРИ, находящихся на территории США, поступило примерно 63 процента от всех полученных СПД, касавшихся атак с использованием программ-вымогателей[2]. Общее количество сообщений, связанных с атаками с применением программ-вымогателей, полученных американским ПФР в 2021 году, также выросло на 188 процентов. Эти сообщения помогли американскому ПФР выявить схемы и проанализировать тенденции для содействия общегосударственным усилиям, направленным на предупреждение и пресечение атак с использованием программ-вымогателей. Например, анализ, проведённый американским ПФР за весь 2021 год, показал, что атаки с использованием программ-вымогателей продолжают представлять серьёзную угрозу

для секторов критически важной инфраструктуры, коммерческим предприятиям и гражданам США. Кроме того, анализ указывает на то, что версии программ-вымогателей, связанные с Россией, использовались в большинстве атак, о которых поступили сообщения, и на их долю пришлось 69 процентов ущерба, нанесённого атаками, а также 75 процентов атак, совершённых во второй половине 2021 года[3].

Источник: США

Примечания:

[1] Документ доступен на французском языке по адресу: www.banque-france.fr/sites/default/files/rapport_45_f.pdf

[2] См. анализ финансовых тенденций, проведённый Сетью FinCEN, документ доступен по адресу: www.fincen.gov/sites/default/files/2021- 10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

[3] См. анализ финансовых тенденций, проведённый Сетью FinCEN, документ доступен по адресу: www.fincen.gov/sites/default/files/2022- 11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf.

41. Всё вышесказанное наглядно показывает полезность стимулирования или введения требований, касающихся направления сообщений, для широкого круга нетрадиционных подотчётных субъектов с учётом рисков и общей ситуации. Это позволяет получать информацию о подозрительной деятельности от разных секторов и рассматривать её под разными углами, что расширяет возможности государственных органов по выявлению неизвестных случаев атак путём сбора воедино сведений, поступающих из различных секторов.

Меры по повышению эффективности выявления подозрительных операций

42. Юрисдикции признают тот факт, что в целом поступающие сведения о подозрительной деятельности, связанной с атаками с использованием программ-вымогателей, вероятно, являются неполными во всех секторах. Сложности в выявлении такой деятельности могут возникать вследствие географически децентрализованного характера преступных группировок, совершающих атаки с применением программ-вымогателей, большого количества разных преступных элементов, участвующих в таких атаках, а также применения разных способов и методов отмывания доходов. Представители ни одного сектора не могут видеть полной картины.

43. Для повышения количества и качества сообщений, направляемых регулируемыми субъектами, а также для более эффективного выявления атак юрисдикции используют разные методы, такие как взаимодействие с частным сектором, формирование списка настораживающих признаков и руководств по выявлению подозрительной деятельности и их распространение (также см. подраздел 8.3 ниже).

Вставка 10: Руководство Управления Израиля по предотвращению отмывания денег и финансирования терроризма (Управление по ПОД/ФТ), касающееся атак с использованием программ-вымогателей

Управление по предотвращению отмывания денег и финансирования терроризма (ПФР Израиля) провело стратегический анализ сообщений о необычной деятельности для определения характеристик операций, касающихся оплаты выкупа в результате совершения атак с использованием программ-вымогателей. Это включало информацию о частоте атак, видах организаций, в отношении которых осуществлялись атаки, о размере выплаченного выкупа, видах использовавшихся виртуальных активов и участия третьих сторон в этом процессе. По итогам этой работы было выпущено Руководство, касающееся атак с использованием программ-вымогателей, в котором приведены настораживающие признаки и примеры дел. Руководство было размещено на вебсайте Управления[1] и разослано всем соответствующим подотчётным субъектам, а также был выпущен официальный пресс-релиз.

Кроме того, результаты этого исследования были неоднократно представлены на публичных форумах и профессиональных конференциях. Публикация Руководства способствовала, помимо всего прочего, развитию взаимодействия с представителями израильских компаний по реагированию на инциденты, что, в свою очередь, способствовало дальнейшему расширению этих отношений и поиску возможностей для сотрудничества и обмена информацией в будущем.

Источник: Израиль

[1] Документ доступен только на иврите по адресу: www.gov.il/BlobFolder/dynamiccollectorresultitem/red-flags-typologyransomware-impa-140222/he/professionaldocs_red_flags_typology_ransomware_impa_140222.pdf

44. В большинстве случаев, когда от ПУВА поступают сообщения о подозрительных операциях, касающихся атак с использованием программ-вымогателей, такие сообщения направляются в связи с подозрениями в том, что виртуальные активы приобретались в целях оплаты выкупа. Полезными индикаторами, на которые полагаются ПУВА при направлении сообщений, являются следующие: заявления от потерпевших при обращении к ПУВА; виртуальные активы приобретаются известной компанией по реагированию на инциденты; исполняемые платежи прямо или косвенно связаны с адресом кошелька виртуальных активов, на который по результатам блокчейн-анализа, вероятно, может переводиться выкуп в результате совершения атак с использованием программ-вымогателей. Поскольку ПУВА выступают в качестве прямого посредника при осуществлении платежных операций с целью оплаты выкупа, они являются основными отправителями СПО о незаконных финансовых потоках, связанных с программами-вымогателями. Обращаем ваше внимание на документ *«Противодействие использованию программ-вымогателей: потенциальные признаки риска»,* в котором содержится перечень соответствующих признаков риска, которые могут использовать ПУВА в своей деятельности.

Вставка 11: Участие компании по управлению кризисными ситуациями

Управление Израиля по предотвращению отмывания денег и финансирования терроризма получило СПО от израильского провайдера услуг в сфере виртуальных активов. Это сообщение касалось компании по управлению кризисными ситуациями (по реагированию на инциденты), которая приобрела виртуальные активы (стоимость которых составляла десятки тысяч долларов на том момент) с намерением использовать их для выплаты выкупа от имени неназванной жертвы атаки с использованием программы-вымогателя. В СПО также было указано, что дополнительная сумма криптовалюты была отдельно приобретена у того же самого израильского ПУВА представителем субъекта, который предположительно стал жертвой атаки.

В результате финансового расследования, проведённого сотрудниками Управления, было установлено, что адрес кошелька, на который была переведена большая часть средств, связан с другими атаками с использованием программ-вымогателей, и на него ранее переводились средства с адресов других кошельков. Также было установлено, что аккумулированные в этом кошельке средства были в дальнейшем переведены на счёт провайдера услуг в сфере виртуальных активов, находящегося в юрисдикции, представляющей повышенный риск. Кроме того, выяснилось, что средства, отдельно приобретённые компанией, были переведены через несколько адресов кошельков, и большая часть из них была, в конечном итоге, смешана с другими средствами посредством миксера. Оперативный отчёт был направлен ПФР в соответствующие правоохранительные органы для проведения дальнейшего расследования.

Источник: Израиль

45. В отличие от ПУВА, банки и другие финансовые и платёжные учреждения могут стать свидетелями случаев, когда жертва кибератаки переводит фиатную валюту провайдеру услуг в сфере виртуальных активов или третьей стороне, действующей от имени жертвы, для выплаты выкупа. В таких случаях они могут направить соответствующее СПО. Однако такие финансовые и платёжные учреждения могут не знать деталей, касающихся выплаты выкупа или последующего отмывания денег, поскольку большинство таких платежей осуществляется в виртуальных активах, а не в фиатной валюте. Поэтому они могут обладать весьма ограниченной информацией об адресах кошельков виртуальных активов или источнике средств, что затрудняет для них использование инструментов блокчейн-анализа. Чтобы преодолеть эти затруднения, таким учреждения во многих случаях требуются косвенные признаки для выявления возможных случаев выплаты выкупа в результате совершения атак с использованием программ-вымогателей. Исходя из конкретных примеров дел, наиболее распространённые признаки такого рода включают в себя следующее: необычные переводы, осуществляемые в адрес ПУВА (особенно если компания, как правило, не использует виртуальные активы в своей коммерческой деятельности); приобретение виртуальных активов компаниями по кибербезопасности, страховыми компаниями и компаниями по реагированию на инциденты; заявления самих клиентов о том, что банковский перевод осуществляется в целях выплаты выкупа; а также информация из открытых источников, подтверждающая факт совершения атаки (например, пресс-релизы, сообщения об инцидентах и т.д.). Подробный перечень соответствующих признаков риска приведён в документе *«Противодействие использованию программ-вымогателей: потенциальные признаки риска».*

Сообщения от потерпевших

46. По причине поступления малого количества СПО, касающихся выплаты выкупа в результате совершения атак с использованием программ-вымогателей, сообщения о подозрительных операциях остаются недостаточным источником информации для выявления или понимания полного масштаба кибератак и связанного с ними ОД, а также для содействия проведению расследований. В этой связи сообщения от потерпевших также являются важным источником информации для выявления и расследования финансовых потоков, связанных с выплатами выкупа в результате совершения атак с использованием программ-вымогателей. Своевременное получение сообщений и заявлений от потерпевших является важным условием, позволяющим правоохранительным органам быстро принимать меры для отслеживания финансовых потоков, и повышает вероятность успешного преследования преступников.

47. Требования, касающиеся информирования об инцидентах, различаются в разных юрисдикциях и зависят от нормативно-правовой базы, имеющейся в каждой конкретной юрисдикции. В большинстве случаев информирование об инцидентах носит добровольный характер. Когда потерпевшие сообщают об атаках, они, как правило, обращаются в полицию, ведомства, занимающиеся вопросами кибербезопасности, специальные подразделения по реагированию на инциденты или в местные группы реагирования на компьютерные инциденты (ГРКИ).

48. Однако, похоже, что потерпевшие не всегда сообщают о такого рода инцидентах, поскольку имеется недостаточно сведений об атаках с использованием программ-вымогателей. Существуют разные причины, по которым потерпевшие могут отказаться сообщать об атаках с применением программ-вымогателей. Некоторые считают, что это может противоречить их собственным коммерческим интересам. К причинам также относятся опасения относительно возможного подрыва репутации, стремление как можно быстрее возобновить деятельность или страх мести со стороны преступников. По своему характеру атаки с использованием программ-вымогателей, как правило, направлены на получение незаконного доступа к персональным и чувствительным данным клиентов. Признание правоохранительным органам или общественности о наличии пробелов в системах безопасности или утечке данных может, по мнению многих потерпевших, негативно отразиться на их бизнесе и привести к подаче гражданских исков со стороны клиентов. Преступники также могут угрожать своим жертвам обнародовать похищенные данные, если последние обратятся в правоохранительные органы.

