



HI-TECH CRIME TRENDS 2021/2022



КИБЕРИМПЕРИЯ ШИФРОВАЛЬЩИКОВ

ДИСКЛЕЙМЕР

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры различных групп для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в отчете информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

HI-TECH CRIME TRENDS 2021/2022



Угроза #1: киберимперия шифровальщиков

История, анализ, партнерские программы
и тренды рынка шифровальщиков

ГЛАВА 2

ОГЛАВЛЕНИЕ

ПОЧЕМУ HI-TECH CRIME TRENDS	5
ВВЕДЕНИЕ	6
КЛЮЧЕВЫЕ ТРЕНДЫ	9
ПРОГНОЗЫ	10
ИСТОРИЯ РАЗВИТИЯ РЫНКА RAAS	11
Зарождение	12
Время локеров, Winlock и первые партнерские программы	15
Первые современные шифровальщики и продолжение господства локеров	19
Появление партнерских программ по шифровальщикам, партнерская программа и автор CryptoLocker	24
Развитие направления RaaS, смена фокуса на бизнес, угроза публикации файлов	27
Дальнейшая популяризация вымогателей, WannaCry	31
Формирование современных трендов RaaS: GandCrab	33
Современные тренды: double extortion, появление DLS, запрет партнерских программ на форумах	38
АНАЛИЗ ТЕКУЩИХ ТРЕНДОВ RAAS	43
Публичные партнерские программы	43
Анализ атак программ-вымогателей на основе компаний, опубликованных на DLS	46
Обзор тактик, техник и процедур в атаках с использованием программ-вымогателей	53
ЗАКУЛИСЬЕ МИРА КИБЕРВЫМОГАТЕЛЕЙ	62
История Hive и разбор DLS	62
Suncrypt	74
RTM: как зарождаются новые партнерские программы, или тихие локеры	82
История Groove и первой Fake DLS	85
РЕКОМЕНДАЦИИ ПО ПРОАКТИВНОМУ ПОИСКУ УГРОЗ	88
ТРОЯНЫ	90
О КОМПАНИИ	93

ПОЧЕМУ HI-TECH CRIME TRENDS?

00

Hi-Tech Crime Trends исследует разные аспекты функционирования киберкриминальной индустрии, анализирует атаки и прогнозирует изменение ландшафта угроз для различных отраслей мировой экономики. Отчет выпускается с 2012 года и интегрирует данные собственных исследований компании, реагирований на киберинциденты по всему миру.

Применяя уникальные инструменты слежения за инфраструктурой киберпреступников и тщательно изучая исследования специалистов из разных стран, эксперты Group-IB ежегодно находят и подтверждают общие паттерны глобального развития киберугроз. На основе этого формулируются прогнозы, которые сбываются каждый год с момента первой публикации отчета Hi-Tech Crime Trends. Они помогают компаниям во всем мире выстраивать эффективные стратегии кибербезопасности с учетом релевантных угроз.

Hi-Tech Crime Trends открывает доступ к максимально полному набору стратегических данных и подробной информации об актуальных киберугрозах в мире, как организациям, которые борются с киберпреступностью, так и потенциальным жертвам.

Hi-Tech Crime Trends предназначен для ИТ-директоров, руководителей команд кибербезопасности, SOC-аналитиков, специалистов по реагированию на инциденты, для которых отчет является практическим руководством стратегического и тактического планирования.

Прогнозы и рекомендации Hi-Tech Crime Trends направлены на сокращение финансовых потерь и простоев инфраструктуры, а также на принятие превентивных мер по противодействию целевым атакам, шпионажу и кибертеррористическим операциям.

Команда Group-IB убеждена в том, что постоянный обмен данными, создание и развитие партнерских отношений между частными компаниями и международными правоохранительными органами – эффективный путь борьбы с киберпреступностью. Осознанное отношение к кибербезопасности поможет сохранить и защитить глобальные возможности цифрового пространства и свободу коммуникаций.

Первый прототип вредоносного программного обеспечения, отдаленно напоминающий методы современных программ-шифровальщиков, распространялся на дискетах или через CD-диски еще в **1989** году и вымогал деньги пользователей, применяя социальную инженерию. Тогда это было больше похоже на мелкое мошенничество и, конечно, тот троян не умел шифровать данные, а его авторы не представляли иных способов монетизации, кроме простого обмана.

До появления первых **Data Leak Site** (DLS) — сайтов с публикацией данных компаний-жертв, отказавшихся платить выкуп, остается еще три десятка лет. До появления первых партнерских программ **Ransomware-as-a-Service** (RaaS) — порядка двадцати.

За это время термин Ransomware стал синонимом кибервымогательства в сети. Став технологическим фундаментом масштабной теневой индустрии, атаки с использованием программ-вымогателей превратились в главную угрозу для коммерческого и государственного секторов во всем мире. Операторы шифровальщиков и участники их партнерских программ зарабатывают миллионы долларов, нанося ущерб компаниям во всем мире.