49. Кроме того, потерпевшие могут не иметь стимул для того, чтобы добровольно сообщить об инциденте после того, как они уже заплатили выкуп. В случаях, когда у потерпевших имеется полис страхования от киберрисков, у них может отсутствовать финансовая мотивация для сообщения об атаке, поскольку страховая компания может покрыть расходы, связанные с выплатой выкупа. В некоторых юрисдикциях потерпевшие могут не сообщить об атаке после выплаты выкупа из-за страха того, что они нарушили местное законодательство (например, перевели платёж субъекту, находящемуся под санкциями), или из-за опасения того, что их сочтут сообщниками преступных группировок.

50. Юрисдикции используют ряд методов для стимулирования потерпевших сообщать об атаках. Например, власти некоторых юрисдикций реализуют политику или проводят мероприятия, направленные на повышение информированности общественности об атаках с использованием программ-вымогателей и призывают сообщать о таких атаках. Такая политика и мероприятия также охватывают

частный сектор для демонстрации того, как власти могут помочь в минимизации ущерба от атак с использованием программ-вымогателей. Это включает в себя возврат активов потерпевшим и предоставление ключей дешифрования для восстановления данных, когда это возможно.

Вставка 12: Вебсайт «No More Ransom»[1]

Вебсайт «No More Ransom» («Больше никакого выкупа») является проектом, реализуемым Национальным подразделением по борьбе с преступлениями в сфере высоких технологий Полиции Нидерландов, Европейским центром по борьбе с киберпреступностью Европола и двумя индустриальными партнёрами. Целью проекта является оказание помощи жертвам атак с использованием программ-вымогателей снова получить доступ к своим зашифрованным данным без выплаты выкупа преступникам. На этом вебсайте имеется хранилище ключей и приложений, позволяющие расшифровать данные, заблокированные программами-вымогателями разных типов. Это помогает жертвам восстановить доступ к своим зашифрованным данным или заблокированным системам без необходимости платить выкуп.

В этом проекте участвует множество партнёров из государственного и частного сектора из разных юрисдикций, в том числе правоохранительные органы и компании, работающие в сфере IT-безопасности. Проект также ставит перед собой цель просвещать пользователей в вопросах, связанных с работой троянцев-вымогателей и контрмерами, которые можно предпринять для эффективного предотвращения заражения. Вебсайт также призывает потерпевших не выплачивать выкуп и содержит ссылки для направления жертв атак на соответствующие вебсайты их страны для подачи заявлений об инцидентах.

Источник: Вебсайт «No More Ransom»

[1] Дополнительную информацию можно найти по адресу: www.nomoreransom.org/en/index.html

51. В целях снятия опасений, касающихся рисков для репутации в связи с сообщением потерпевшими об атаках, некоторые юрисдикции пытаются создать безопасные условия для компаний, ставших жертвами атак с использованием программ-вымогателей, с тем, чтобы такие жертвы добровольно сообщали об атаках, не боясь репутационного ущерба. Это включает, например, регулярное взаимодействие и участие в бизнес конференциях. Ещё одним примером передовой практики является создание веб-порталов по типу «единое окно», через которые потерпевшие могут сообщать об инцидентах. Кроме того, такие порталы могут одновременно служить информационными центрами, в которых можно получить консультации экспертов и советы по устранению последствий. Хотя эти усилия часто сосредоточены на выявлении самих атак с использованием программ-вымогателей, информация, полученная из сообщений потерпевших, является важной и ценной для проведения финансовых расследований, в том числе для отслеживания финансовых потоков и отмывания денег, связанных с атаками.

Вставка 13: Канадский центр кибербезопасности

Канадский центр кибербезопасности (Киберцентр), открывшийся в 2018 году, является одной из ключевых инициатив в рамках канадской Национальной стратегии в сфере кибербезопасности. Киберцентр представляет собой единый источник, предоставляющий экспертные консультации, руководящие указания, услуги и поддержку в сфере кибербезопасности для правительства, владельцев и операторов объектов критической инфраструктуры, предприятий частного сектора и граждан Канады. Он предлагает свои ресурсы физическим и юридическим лицам, в том числе руководящие указания относительно того, как предотвратить и оправиться после атак с использованием программ-вымогателей, а также публикует отчёты о характере угроз, связанных с применением программ-вымогателей. Киберцентр собирает сообщения об атаках/инцидентах от канадских и зарубежных государственных органов и представителей частного сектора. Такие сообщения можно направлять через Интернет, по электронной почте или по телефону. Центр также призывает обращаться в полицию в случаях, когда киберинцидент представляет непосредственную угрозу для жизни или носит криминальный характер.

Источник: Канада

52. В некоторых юрисдикциях используется подход, предусматривающий определение конкретных секторов или случаев, когда потерпевшие должны в обязательном порядке сообщать об инцидентах, например, в случае атак на критические объекты инфраструктуры (такие как энергетические объекты, объекты связи, учреждения здравоохранения и т.д.) или в случае утечки данных. Во многих юрисдикциях эти секторы могут также включать сегменты финансового сектора, на которые распространяются требования ПОД/ФТ (банки) и в которых регулируемые субъекты обязаны сообщать о существенных инцидентах компетентным органам, таким как надзорные органы, в рамках действующего регулятивного режима. Нормативно-правовые акты, касающиеся защиты данных, также могут содержать положения, стимулирующие или обязывающие сообщать о случаях несанкционированного доступа или утечки данных, в том числе персональных данных, что может способствовать своевременному обнаружению атак с использованием программ-вымогателей. Для более эффективного выявления незаконных финансовых потоков полезно собирать и фиксировать соответствующую финансовую информацию, содержащуюся в таких сообщениях (например, адреса кошельков, виды виртуальных активов).

Другие источники информации для выявления атак с использованием программ-вымогателей

53. Как указано выше, обмен информацией и сотрудничество с заинтересованными сторонами помимо участников секторов ФУ, УНФПП и ПУВА (например, с провайдерами Интернет-услуг и организациями, работающими в сфере кибербезопасности) может оказаться полезным источником информации. Однако на субъекты этих секторов могут не распространяться регулятивные требования в сфере ПОД/ФТ, в том числе требования о направлении сообщений о подозрительных операциях. В некоторых случаях может даже возникнуть конфликт интересов (например, когда компании по кибербезопасности действуют от имени своих клиентов), что может помешать направлению сообщений в инициативном порядке. В таких обстоятельствах информацию можно получить, используя неофициальные механизмы, такие как государственно-частные партнёрства с участием этих субъектов, либо путём прямого взаимодействия с ними.

Вставка 14: Сотрудничество с компанией по кибербезопасности

Потерпевшая компания заключила договор с компанией по кибербезопасности после того, как она подверглась атаке со стороны группировки преступников, совершающих атаки с использованием программ-вымогателей. Преступники потребовали выплатить выкуп либо в биткоинах, либо в монеро. В конечном итоге, потерпевшая компания выплатила выкуп этой преступной группировке через компанию по кибербезопасности.

После выплаты выкупа компания по кибербезопасности сообщила об этом инциденте в правоохранительные органы, что позволило компетентным органам отследить незаконные финансовые потоки. Управление часто взаимодействует и сотрудничает с компаниями по кибербезопасности. Это взаимодействие построено таким образом, чтобы минимизировать вмешательство в работу компаний по кибербезопасности, когда они действуют в интересах своих клиентов, но при этом обеспечивается предоставление IP-адресов и адресов кошельков криптоактивов для проведения уголовных расследований.

В рассматриваемом случае сотрудники правоохранительных органов обнаружили, что злоумышленники использовали методы для повышения степени анонимности. В частности, они использовали «миксеры», а также большое количество адресов автономных кошельков. На момент проведения расследования значительная часть активов находилась в автономных кошельках, вследствие чего отследить их дальнейшее перемещение было невозможно. По имеющимся сведениям, значительная часть средств была в дальнейшем переведена через двух ПУВА, находящихся в зарубежных юрисдикциях.

Источник: Швейцария

54. Компетентные органы также выявляют платежи и атаки с использованием программ-вымогателей путём проведения независимых финансовых расследований и использования инструментов блокчейн-анализа в отношении кошельков, о которых известно, что они связаны с получением выкупа в результате совершения таких атак. Сюда также относится осуществление мониторинга известных атак и блогов, использование результатов анализа информации из открытых источников, предоставляемых компаниями, занимающимися блокчейн-анализом, а также инициативные контакты с потенциальными жертвами после проведения анализа.

55. Такая работа может дать дополнительные зацепки в отношении атак с использованием программ-вымогателей, которые были осуществлены в прошлом. В результате создается представление о масштабе атаки, приписываемой хакеру-вымогателю. Кроме того, такая работа способствует выявлению тенденций, типологий и инфраструктуры, используемой преступниками для отмывания, получения и дальнейшего использования своих незаконных доходов.

Вставка 15: Анализ информации из открытых источников для установления преступников, предоставляющих программы-вымогатели как услугу

Подразделение финансовой разведки Турции получило от провайдера услуг в сфере виртуальных активов СПО, касавшееся адреса кошелька виртуальных активов, связанного с человеком, указанным в сообщении под «Именем 1». В результате поиска по этому имени в Интернете был обнаружен вебсайт, зарегистрированный на это имя. В результате дальнейшего расследования выяснилось, что на этом вебсайте осуществлялась деятельность, связанная с сетью «Даркнет», а сам вебсайт служил в качестве посредника при продаже программ-вымогателей и другого вредоносного программного обеспечения.

В ходе дальнейшего анализа информации, найденной в открытых источниках, было установлено следующее:

- Человек, участвовавший в операции, указанной в СПО, использовал другой псевдоним («Имя 2»). В результате было установлено настоящее имя этого человека («Человек X»). Личностью этого человека ранее интересовался Отдел по борьбе с киберпреступлениями Управления полиции.
- Подозреваемый («Человек X») предлагал продукты и услуги, такие как несанкционированный доступ, доступ к конфиденциальной информации, поддельные идентификационные и учётные данные, взлом аккаунтов в социальных сетях, продажа вредоносных ссылок и фишинговые страницы.
- Оплата за эти незаконные продукты/услуги осуществлялась биткоинами и другими виртуальными активами.

После этого сотрудники турецкого подразделения финансовой разведки запросили у ПУВА дополнительную информацию о фигуранте СПО, в частности сведения об адресах кошельков виртуальных активов, информацию о финансовых операциях (как в виртуальных активах, так и в фиатной валюте) и другие персональные данные. Подготовлен аналитический отчёт, который направлен в Управление по борьбе с киберпреступлениями Национальной полиции Турции. В этом отчёте изложены подозрения о том, что человек, фигурирующий в СПО, являлся посредником при продаже программ-вымогателей и другого вредоносного программного обеспечения. Расследование по этому делу продолжается.

Источник: Турция

56. Юрисдикции также могут получать предупреждения об атаках с использованием программ-вымогателей и выплате выкупа благодаря информации, предоставляемой другими юрисдикциями. Международное сотрудничество, оказание взаимной правовой помощи и неофициальный обмен информацией с зарубежными юрисдикциями – всё это может стать источником информации о средствах, которые преступники пытаются скрыть путём их перевода через местные криптобиржи, имеющие отношение к атакам, совершённым за рубежом, и/или к жертвам таких атак, находящимся за рубежом.

Предлагаемые меры

- Юрисдикциям следует оказывать содействие регулируемым субъектам в выявлении случаев осуществления атак с использованием программ-вымогателей и связанного с этим отмывания денег, а также в направлении сообщений о подозрительных операциях. Для этого следует, в том числе, информировать соответствующих подотчётных субъектов о тенденциях, настораживающих признаках (аналогичных тем, которые приведены в документе *«Противодействие использованию программ-вымогателей: потенциальные признаки риска»*) и предоставлять руководства по выявлению таких случаев.
- Юрисдикциям следует стимулировать и поощрять потерпевших добровольно сообщать о случаях таких атак, например, путём повышения информированности о доступной поддержке и ресурсах или путём создания защищённых и безопасных каналов связи для сообщения о таких случаях.
- Юрисдикциям следует рассмотреть возможность установления каналов связи с нетрадиционными субъектами, на которых могут не распространяться требования в сфере ПОД/ФТ (компании по кибербезопасности и компании по реагированию на инциденты) с целью расширения спектра источников информации для выявления случаев атак с использованием программ-вымогателей.

Стратегии проведения финансовых расследований

57. Целью почти всех атак с использованием программ-вымогателей является получение незаконных доходов. Большинство юрисдикций понимает и признаёт, что расследования атак с применением программ-вымогателей включают в себя существенный финансовый компонент. Примеры дел показывают, что отслеживание виртуальных активов является одним из ключевых элементов расследований атак с использованием программ-вымогателей. В юрисдикциях, которые сообщили о том, что они проводили расследования случаев атак с применением программ-вымогателей, как правило, проводятся параллельные финансовые расследования для отслеживания средств, выплаченных в качестве выкупа.

58. Очевидно, что в мире накоплено мало опыта расследований случаев отмывания доходов от атак с использованием программ-вымогателей. В очень небольшом количестве юрисдикций имели место случаи предъявления обвинений в отмывании доходов в рамках дел, касающихся совершения атак с применением программ-вымогателей. Это частично может быть обусловлено трудностями в выявлении и информировании о таких случаях, как отмечено в разделе 5 выше.

59. В данном разделе рассматриваются сложности и передовая практика проведения успешных финансовых расследований атак с использованием программ-вымогателей и связанного с этим отмывания денег, включая (i) работу с потерпевшими для получения информации; (ii) использование следственных методов и механизмов; и (iii) возврат активов.

Оперативное реагирование и работа с потерпевшими для получения информации

60. Принимая во внимание характер киберпреступлений, таких как атаки с использованием программ-вымогателей, успешные результаты расследований, проводимых правоохранительными органами, напрямую зависят от их способности действовать оперативно и осуществлять сбор ключевой информации, касающейся самой атаки с применением программ-вымогателей и выплаты потерпевшими выкупа. Такая информация включает следующее: адреса кошельков виртуальных активов; общая сумма выплаченного выкупа и вид виртуальных активов, использовавшихся для выплаты выкупа; даты осуществления операций; виды использовавшихся услуг; идентификационные данные потерпевшего; переговоры между потерпевшим и преступниками; а также сведения о любой третьей стороне, участвовавшей в выплате выкупа.

61. Во многих случаях сбор такой информации зависит от сотрудничества со стороны потерпевших или третьих сторон, участвовавших в реагировании на инцидент и/или в процедуре выплаты выкупа. Однако, как говорилось ранее, потерпевшие могут не захотеть сообщать об инциденте/атаке правоохранительным органам (см. подраздел 5.3 выше). Потерпевшие также могут не идти на сотрудничество со следствием, посчитав, что их интересы противоречат интересам правоохранительных органов – потерпевшие часто хотят возобновить свою коммерческую деятельность как можно быстрее и предпочитают выплатить выкуп преступникам. Они также могут бояться возмездия со стороны преступников, если обратятся в правоохранительные органы. С другой стороны, правоохранительным органам может потребоваться определённое время для сбора данных криминалистической экспертизы и улик, а также для подготовки контролируемых операций и осуществления других следственных мероприятий, что может задержать возобновление деятельности потерпевших.

62. Несвоевременное или неполное информирование правоохранительных органов об атаках, а также нежелание потерпевших сотрудничать со следствием может снизить качество доступной информации необходимой для успешного производства и расследования по делу. Отсутствие чёткого плана действий потерпевших после совершения атаки и/или выплаты выкупа может привести к невозможности использования имеющихся доказательств по причине того, что соответствующие данные не будут ими сохранены. Примеры передовой практики, приведённые в подразделе 5.3, например, проведение информационно-разъяснительной работы среди населения и другие меры, направленные на стимулирование потерпевших сотрудничать со следствием, являются важным средством для преодоления этих затруднений.

63. Некоторые юрисдикции также подчеркнули важность обмена информацией между следователями, расследующими киберпреступления (т.е. предикатные преступления), и следователями, занимающимися расследованием отмывания денег. В ходе сбора улик в рамках расследования предикатного преступления, касающегося совершения атаки с использованием программ-вымогателей, сотрудники правоохранительных органов неизбежно получат информацию, которая будет являться актуальной для расследования ОД. Такая информация позволит правоохранительным органам выявить связи между различными группировками и сообщниками преступников, а также получить зацепки и ориентиры для проведения более широкого финансового расследования. Более подробная информация о возможностях эффективного сотрудничества между разными национальными правоохранительными органами приведена в подразделе 8.2.

Вставка 16: Источники улик для финансовых расследований, получаемые в ходе расследования предикатных преступлений

Улики и данные криминалистической экспертизы: Примеры этого включают следующее: векторы атаки (т.е. как преступники осуществили несанкционированный доступ); информация о типе/разновидности использовавшихся программ-вымогателей; IP-адреса; имена или псевдонимы (ники), использовавшиеся преступниками; и устройства, применённые хакерами. Такая информация может быть получена непосредственно от потерпевших, от провайдеров Интернет-услуг, от компаний по кибербезопасности и реагированию на инциденты; а также путем использования криминалистических технологий.

Прямые доказательства от представителей частного сектора: Это относится к соответствующим компаниям частного сектора, в том числе к владельцам технологий или инфраструктуры, которые были незаконным образом использованы для осуществления атаки с применением программ-вымогателей. Следователи могут получить информацию о подписчиках от компаний-владельцев социальных сетей и провайдеров услуг электронной почты, у которых злоумышленник может иметь аккаунты для связи со своей жертвой.

Информация из открытых источников: Анализ информации из открытых источников, включая социальные сети, Интернет-форумы и рынки в сети «Даркнет», а также анализ переговоров, сообщений и корреспонденции хакеров-вымогателей может помочь в установлении потенциальных злоумышленников.

Механизмы и методы расследований

Актуальность традиционных следственных методов

64. Технологии, которые используют преступники для сокрытия своего местонахождения, личности и финансовых потоков, могут затруднить проведение расследований. В частности, к таким трудностям относится использование злоумышленниками виртуальных частных сетей (VPN), «луковичного (многослойного) маршрутизатора»[35] или зашифрованной электронной почты, что позволяет повысить степень анонимности и безопасности, а также обеспечивает возможность осуществления анонимной деятельности по мере того, как трафик движется по сети. Эти трудности могут усугубляться вследствие скорости развития таких технологий.

65. Рекомендация 31 ФАТФ закладывает основы для предоставления правоохранительным органам необходимых полномочий для проведения эффективных финансовых расследований. Традиционные следственные методы продолжают оставаться актуальными для преодоления указанных трудностей, позволяя осуществлять сбор и анализ ключевой информации, касающейся финансовых потоков, связанных с атаками с использованием программ-вымогателей. Эти методы включают в себя наблюдение, перехват переговоров и корреспонденции, а также проведение операций под прикрытием. Однако эти традиционные следственные методы нуждаются в адаптации при проведении финансовых расследований

[35] Луковичный или многослойный маршрутизатор (или «TOR») – это свободное и открытое программное обеспечение, позволяющее пользователям анонимно пользоваться Интернетом.

в отношении виртуальных активов. Примерами того, что нужно сделать для достижения успешных результатов в ходе расследований, являются:

- *Наблюдение:* Определение типов электронных устройств, используемых подозреваемым лицом; установление любых используемых кошельков виртуальных активов, а также предпочитаемых способов электронной связи.
- *Перехват средств связи и проведение операций под прикрытием:* Получение сведений о деталях деятельности подозреваемого лица и методах работы преступной организации; установление лиц, связанных с подозреваемым, а также получение информации о финансах и активах; проникновение в преступные сообщества (например, на форумы в сети «Даркнет») для выяснения настоящей личности (деанонимизации) конечных исполнителей и бенефициаров.
- *Постановление о предоставлении информации:* Получение информации у ПУВА или у других финансовых учреждений, участвовавших в процессе выплаты выкупа.

66. Для более эффективного применения этих инструментов в ходе финансовых расследований могут использоваться сведения, полученные в результате СПО или заявлений потерпевших (см. раздел 5 выше). Правоохранительные органы могут определять соответствующие финансовые учреждения и ПУВА путём анализа СПО и блокчейна (см. подраздел 6.2.2 ниже) для получения от них необходимых доказательств с помощью постановлений о предоставлении информации и документов. Провайдеры услуг в сфере виртуальных активов могут предоставить полезные идентификационные данные для финансовых расследований, которые помогут получить базовую информацию о клиентах, информацию о бенефициарных владельцах, а также информацию об операциях (например, идентификационные данные и другую информацию о пользователях, IP-адреса, сведения о кредитных картах или банковских счетах и т.д.).

67. Однако, как отмечено в разделе 3 выше, некоторые преступные сети также связаны с представляющими высокий риск юрисдикциями, в которых не установлены или установлены недостаточные требования в сфере ПОД/ФТ для провайдеров услуг в сфере виртуальных активов или в которых ПУВА часто не выполняют такие требования. В этой связи следователи могут столкнуться с трудностями, если средства были переведены через таких ПУВА или хранятся у таких ПУВА. В этих случаях такие провайдеры услуг в сфере виртуальных активов могут вообще не осуществлять сбор соответствующей информации или не отвечать на запросы правоохранительных органов.

68. Следователи сталкиваются с аналогичными трудностями в случаях, когда преступники используют анонимные кошельки. Это позволяет пользователям контролировать виртуальные активы без участия ПУВА и таким образом создаёт трудности для выявления и предупреждения деятельности, связанной с отмыванием денег. Отсутствие связи со сторонним субъектом (т.е. субъектом, подлежащим регистрации/лицензированию в соответствии со Стандартами ФАТФ) может ограничить возможности компетентных органов по установлению личности владельца кошелька, поскольку отсутствует сторонний субъект, у которого можно было бы запросить соответствующую информацию.

69. Недостаточная реализация «дорожного правила» (как того требуют Стандарты ФАТФ) со стороны провайдеров услуг в сфере виртуальных активов даёт киберпреступникам возможность уклоняться от идентификации и затрудняет проведение

расследований. В соответствии с «дорожным правилом» ПУВА и другие финансовые учреждения, осуществляющие операции с виртуальными активами, обязаны предоставлять информацию об отправителях и получателях по всей цепочке переводов. Это повышает прозрачность операций, не позволяя преступникам осуществлять их в незаконных целях, а также служит источником информации, которую правоохранительные органы могут использовать для установления личности участников конкретной операции. Однако в отчёте ФАТФ от 2022 года отмечено, что только одна треть юрисдикций сообщила о принятии законов для введения «дорожного правила» в отношении ПУВА и ещё меньшее число юрисдикций обеспечивает выполнение этих требований на практике[36]. Таким образом, отсутствие единообразного регулирования снижает объём информации, которую правоохранительные органы могут получить от ПУВА, располагающихся в юрисдикциях, в которых не установлены обязательства, касающиеся «дорожного правила». Это также означает, что, когда ПУВА, находящиеся в юрисдикциях, выполняющих это требование, осуществляют операции с ПУВА, находящимися в юрисдикциях, не выполняющих это требование, они вряд ли смогут получить такую информацию, что, в свою очередь, ограничивает объём информации доступной для следователей даже в тех юрисдикциях, которые ввели «дорожной правило».

Вставка 17: Применение традиционных следственных методов и методов финансовых расследований в отношении группировки преступников, совершающих атаки с использованием программ-вымогателей

Итальянская компания, ставшая жертвой преступников, совершающих атаки с использованием программ-вымогателей, обратилась с заявлением в полицию после того, как заплатила выкуп в биткоинах и успешно разблокировала свои данные, которые были заражены в результате атаки с использованием программы-вымогателя. Платёж был осуществлён через провайдера услуг в сфере виртуальных активов, который был указан преступниками в требовании о выплате выкупа.

В ходе полицейского расследования в отношении данного ПУВА было установлено, что он официально зарегистрирован в Италии. В дальнейшем была установлена личность этого итальянского субъекта, и выяснилось, что ранее он неоднократно содействовал переводам биткоинов, связанных с выплатой выкупа в результате атак с применением программ-вымогателей. Полиция провела обыск в квартире этого человека и изъяла платёжные карты, мобильные телефоны и другие устройства, включая жёсткие диски, USB-драйверы и планшеты. В результате прослушивания телефонных разговоров и анализа сообщений, передаваемых с помощью мобильных телефонов, была установлена группа других итальянских субъектов («Группа»), которые исполняли аналогичные функции в обеспечении переводов биткоинов, выплачиваемых в качестве выкупа в результате атак с использованием программ-вымогателей. В ходе финансового расследования выяснилось, что фиатные деньги, отправляемые жертвами атак, переводились членами указанной группы на счета в зарубежных банках, принадлежащие иностранным ПУВА, в том числе находящимся в представляющих высокий риск юрисдикциях.

[36] ФАТФ (июнь 2022 г.), Обновлённый целевой обзор выполнения Рекомендаций ФАТФ, касающихся виртуальных активов и провайдеров услуг в сфере виртуальных активов. В этот обзор включены только те страны, отчёты о взаимной оценке/отчёты о прогрессе которых были опубликованы в период с июня 2021 года по май 2022 года.

На основании результатов финансовых расследований и криминалистической экспертизы телефонов и других устройств компетентные органы пришли к выводу, что эта группа рассылала вредоносные программы жертвам и требовала от них выплаты выкупа, размер которого составлял несколько сотен евро в случае каждой атаки. Членам этой группы были предъявлены обвинения в вымогательстве и последующем отмывании незаконных доходов, которые составили в общей сложности порядка 300 000 евро, заплаченных разными потерпевшими. Расследование в настоящее время продолжается.

Источник: Италия

Специальные следственные методы применительно к виртуальным активам

70. Помимо традиционных следственных методов, при проведении финансовых расследований по делам, связанным с атаками с применением программ-вымогателей, правоохранительным органам следует использовать специальные методы, учитывающие специфику виртуальных активов. Большинство виртуальных активов функционирует на основе технологии публичного блокчейна. Публичный блокчейн представляет собой доступную для просмотра базу данных, через которую можно отслеживать анонимную информацию, связанную с транзакциями с виртуальными активами, с помощью инструментов блокчейн-анализа доступных из открытых источников или по подписке (см. раздел 7 ниже). Анализ блокчейна, наряду с традиционными следственными методами, может позволить следователям получить информацию необходимую для установления личности преступников, действующих в Интернете, и их сообщников, а также отследить движение незаконных доходов.

71. Для отслеживания преступных доходов с использованием инструментов блокчейн-анализа, как правило, необходимо установить адрес исходного кошелька. Поэтому нахождение и сбор информации о выплате выкупа является чрезвычайно важным первым шагом в расследовании. После получения адреса исходного кошелька следователи могут установить, помимо всего прочего, входящие и исходящие платежи, отправленные/полученные на адрес этого кошелька. Однако доступная информация может зависеть от конкретных используемых услуг. Хотя в публичном блокчейне содержится полезная информация для проведения финансовых расследований, некоторые транзакции с виртуальными активами могут осуществляться вне блокчейна. Кроме того, в некоторых инструментах блокчейн-анализа используются алгоритмы кластеризации и другие методы для группирования адресов кошельков или операций, которые могут быть связаны с преступной деятельностью, такой как атаки с применением программ-вымогателей.

72. Информация, полученная по результатам анализа блокчейна, может стать основанием для применения традиционных следственных методов. Например, анализ блокчейна может помочь установить ПУВА, обслуживающий кошелёк, на адрес которого приходили платежи, отправленные для/или от преступников, совершающих атаки с использованием программ-вымогателей. А это может побудить правоохранительные органы использовать принудительные меры для запроса у этого ПУВА информации, касающейся адреса кошелька.

Вставка 18: Расследования в отношении известных кошельков, использовавшихся при совершении атак с использованием программ-вымогателей, которые привели к установлению дополнительных ранее неизвестных потерпевших

В ходе анализа и оценки угроз, исходящих от использования технологий блокчейна, был проанализирован адрес биткойн кошелька, на который, по имеющимся данным, было переведено 20 биткоинов в период с 12 мая 2017 года по 27 мая 2021 года. Также установлено, что этот адрес биткоин кошелька напрямую связан с вредоносным программным обеспечением, которое заразило компьютерные системы ряда коммерческих предприятий и правительственных учреждений в ЮАР. По результатам анализа выяснилось, что в феврале 2018 года с ещё одного адреса местного биткойн кошелька, принадлежащего южноафриканскому ПУВА, было переведено 0,06 биткоинов на вышеуказанный адрес кошелька, в отношении которого велось расследование.

После получения от ПУВА информации о подписчиках был установлен ещё один потерпевший, который признался, что понёс финансовый ущерб. Он предпочёл не сообщать об этом инциденте местным следственным органам, так как боялся общественного резонанса в связи с тем, что он не обеспечил надлежащую защиту и сохранность клиентских данных. Материалы этого дела были переданы южноафриканским ПФР местным следственным органам. Однако, ввиду того, что установленный потерпевший не захотел предъявлять никаких уголовных обвинений, дело было закрыто местными правоохранительными органами.

Источник: ЮАР

73. Методы, повышающие степень анонимности, которые используются преступниками в процессе отмывания своих преступных доходов (о которых говорилось в разделе 3 выше), также затрудняют для правоохранительных органов задачу по отслеживанию операций с помощью инструментов блокчейн-анализа. Следует отметить, что ряд компаний, специализирующихся на анализе блокчейна, разработали технологии для нивелирования некоторых из этих мер. Использование злоумышленниками «партнёрских» моделей, моделей «программа-вымогатель как услуга», а также привлечение «денежных мулов» усложняет проведение финансовых расследований, связанных с атаками с применением программ-вымогателей. Поскольку не всегда возможно отследить цепочку платежей вплоть до потерпевшего, возникают трудности с установлением адресов, использовавшихся для исходной оплаты в виртуальных активах. Адреса, как правило, являются зацепкой для проведения блокчейн-анализа.

74. Помимо использования инструментов блокчейн-анализа для отслеживания платежей выкупа в результате атак с применением программ-вымогателей и последующего отмывания денег, следователям также следует выявлять предыдущие операции, связанные с преступными группировками. Эта дополнительная мера позволяет правоохранительным органам выявлять возможные тенденции и типологии и/или дополнительную преступную деятельность.

75. В качестве передовой практики можно отметить, что правоохранительные органы ряда юрисдикций создали базы данных, в которых содержится ключевая

информация о «денежных мулах» и адресах кошельков, фигурировавших в делах, связанных с атаками с использованием программ-вымогателей. В таких базах данных, как правило, содержится информация об инцидентах, идентификационные данные «денежных мулов», сведения о размере нанесённого ущерба и имеющиеся данные о преступниках (например, номера счетов, адреса кошельков, имена пользователей). Такие базы данных помогают выявлять и отслеживать выплаты выкупа в результате атак, а также случаи последующего отмывания денег, так как в них накоплены данные, позволяющие проводить сравнение и находить совпадения с предыдущими следственными уликами (включая информацию о платежах) при расследовании текущих и будущих инцидентов. Кроме того, это позволяет правоохранительным органам получить представление о более широких сетях, занимающихся отмыванием денег, в которые могут быть вовлечены различные регулируемые субъекты и представители разных секторов.

Возврат активов

76. Помимо наращивания возможностей по выявлению преступлений и проведению финансовых расследований, правоохранительные органы также должны обладать закреплёнными в законодательстве полномочиями и возможностями для наложения ареста и конфискации виртуальных активов. Операции с виртуальными активами проводятся почти мгновенно. Это означает, что как только правоохранительные органы узнают об атаке с использованием программ-вымогателей и выплате выкупа, они должны быть в состоянии быстро отследить оплату выкупа и иметь полномочия для оперативного (в идеале, в течение нескольких часов) ареста виртуальных активов с целью недопущения их распространения. В соответствии с Рекомендацией 4 ФАТФ многие юрисдикции должны обладать такими полномочиями, которые могут различаться по своей форме.

77. Несколько юрисдикций также отметили полезность использования альтернативных инструментов для перехвата незаконных доходов, например, полномочий ПФР по приостановке операций, при проведении расследований в отношении потенциальных преступных активов, указанных в СПО. Для того чтобы идти в ногу с динамично развивающейся сферой виртуальных активов, возможно, также потребуется рассмотреть необходимость пересмотра и обновления действующего законодательства, политики, нормативных актов и процедур, касающихся изъятия и конфискации активов.

Вставка 19: Дело компании «Colonial Pipeline»

В июне 2021 года Министерство юстиции США сообщило об аресте 63,7 биткоинов стоимостью примерно 2,3 миллионов долларов. По заявлению Минюста, эти средства являлись доходами, выплаченными в качестве выкупа группировке «DarkSide», которая совершила атаку с применением программы-вымогателя на компанию «Colonial Pipeline», что привело к временной остановке работы объекта критической инфраструктуры. На биткоины был наложен арест в тот же день, когда судья штата Калифорния выдал ордер на арест активов.

Примерно 7 мая 2021 года компания «Colonial Pipeline» подверглась резонансной атаке с использованием программы-вымогателя, в результате которой ей пришлось временно остановить работу нескольких своих инфраструктурных объектов. Представители компании сообщили Федеральному бюро расследований, что её компьютерная сеть была взломана хакерской группировкой под названием «DarkSide», после чего компания получила требование и заплатила выкуп в размере порядка 75 биткоинов. Как указано в дополнительном аффидевите (т.е. заверенных письменных показаниях в поддержку устных показаний), правоохранительные органы провели анализ публичного реестра биткоинов. По результатам этого анализа они смогли отследить неоднократные переводы биткоинов и установить, что примерно 63,7 биткоинов, являвшихся доходами, полученными в результате выплаты жертвой выкупа, были переведены на конкретные адреса. Было доказано, что эти доходы в биткоинах имели отношение к несанкционированному проникновению в компьютерную сеть и являются легализованным имуществом, полученным преступным путём, и поэтому на них может быть наложен арест в соответствии с положениями уголовного и гражданского законодательства об аресте и конфискации.

Источник: США

Предлагаемые меры

- Компетентным органам следует использовать и адаптировать, при необходимости, традиционные правоохранительные методы, а также конкретные технологии применительно к виртуальным активам для проведения расследований случаев отмывания доходов от атак с использованием программ-вымогателей.
- Юрисдикциям следует обеспечить, чтобы сотрудники правоохранительных органов постоянно обладали необходимыми возможностями и полномочиями для оперативного и эффективного наложения ареста и конфискации активов, особенно виртуальных.

Знания и навыки

78. Как отмечено в подразделе 6.2, хотя традиционные методы правоохранительных органов по-прежнему остаются чрезвычайно важными для расследования случаев отмывания доходов от атак с использованием программ вымогателей, для успешных расследований и судебных преследований за отмывание доходов, полученных в результате таких атак, а также для возврата виртуальных активов требуются специальные технические знания. Это включает технические и юридические знания в сфере виртуальных активов.

79. Помимо этого, в состав следственных групп, занимающихся делами, связанными с отмыванием денег или возвратом активов в результате атак с применением программ-вымогателей, следует включать сотрудников, обладающих техническими навыками и знаниями в сфере кибербезопасности, компьютерной криминалистики, интернет-аналитики и открытых платформ. При этом акцент должен быть сделан на интернет-разведке с целью сбора финансовой информа-

ции, касающейся операций с виртуальными активами в открытых сетях, в том числе для сбора сведений, которые могут быть получены путём анализа блокчейна, сканирования вебсайтов, социальных сетей, интернет-форумов, сети «Даркнет» и «Дарк-маркетов», а также путём отслеживания сообщений о незаконной деятельности в Интернете.

80. При расследовании дел, связанных с виртуальными активами, сотрудникам компетентных органов могут потребоваться новые знания и навыки для сбора и толкования данных. В частности, сотрудникам правоохранительных органов необходимо ознакомиться с возможностями блокчейн-аналитики и мониторинга, например, научиться использовать инструменты анализа блокчейна, включая общедоступное программное обеспечение для просмотра открытого блокчейна, и применять аналитические методы для отслеживания средств. Следует также отметить, что разные инструменты предоставляют различные взаимодополняющие возможности (анализ различных видов виртуальных активов, возможность для анализа схем «прыжков между сетями», сбор оперативных данных из открытых источников и т.д.).

81. Для разработки таких различных инструментов и их использования при проведении расследований требуется специальное обучение и технические знания. Некоторые юрисдикции нашли пути подключения соответствующих специалистов к конкретным расследованиям (см. подраздел 8.2). Однако привлечение требуемых специалистов может оказаться весьма затратным делом, и некоторые юрисдикции могут не иметь ресурсов для развития таких навыков, что может снизить возможности компетентных органов проводить расследования и осуществлять судебные преследования за отмывание доходов, полученных в результате атак с использованием программ-вымогателей.

82. Если собственные знания отсутствуют или являются недостаточными, юрисдикции могут рассмотреть возможность использования инструментов, создаваемых компаниями частного сектора. Такие инструменты, разработанные третьими сторонами, могут помочь компетентным органам выявлять и отслеживать транзакции с виртуальными активами, осуществляемые на всех основных и на большинстве второстепенных блокчейнах. В настоящее время эти инструменты поддерживают функционирование сотен видов токенов, и в них применяются такие технологии как алгоритмы кластеризации, веб-скрейпинг (технология получения веб-данных путём их извлечения со страниц веб-ресурсов), мониторинг баз данных о мошеннических схемах, которые позволяют следователям привязывать широкой спектр транзакций к реальным физическим и юридическим лицам. Эти инструменты создают графы транзакций и позволяют проводить сетевой анализ, что даёт компетентным ведомствам возможность понять и затем представить сложные связи присяжным и судьям в ходе последующих судебных процессов и действий по возврату активов. Эти инструменты также могут помочь компетентным органам выявлять ПУВА, которые могли быть использованы для отмывания или обмена незаконных доходов на фиатную валюту и которые могут обладать актуальной информацией для оказания содействия следствию.

83. Что касается возврата активов, то для ареста и управления виртуальными активами также требуются дополнительные технические и юридические знания. Компетентные органы должны быть готовы принять соответствующие меры и реализовать процедуры для обеспечения надлежащего ареста и хранения виртуальных активов. Примером передовой практики является создание специальных механизмов для наложения ареста, конфискации и утилизации вир-

туальных активов. Это может включать в себя тщательное и надлежащее планирование ареста, использование сид-фраз (мнемонических фраз)[37], «холодное» хранение арестованных виртуальных активов (т.е. их хранение в бессерверных оффлайн кошельках), а также регулирование вопросов, касающихся цепочки ответственности.

Предлагаемые меры

- Сотрудникам компетентных органов необходимо обладать специализированными навыками и знаниями, требуемыми для проведения успешных финансовых расследований по делам, связанным с атаками с использованием программ-вымогателей. Это включает разработку, предоставление доступа и обучение использованию инструментов мониторинга и анализа блокчейна.
- Юрисдикциям также следует обеспечить наличие специальных механизмов для надлежащего управления арестованными виртуальными активами.

Политика и взаимодействие на национальном уровне

Национальная оценка и стратегия

84. В соответствии с Рекомендацией 1 ФАТФ, юрисдикции должны выявлять и оценивать свои риски ОД и применять риск-ориентированный подход для снижения этих рисков. Этот подход также должен служить основой для эффективного выделения и распределения ресурсов в рамках режима ПОД/ФТ.

85. Атаки с использованием программ-вымогателей часто рассматриваются с точки зрения оценки угроз для кибербезопасности. Например, некоторые юрисдикции разработали стратегии кибербезопасности или борьбы с киберпреступностью, которые содействуют сотрудничеству и взаимодействию на национальном уровне. Кроме того, в таких стратегиях содержатся политические обязательства активно бороться с преступлениями, совершаемыми с помощью программ-вымогателей, и связанными с этим незаконными финансовыми потоками. Национальные стратегии, как правило, предусматривают участие различных государственных ведомств[38] и могут включать соответствующие органы, отвечающие за ПОД/ФТ, такие как министерства юстиции, финансов и внутренних дел, а также представителей частного сектора. При этом необходимо отметить, что целью многих таких стратегий не обязательно является снижение рисков, связанных с незаконными финансовыми потоками. Эти риски должны рассматриваться и анализироваться в рамках национальных оценок рисков.

[37] Группа случайных слов, сгенерированная приложением кошелька в определённом порядке, которая может использоваться для восстановления или получения доступа к закрытому ключу (ключам) в обход дополнительных мер защиты (например, паролей).

[38] Учитывая угрозу для национальной безопасности, представляемую атаками с использованием программ-вымогателей, в число этих ведомств входят органы, отвечающие за обеспечение правопорядка, оборону, безопасность, связь и информационные технологии.

Вставка 20: Национальная стратегия кибербезопасности Испании

Национальная стратегия кибербезопасности Испании (последние изменения в которую были внесены в 2019 году) направлена на развитие умений и навыков с целью противодействия киберугрозам. В ней изложены приоритеты, задачи и соответствующие меры для достижения и поддержания высокого уровня безопасности сетей и информационных систем. Некоторые из ключевых направлений деятельности, определённых в Стратегии, направлены на развитие навыков для борьбы с киберугрозами, а также на наращивание возможностей для расследования и судебного преследования за совершение киберпреступлений.

В Стратегии заявлена необходимость развития и укрепления сотрудничества в правовой и правоохранительной сфере, а также выделение достаточных ресурсов компетентным органам и проведение обучения с целью повышения уровня профессиональных навыков и умений. Это также связано с формированием институциональной базы в сфере кибербезопасности, в частности, с созданием Национального совета по кибербезопасности. Целью этого Совета, возглавляемого премьер-министром Испании, является координация национальной политики в области кибербезопасности, а также содействие сотрудничеству и взаимодействию между государственными административными органами[1] и частным сектором[2], что играет существенную роль в реализации междисциплинарного подхода.

Источник: Испания

Примечания

[1] Министерство иностранных дел, Министерство юстиции, Министерство обороны, Министерство внутренних дел, Казначейство, Аппарат Премьер-министра, Национальный разведывательный центр, Управление национальной безопасности и другие.

[2] Специалисты и эксперты частного сектора включают в себя представителей профессиональных объединений, компаний и научных кругов.

86. В рамках своих национальных оценок рисков ОД в соответствии с Рекомендацией 1 ФАТФ юрисдикциям также следует рассмотреть угрозы, исходящие от атак с использованием программ-вымогателей. Такая оценка служит основой, на которой юрисдикции могут разрабатывать меры, направленные на снижение этих рисков и угроз, в том числе меры, предложенные в данном отчёте. Хорошее понимание рисков ОД, связанных с атаками с использованием программ-вымогателей, юрисдикции смогут распределить ресурсы в соответствии с риск-ориентированным подходом, в том числе для развития и повышения знаний и навыков в сфере виртуальных активов, а также приобретения инструментов блокчейн-анализа для соответствующих компетентных органов, отвечающих за ПОД/ФТ.

87. Юрисдикции, в которых атаки с использованием программ-вымогателей и связанное с этим отмывание денег в настоящее время не представляют серьёзной внутренней угрозы, также должны учитывать риски незаконных финансовых потоков, исходящих от хакерских атак с применением программ-вымогателей, в частности по причине уникальной взаимосвязи между программами-вымогателями и виртуальными активами. Юрисдикциям следует учитывать не только угрозу, которую атаки с применением программ-вымогателей представляют для их граждан и организаций, но также возможность того, что преступники могут

находиться на их территории или что ПУВА, находящиеся под их юрисдикцией, могут использоваться для отмывания или обналичивания доходов, полученных в результате таких атак. Например, у многих ПУВА может присутствовать распределённая архитектура в нескольких юрисдикциях. ПУВА может быть зарегистрирован в одной юрисдикции, его сотрудники могут находиться в другой юрисдикции, а техническая инфраструктура и частные ключи могут находиться в третьей юрисдикции. Это означает, что такие юрисдикции могут использоваться для незаконного перемещения денежных средств, связанных с атаками с применением программ-вымогателей, в частности через сектор ПУВА.

Вставка 21: Оценка угроз, представляемых атаками с использованием программ-вымогателей в рамках национальной оценки рисков отмывания денег

В марте 2022 года власти США опубликовали третий Отчёт о национальной оценке рисков отмывания денег, в котором определены наиболее существенные угрозы, исходящие от незаконных финансовых потоков, в том числе от киберпреступности, а также уязвимости, связанные с виртуальными активами. В этом Отчёте указано, что количество киберпреступлений значительно возросло с 2018 года и что атаки с использованием программ-вымогателей представляют особо существенную угрозу, связанную с незаконными финансовыми потоками. Например, в Отчёте говорится, что серьёзность и сложность атак с применением программ-вымогателей существенно возросли в период пандемии COVID-19. В Отчёте содержится основная информация о тенденциях совершения атак с применением программ-вымогателей, включая использование модели «программа-вымогатель как услуга» и тактики двойного вымогательства. В Отчёте также приведено множество типологий отмывания денег, например, использование зарубежных ПУВА, для которых характерны слабые меры контроля в целях ПОД/ФТ или их полное отсутствие, с целью размещения доходов от хакерских атак с применением программ-вымогателей. Установленные факты и выводы по итогам Национальной оценки рисков ОД были использованы при разработке Национальной Стратегии США по борьбе с терроризмом и другим незаконным финансированием от 2022 года (в которой содержатся рекомендации по снижению рисков, связанных с незаконными финансовыми потоками). Выводы НОР ОД были также использованы при подготовке Плана действий по снижению рисков незаконного финансирования, связанных с цифровыми активами.

Источник: США

Сотрудничество и взаимодействие на национальном уровне

88. В соответствии с Рекомендацией 2 ФАТФ юрисдикции должны иметь механизмы для сотрудничества, взаимодействия и обмена информацией между директивными органами, ПФР, правоохранительными ведомствами и другими компетентными органами. Атаки с использованием программ-вымогателей затрагивают широкий спектр областей, и поэтому в расследованиях могут принимать участие другие субъекты, не входящие в традиционную систему ПОД/ФТ, такие как ведомства, отвечающие за кибербезопасность и защиту данных. Наличие эффективных механизмов сотрудничества на национальном уровне является чрезвы-

чайно важным для сбора информации и привлечения различных экспертов, в том числе из частного сектора, в целях реализации комплексных мер реагирования, направленных на снижение рисков, представляемых атаками с применением программ-вымогателей и связанным с этим отмыванием денег. Это также позволяет осуществлять важный обмен информацией между правоохранительными органами, проводящими расследования предикатных преступлений и параллельные финансовые расследования.

89. В качестве примера передовой практики можно привести создание групп из представителей правоохранительных или междисциплинарных органов для борьбы с киберпреступлениями (или даже конкретно с атаками с использованием программ-вымогателей). Такие группы могут координировать проведение расследований атак с использованием программ-вымогателей и отмывания доходов, полученных в результате таких атак, для раскрытия которых требуются широкие экспертные знания (например, эксперты ПФР или правоохранительные органы, прокуроры, технические инженеры, переговорщики и т.д.). В рамках этого подхода, как правило, задействованы сотрудники правоохранительных органов, имеющих опыт отслеживания виртуальных активов. Такой подход может оказаться полезным для объединения специальных технических знаний и опыта экспертов особенно в случае ограниченных ресурсов и возможностей.

Вставка 22: Координационные механизмы для объединения оперативных данных и следственных знаний и опыта

Для реагирования на растущие угрозы в сфере кибербезопасности правительство США создало в 2008 году Национальную объединенную целевую группу по кибер-расследованиям (NCIJTF). Эта Группа состоит из представителей более 30 партнерских ведомств, входящих в структуры правоохранительных органов, разведывательного сообщества и министерства обороны. Представители этих ведомств базируются в одном месте и тесно взаимодействуют друг с другом с целью выполнения задачи организации на основе общегосударственного подхода.

Являясь уникальным межведомственным кибернетическим центром, NCIJTF в первую очередь отвечает за координацию, обобщение и обмен информацией в поддержку исследований киберугроз, выполнение анализа оперативных данных и представление его результатов лицам, принимающим решения. NCIJTF также оказывает содействие другим непрерывным усилиям по борьбе с киберугрозами для национальной безопасности.

В конце 2014 года в рамках NCIJTF была создана отдельная Группа по виртуальным валютам (VTC). Основная задача Группы - отслеживание операций с криптовалютами, которые имеют отношения к киберпреступлениям. Эта Группа обеспечивает отслеживание криптовалют для всех членов NCIJTF. В рамках проведения своих собственных расследований члены NCIJTF, такие как Федеральное бюро расследований и Секретная служба США, создали собственные отдельные группы для отслеживания виртуальных активов, поскольку они стали всё чаще использоваться при совершении различных видов преступлений.

В начале 2022 года Федеральное бюро расследований создало подразделение по виртуальным активам (VAU). Это подразделение является мозговым центром всех программ ФБР, связанных с виртуальными активами, который предоставляет опе-

ративные данные, технологии и оперативную поддержку другим подразделениям ФБР. В подразделении VAU эксперты по виртуальным активам и ресурсы из разных подразделений собраны в единый центр для объединения оперативных данных и операций в рамках всего ФБР.

Источник: США

Сотрудничество и руководства для частного сектора

90. Как отмечено в подразделе 5.2, взаимодействие с частным сектором является полезным для преодоления некоторых трудностей, описанных в данном отчёте. Например, регулируемые субъекты могут столкнуться с трудностями при выявлении подозрительных операций, связанных с атаками с применением программ-вымогателей. При этом некоторые юрисдикции отметили повышение количества и качества СПО, связанных с атаками с использованием программ-вымогателей, после того как они усилили взаимодействие с подотчётными субъектами и предоставили им Руководство, включая информацию о подозрительных индикаторах (см. «Противодействие использованию программ-вымогателей: потенциальные признаки риска», ФАТФ, 2023), а также руководящие указания по выявлению таких подозрительных операций.

Вставка 23: Австралийские руководства по выявлению финансовых преступлений

Австралийский альянс по борьбе с тяжкими финансовыми преступлениями «Fintel Alliance»[1] публикует различные справочники, включая руководства по выявлению финансовых преступлений, для оказания содействия коммерческим организациям в понимании, выявлении и направлении сообщений о подозрительной финансовой деятельности в целях выявления и предупреждения преступной деятельности.

В руководствах по выявлению финансовых преступлений содержится подробная информация о финансовых аспектах различного рода преступлений. В них также включены примеры дел и признаки для оказания помощи участникам сектора финансовых услуг в определении и выявлении подозрительных операций.

Для оказания содействия в борьбе с атаками с использованием программ-вымогателей в апреле 2022 года Австралийский центр отчетов и анализа транзакций (AUSTRAC – австралийское ПФР) выпустил два руководства, касающихся финансовых преступлений. Одно из этих руководств посвящено недопущению использования цифровых валют в преступных целях, а второе - выявлению и пресечению атак с использованием программ-вымогателей и последующей выплате выкупа. В этих двух руководствах содержится практическая информация и перечни ключевых признаков риска для выявления и реагирования на случаи, когда кто-нибудь становится целью преступников, требующих выплаты выкупа, или пытается получить выкуп в результате совершённой атаки с применением программы-вымога-

теля. Оба этих руководства по финансовым преступлениям доступны на вебсайте Центра AUSTRAC:

- Выявление и пресечение выплаты выкупа в результате атак с использованием программ-вымогателей/ AUSTRAC
- Предотвращение использования цифровых валют в преступных целях/AUSTRAC

Источник: Австралия

[1] Альянс «Fintel Alliance» является австралийским государственно-частным партнёрством, объединяющим экспертов из целого ряда организаций, участвующих в противодействии отмыванию денег, финансированию терроризма и в борьбе с другими тяжкими преступлениями. Партнёрами Альянса являются крупные банки, провайдеры услуг денежных переводов, организаторы азартных игр, а также правоохранительные ведомства и органы безопасности из Австралии и других стран.

91. Форма и степень сотрудничества с частным сектором в целях борьбы с атаками с использованием программ-вымогателей различаются в юрисдикциях. Государственно-частное партнёрство (ГЧП) является хорошо известной и полезной моделью такого сотрудничества, хотя во многих юрисдикциях в таких партнёрствах по-прежнему участвуют в основном традиционные субъекты (в частности, банки и другие финансовые учреждения, хотя также наблюдается участие всё большего числа УНФПП). Конкретный состав будет различаться в зависимости от целей и задач ГЧП, но члены партнёрства могут включать в себя нетрадиционных субъектов. В целях эффективного предупреждения и выявления атак с использованием программ-вымогателей государственно-частные партнёрства следует использовать для объединения усилий правоохранительных органов, местных групп реагирования на компьютерные инциденты, ПФР и ПУВА в дополнение к компаниям по кибербезопасности, провайдерам телекоммуникационных услуг и компаниям, занимающимся анализом блокчейна (например, в качестве подгруппы или оперативной группы в составе существующего ГЧП).

92. Общие задачи государственно-частных партнёрств включают повышение уровня информированности об атаках с использованием программ-вымогателей и последующего отмывания денег, обмен информацией о текущих тенденциях и исследование существующих и новых угроз. Эти механизмы также могут способствовать укреплению отношений с частным сектором и стимулировать направление сообщений.

93. Юрисдикции также используют ГЧП для достижения различных целей правоохранительных органов. Государственно-частные партнёрства являются полезной площадкой для обмена тактическими ориентировками в целях сбора оперативных данных, позволяют более эффективно выявлять «денежных мулов» и сети по отмыванию денег в различных регулируемых секторах и способствуют проведению расследований.

94. У ПУВА имеется ценная информация для успешного проведения расследований правоохранительными органами (в том числе сведения о владельцах кошельков и информация о снятии средств в фиатных валютах). В этой связи развитие отношений и сотрудничества с субъектами сектора ПУВА также мо-

жет позволить компетентным органам оперативно получать доступ к информации для отслеживания виртуальных активов, а также для эффективного ареста и конфискации активов.

Вставка 24: Проект «Gateway» и операция «Cyclone» Интерпола

Проект «Gateway» представляет собой механизм для обмена данными с частным сектором. Он был запущен в 2016 году с целью обмена информацией, касающейся киберпреступлений. Этот проект способствует активному развитию партнёрских отношений между правоохранительными органами и субъектами частного сектора, что обеспечивает получение данных об угрозах из множества разных источников и позволяет органам полиции предотвращать атаки. Субъекты, участвующие в проекте «Gateway», занимаются деятельностью, имеющей отношение к сфере киберпреступности. К их числу относятся компании по кибербезопасности, компании, занимающиеся анализом угроз, а также провайдеры услуг в сфере виртуальных активов и банки.

Этот механизм позволяет осуществлять двусторонний обмен информацией о киберпреступлениях между Интерполом и частным сектором, а также даёт субъектам частного сектора возможность оказывать содействие Интерполу в проведении анализа киберпреступности. Партнёры из частного сектора приносят пользу благодаря своим техническим знаниям, которые помогают определять виды программ-вымогателей, используемых преступниками для заражения систем (если они неизвестны), а также анализировать любые возможные зацепки.

Операция «Cyclone» («Циклон»)[1] была начата после международного полицейского расследования атак, совершённых в отношении южнокорейских компаний и американских научно-образовательных учреждений хакерской группировкой, использовавшей программу-вымогатель Cl0p. В результате этой международной операции в июне 2021 года были арестованы шесть членов группировки, использовавшей это вредоносное программное обеспечение. Операция координировалась Интерполом совместно с правоохранительными органами Южной Кореи, Украины и США. Считается, что подозреваемые способствовали переводу и обналичиванию активов на сумму более 500 миллионов долларов США от имени группировки хакеров. Интерпол начал операцию «Cyclone» благодаря информации, предоставленной его партнёрами из частного сектора в рамках проекта «Gateway».

Источник: Интерпол

[1] Дополнительную информацию можно найти по адресу: www.interpol.int/en/News-andEvents/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrimering

Предлагаемые меры

- В рамках проведения своих национальных оценок рисков юрисдикциям следует обеспечить выявление и оценку рисков ОД, представляемых атаками с использованием программ-вымогателей. Принимая во внимание децентрализованный характер виртуальных активов и наличие преступных группировок, специализирующихся на использовании программ-вымогателей, это также касается юрисдикций, в которых имеются секторы виртуальных активов, но атаки с использованием программ-вымогателей в настоящее не представляют внутреннюю угрозу. Такое выявление и анализ рисков может оказаться полезным в разработке национальных стратегий кибербезопасности, поскольку это позволит получить комплексную национальную картину рисков, исходящих от использования программ-вымогателей.
- Юрисдикциям следует разработать механизмы взаимодействия между соответствующими компетентными органами, начиная от правоохранительных органов, органов, отвечающих за ПОД/ФТ, и органов, занимающихся борьбой с киберпреступностью, и заканчивая нетрадиционными партнёрами, такими как ведомства, отвечающие за кибербезопасность и защиту данных. Это способствует обмену информацией и оперативными данными, а также обеспечивает механизм для взаимного обмена различными техническими знаниями и опытом.
- Юрисдикциям следует определить и создать механизмы для поддержки сотрудничества между государственным и частным сектором. Юрисдикциям следует рассмотреть возможность включения ПУВА и других нетрадиционных партнёров в такие механизмы сотрудничества.

Международное сотрудничество

95. Атаки с использованием программ-вымогателей и связанные с этим финансовые потоки часто носят трансграничный и многонациональный характер. Преступники, совершающие атаки с использованием программ-вымогателей, обычно находятся в юрисдикциях, отличных от тех, через которые осуществляется отмывание и конечное обналичивание средств (особенно виртуальных активов). Сложность схем ОД, связанных с атаками с применением программ-вымогателей, а также трудности в выявлении и расследовании таких схем, требуют постоянного трансграничного сотрудничества между правоохранительными органами с использованием соответствующей информации, инструментов и знаний. Создание новых и использование существующих механизмов международного сотрудничества является первоочередным условием для успешного проведения финансовых расследований и возврата активов, особенно в случае атак с применением программ-вымогателей.

Вставка 25: Совместное международное расследование в отношении вредоносного программного обеспечения Lockergoga

В январе 2019 года крупная французская компания подверглась атаке со стороны хакеров-вымогателей. Было установлено, что вредоносное ПО Lockergoga было использовано в качестве программы-вымогателя для шифрования нескольких файлов и внутренних серверов компании. Хотя после переговоров со злоумышленниками они запросили выкуп в размере 410 биткоинов, компания не заплатила выкуп. При этом было установлено, что программа-вымогатель Lockergoga использовалась хакерами при проведении ряда других атак.

Был создана совместная следственная группа под эгидой Евроюста/Европола, в состав которой вошли представители нескольких европейских юрисдикций. Это позволило осуществлять эффективный обмен информацией, включая сотрудничество между органами юстиции и судебными органами в рамках Директивы ЕС о европейском ордере на производство следственных действий по уголовным делам (европейский следственный ордер) и Договора об оказании взаимной правовой помощи, что помогло ускорить проведение расследований. Европол/Евроюст также оказали техническую поддержку, предоставив большое количество оборудования и финансирование. После этого была вскрыта инфраструктура контроля и управления преступников и расшифрованы сообщения, которыми обменивались хакеры. В конечном итоге было установлено, что хакерская группировка находилась в одной из юрисдикций на востоке, что позволило провести несколько арестов в этой юрисдикции.

Тем не менее расследования продолжаются. Проведя анализ блокчейна, следователи раскрыли различные схемы «цепочек списания», использовавшиеся преступниками. Это привело к аресту в Швейцарии одного из основных фигурантов, занимавшихся отмыванием денег. Также были задержано несколько «денежных мулов» в разных юрисдикциях. В ходе расследований также было установлено, что выплачиваемый жертвами выкуп не переводился исключительно в пользу хакеров. Например, группировке необходимо было осуществлять незаконные платежи за услуги своим «партнёрам» по криминальному бизнесу. Кроме того, средства, полученные в качестве выкупа, использовались для поддержки инфраструктуры (для оплаты услуг инженеров и разработчиков программного обеспечения, за услуги хостинга защищённых серверов, за услуги защищённых виртуальных частных сетей для сокрытия связи с серверами контроля и управления, за услуги по организации цепочки списаний средств в целях отмывания денег и т.д.), а также для поиска «денежных мулов» и механизмов по обналичиванию средств.

Источник: Франция

96. При направлении международных запросов запрашиваемая информация обычно касается данных криминалистической экспертизы и улик, необходимых для расследования предикатных преступлений, а также финансовых данных, необходимых для расследований отмывания денег. Это включает информацию о зарубежных IP-адресах, сведения об используемых именах и псевдонимах, данные о подписчиках, а также информацию о бенефициарных владельцах, сведения об операциях и данные о контрагентах, связанных с кошельками, размещёнными у зарубежных ПУВА.

Затруднения, обусловленные использованием виртуальных активов

97. Использование виртуальных активов для отмывания доходов, полученных в результате атак с применением программ-вымогателей, создаёт новые затруднения в процессе трансграничного сотрудничества. Различия в отношении к виртуальным активам или регулированию виртуальных активов в рамках разных правовых систем (а также ограниченное вмешательство или надзор со стороны государственных органов в отношении сектора виртуальных активов или отсутствие такого вмешательства/надзора в некоторых юрисдикциях) может ограничить возможности или желание компетентных органов участвовать в международном сотрудничестве.

98. Например, в юрисдикциях, в которых не осуществляется регистрация или надзор за ПУВА, компетентные органы могут испытывать затруднения в определении компаний, у которых следует запрашивать информацию. Даже если соответствующий субъект установлен, компетентные органы могут не обладать никакими другими возможностями, кроме того как использовать принудительные следственные методы для исполнения зарубежного запроса, полученного в рамках международного сотрудничества. Это может ограничить объём информации, которую можно получить в рамках неофициального сотрудничества.

99. Эта проблема усугубляется в реальности тем, что власти многих юрисдикций, в которых находятся преступники, совершающие атаки с использованием программ вымогателей, и их «денежные мулы» или в которых находятся или осуществляют деятельность ПУВА, используемые для отмывания и обналичивания незаконных доходов хакеров, спокойно относятся к этой деятельности и могут не отвечать на запросы зарубежных правоохранительных органов. Если ПУВА находятся в юрисдикциях, в которых на них не распространяются обязательства в сфере ПОД/ФТ, у них могут отсутствовать соответствующие записи и документы для передачи правоохранительным органам. Это, в конечном итоге, заводит в тупик ведущиеся финансовые расследования и сводит на нет попытки вернуть активы. Эти проблемы и трудности ещё раз подчёркивают важность ускоренной реализации требований Рекомендации 15 ФАТФ (включая «дорожное правило»).

Вставка 26: Затруднения, возникшие в ходе расследования по причине отказа от сотрудничества со стороны зарубежного ПУВА

Компания «X» подверглась атаке с использованием программы-вымогателя (предположительно это была вредоносная программа Caley). В результате переговоров компания заплатила хакеру выкуп в размере 0,25 биткоинов, после чего она получила по электронной почте ключ для дешифрования, позволивший компании возобновить нормальную деятельность, расшифровав свои файлы.

Власти с опозданием узнали об этом инциденте через полицию, которая получила сообщение от потерпевшей компании через несколько дней после выплаты выкупа, когда след от выплаты уже «остыл». Несмотря на это, был проведён анализ блокчейна, в результате которого след от выплаты выкупа привёл к находящемуся за рубежом провайдеру услуг в сфере виртуальных активов. Также было установлено, что остаток платежа был помещён в кошелёк виртуальных активов, открытый у этого

зарубежного ПУВА. Однако с того времени этот ПУВА хранит молчание, несмотря на направленные в его адрес многочисленные запросы о предоставлении информации. Проведение расследования было затруднено ещё и тем, что злоумышленник использовал «миксеры» для сокрытия операций. С учётом обстоятельств этого дела, личность злоумышленника остаётся неизвестной, и отсутствует возможность провести его арест или возвратить активы.

Источник: Сингапур

100. Распределённая архитектура некоторых ПУВА (которые осуществляют деятельность сразу в нескольких юрисдикциях) также может значительно увеличить следственную нагрузку на правоохранительные органы. Это связано с тем, что правоохранительным органам потребуется определить соответствующего субъекта, у которого следует запрашивать информацию, или определить соответствующую юрисдикцию, в которую следует направить запрос об оказании помощи. Например, одна юрисдикция указала на трудности в определении соответствующей юрисдикции, у которой следует запрашивать помощь, на основании международного номера банковского счёта (IBAN), который предположительно присвоен банковскому счёту, находящемуся под управлением ПУВА в зарубежном финансовом учреждении. Ещё одна юрисдикция отметила, что ПУВА не присутствуют физически во многих юрисдикциях, в которых они осуществляют свою деятельность, что затрудняет поиск нужной юрисдикции для сотрудничества.

Необходимость быстрого и оперативного сотрудничества

101. Поскольку преступники, совершающие атаки с использованием программ-вымогателей, могут находиться в самых разных странах по всему миру, а переводы виртуальных активов могут осуществляться практически мгновенно, правоохранительным органам необходимо действовать быстро для отслеживания доходов от атак с использованием программ-вымогателей до того, как они утекут через границы и растворятся за рубежом. Для этого, как правило, требуются механизмы официального международного сотрудничества (такие как механизмы взаимной правовой помощи) в целях получения доказательств и ареста активов в процессе уголовного производства. Однако такие механизмы официального сотрудничества не всегда позволяют быстро принимать необходимые меры, что может замедлить, застопорить или даже свести на нет расследования. Сложность расследований атак с использованием программ-вымогателей, в которых фигурирует множество юрисдикций и компаний, дополнительно усугубляет эти трудности, поскольку международное сотрудничество в отношении атак с применением программ вымогателей занимает больше времени и ресурсов, нежели в отношении других видов преступной деятельности.

102. Использование механизмов неофициального сотрудничества помогает в преодолении этих трудностей, а также упрощает и ускоряет исполнение запросов об оказании взаимной правовой помощи. В целях содействия осуществлению своевременного сотрудничества некоторые юрисдикции отметили важность использования существующих связей и создания неофициальных каналов для взаимодействия с зарубежными партнёрами. Это обеспечивает быстрый обмен информацией необходимой для производства по уголовным делам при условии соблюдения установ-

ленных правил, касающихся защиты такой информации. Такой неофициальный обмен информацией между ПФР может осуществляться через защищённую сеть Эгмонт, а сотрудничество между органами полиции может осуществляться через сеть Интерпола I-24/7 или через другие неофициальные сети, включая Камденскую межведомственную сеть по возврату активов (CARIN) и региональные межведомственные сети по возврату активов (ARIN). Властям также следует установить процедуры и назначить контактных лиц в рамках существующих каналов международного и регионального сотрудничества для содействия оперативному отслеживанию средств и эффективному возврату активов.

103. Некоторые юрисдикции отметили успешное сотрудничество в рамках установленных двусторонних отношений. Прикомандирование в зарубежные страны специальных сотрудников по связям, занимающихся вопросами киберпреступлений, может значительно ускорить обмен информацией и оперативными данными между юрисдикциями, направившими и принявшими таких сотрудников по связям, а также позволить компетентным органам собирать и передавать доказательства в ходе расследования атак с использованием программ-вымогателей. В целях содействия и развития двустороннего сотрудничества властям следует рассмотреть возможность опубликования процедур и списков контактных лиц для сотрудничества, в частности для содействия оперативному отслеживанию средств и возврата активов.

Вставка 27: Проект «CODA»

В ноябре 2021 года был арестован канадский хакер, причастный к серии атак с использованием программ-вымогателей, а также к взлому компьютерных систем правительственных организаций и медицинских учреждений в штате Аляска. Ему были предъявлены обвинения в совершении целого ряда киберпреступлений. Перед тем как связаться с зарубежными партнёрами, ФБР проводило расследование нескольких похожих кибервзломов. После того как личность и местонахождение подозреваемого были установлены, сотрудники ФБР связались с контактным лицом из Полиции штата Онтарио, назначенным в рамках двустороннего сотрудничества.

После этого были начаты параллельные расследования в обеих юрисдикциях. В ходе этих расследований Канадский национальный координационный центр по борьбе с киберпреступностью (Центр NC3), Европол и правоохранительные органы Нидерландов оказывали содействие сотрудникам Полиции Онтарио и ФБР. В частности, Центр NC3 оказывал оперативную поддержку, осуществлял анализ данных и поведения фигурантов расследования, предоставлял оперативные сводки и отчёты, помогал отслеживать криптовалюты и оказывал аналитические услуги на протяжении 23 месяцев, пока шло международное расследование. Это помогло подтвердить личность подозреваемого и привело к его последующему аресту. Использование передовых технических методов анализа и специальных инструментов, таких как инструменты отслеживания криптовалют, играет ключевую роль в расследованиях таких видов киберпреступлений.

Источник: Канада и США

Важность многостороннего взаимодействия

104. В примерах, касающихся успешных действий правоохранительных органов, как правило, участвуют компетентные органы из нескольких юрисдикций. Это отражает международный и децентрализованный характер атак с использованием программ-вымогателей и отмывания доходов от таких атак. Существенным условием для достижения успеха является необходимость международного сотрудничества и взаимодействия между пострадавшими юрисдикциями для одновременного выявления и пресечения деятельности преступных киберсиндикатов и их сообщников. Это также снижает риск смены места базирования, когда преступные организации могут переместить свои цифровые операции в другое безопасное место.

105. Имеется несколько механизмов для международной координации деятельности правоохранительных органов, таких как Европол/Евроюст или Интерпол, которые могут быть использованы в этих целях. Эти организации ведут базы данных и оказывают логистическую и экспертную поддержку для координации усилий заинтересованных ведомств из нескольких юрисдикций. Такие многосторонние механизмы могут оказаться полезными, особенно для ускорения обмена критически важной информацией необходимой для проведения финансовых расследований и возврата активов.

Вставка 28: Операция «GoldDust»[1]

В ноябре 2021 года румынские власти арестовали двух человек, подозреваемых в совершении атак с использованием программы-вымогателя «Sodinokibi/REvil». По имеющимся данным они ответственны за 5 000 случаев заражения компьютерных систем и получили в общей сложности полмиллиона евро в качестве выкупа. Начиная с февраля 2021 года, правоохранительные органы арестовали ещё двух сообщников причастных к атакам с использованием программы-вымогателя «Sodinokibi/REvil», а также двух подозреваемых, связанных с применением программы-вымогателя «GandCrab». Это лишь некоторые из результатов операции «GoldDust», в которой участвовали 17 юрисдикций[2], Европол, Евроюст и Интерпол. Все аресты стали результатом совместных международных усилий правоохранительных органов по выявлению, прослушиванию переговоров и наложению ареста на некоторые элементы инфраструктуры, с помощью которой использовались разновидности программы-вымогателя «Sodinokibi/REvil». Программа «Sodinokibi/REvil» считается «потомком» семейства компьютерных вирусов «GandCrab».

Операция «GoldDust» началась на основании ориентировок и зацепок, полученных в ходе предыдущих расследований атак с использованием программы-вымогателя «GandCrab», в частности расследования, проводившегося под руководством Румынии при поддержке Европола и правоохранительных органов нескольких юрисдикций, включая Великобританию и США.

Европол содействовал обмену информацией, помогал координировать операцию «GoldDust», оказывал оперативную аналитическую поддержку, осуществлял анализ криптовалют и вредоносных программ, а также проводил криминали-

стическую экспертизу и анализ. Европол также направил экспертов в каждую юрисдикцию, принимавшую участие в расследованиях, и использовал виртуальный пункт управления для координации деятельности на местах. Международное сотрудничество также позволило Европолу оптимизировать совместно с другими юрисдикциями-членами ЕС меры, принимаемые потерпевшими для минимизации ущерба. Эти действия позволили не допустить того, чтобы другие частные компании стали жертвами атак с использованием программы-вымогателя «Sodinokibi/REvil».

Объединённая целевая группа по борьбе с киберпреступностью Европола (J-CAT) также оказала содействие проведению операции. В состав этой постоянной оперативной группы входят сотрудники по связям в сфере борьбы с киберпреступностью из различных юрисдикций, которые работают в одном месте над расследованием резонансных киберпреступлений.

Источник: Европол

Примечания

[1] Дополнительную информацию можно найти по адресу: www.europol.europa.eu/mediapress/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

[2] Юрисдикции, принявшие участие в операции: Австралия, Бельгия, Канада, Франция, Германия, Нидерланды, Люксембург, Норвегия, Филиппины, Польша, Румыния, Южная Корея, Швеция, Швейцария, Кувейт, Великобритания и США

Предлагаемые меры

- Юрисдикциям следует создать и активно участвовать в двусторонних, региональных и многосторонних механизмах сотрудничества, например, используя прикомандированных сотрудников по связям и путем назначения контактных лиц доступных в круглосуточном режиме, для содействия оперативному международному сотрудничеству и обмену информацией.

Заключение

106. Несмотря на увеличение в последние годы объёмов незаконных финансовых потоков, связанных с атаками с использованием программ-вымогателей, количество расследований случаев отмывания доходов от таких атак по-прежнему является недостаточным. Данное исследование показало, что атаки с использованием программ-вымогателей являются многоплановой международной проблемой. Всё это требует применение скоординированного подхода для эффективного реагирования на эту угрозу. Для достижения этой цели юрисдикциям следует использовать механизмы партнёрства на трёх уровнях: государственно-государственное партнёрство; государственно-частное партнёрство; и партнёрство с зарубежными юрисдикциями и многосторонними организациями.

107. Данное исследование также показывает важность ускоренной реализации Стандартов ФАТФ для создания эффективного механизма борьбы с незаконными доходами, полученными в результате атак с использованием программ-вымогателей, особенно в секторе виртуальных активов и ПУВА. ФАТФ продолжит активно содействовать реализации Стандартов в этом секторе.

108. Роль виртуальных активов в отмывании доходов, полученных в результате атак с использованием программ-вымогателей, а также всё более совершенные методы, используемые преступными группировками, представляют дополнительные трудности. В этой связи компетентным органам следует обеспечить, чтобы нормативно-правовые акты, регулирующие их деятельность, оставались актуальными, а их сотрудники обладали знаниями и навыками для оперативного и эффективного реагирования в условиях динамично изменяющейся обстановки в сфере киберпреступности.

www.fatf-gafi.org

Март 2023

Противодействие использованию программ-вымогателей: потенциальные признаки риска

Этот перечень возможных признаков риска поможет субъектам государственного и частного сектора в выявлении подозрительной деятельности, связанной с атаками с использованием программ-вымогателей. Данный перечень признаков дополняет отчёт ФАТФ «Противодействие использованию программ-вымогателей», в котором анализируются методы, используемые преступниками для совершения атак с применением программ-вымогателей, а также то, как осуществляется выплата выкупа и происходит отмывание этих незаконных доходов.