Тысячи злоумышленников, занимавшихся взломами сетей, трафиком, загрузками, разработкой ВПО, целевыми атаками оказались востребованными в новой гигантской нише киберкриминального мира. Так появилась киберимперия шифровальщиков.

За неполный 2021 год более 60% всех расследованных специалистами Group-IB инцидентов пришлось на атаки шифровальщиков. Активное развитие рынка RaaS, а также смещение фокуса многих финансово-мотивированных групп на организацию атак с использованием программ-вымогателей, значительно повлияло на количество расследуемых инцидентов такого типа.

Чтобы понять, как произошел переход киберпреступности от сложных целевых атак к нецелевым партнерским программам по распространению вредоносного ПО, необходимо проследить историю развития подобных сервисов. Именно эту цель мы положили в основу данного исследования.

Используя возможности нашей системы **Group-IB Threat Intelligence & Attribution**, хранящей исторические данные о вредоносном ПО, злоумышленниках и хакерских группах и их связях за последние 15 лет, мы подробно останавливаемся на наиболее значимых экземплярах ВПО, тактиках, методах и инструментах киберпреступников, а также на событиях в даркнете, которые привели к становлению империи кибервымогателей.

более 60%

расследованных Group-IB атак пришлось на шифровальщиков

Исторические вехи: от 1000 рублей до 240 млн долларов

Способ обогащения через вымогательство был распространен среди злоумышленников, которые использовали угрозу DDoS-атак для получения денежных средств со своих жертв. Основной причиной популярности такого метода «заработка» было слабое распространение CDN-сервисов, в связи с чем обычному пользователю было крайне сложно защититься от DDoS-атак. Появление CDN с интегрированной защитой от DDoS привело к тому, что злоумышленники начали искать новые способы монетизации.

Вредоносное ПО, которое уже умело шифровать данные на машинах жертв, появилось в 2004 году. Это был PGPcoder и он требовал по нынешним меркам смешную сумму — 1000 руб. — за расшифровку данных жертвы.

Однако PGPcoder не получил широкого распространения, потому что был нацелен исключительно на физических лиц и сильно загружал низкоСпроизводительные на тот момент машины жертв. Это приводило к тому, что активность вредоносного ПО было достаточно просто обнаружить.

Ближе к концу 2000-х злоумышленники решили использовать более простой подход, перейдя на блокирование определенных функций работы операционной системы и требования выкупа. Настала эпоха **WinLocker**, а вместе с ней появилось явление, которое сегодня принято называть Ransomware-as-a-service (RaaS).

В 2010 году появились разработчики вредоносного ПО, которые быстро поняли, что сложно разрабатывать и совершенствовать свои трояны и при этом заниматься их распространением, поэтому они стали скупить трафик и загрузки. В целях оптимизации были созданы прототипы первых партнерских программ, схемы которых взяли на вооружение и доработали все современные RaaS-сервисы. Активность винлокеров продолжалась до 2013 года, пока не появился шифровальщик **Cryptolocker**.

Его популярность и огромное количество упоминаний атак 2013-2014 гг. с использованием CryptoLocker в СМИ привело к взлету количества предложений по продаже шифровальщиков и партнерских программ по ним на андеграундных форумах. Однако в те годы основными жертвами шифровальщиков оставались физические лица.

В 2016-2017 году по миру прокатилась волна атак **WannaCry** и **NotPetya**. Именно они заставили бизнес впервые серьезно задуматься об этой угрозе.

В 2018 году появилась первая профессиональная партнерская программа **GandCrab**. Её основным отличием от предшествующих попыток стало то, что злоумышленники собирали команды по разным направлениям, одним из которых стали атаки на сети крупных предприятий. Это явление позже получит название **Big Game Hunting**.

Последующие годы покажут, что именно Big Game Hunting предопределил основные цели всех партнерских программ. Следующее глобальное изменение принесли группы **Snatch** и **Maze**, когда они стали не только шифровать данные компаний, но также выгружать их из сетей жертвы и публиковать на своих ресурсах. Это привело к сильному увеличению конвертации у злоумышленников: техника была взята на вооружение.

2004

год, когда появился первый шифровальщик PGPcoder

≈2009

начало эпохи винлокеров и появление Ransomware-as-a-service (RaaS)

2018

появление партнерской программы GandCrab, которая отдельно фокусировалась на атаках больших компаний

А дальше произошли события, которые вывели атаки шифровальщиков на первые полосы всех СМИ в мире: жертвами шифровальщиков стали Garmin, JBS, Colonial Pipeline, Kaseya... и MediaMarkt, с которого операторы программы-вымогателя Hive потребовали 240 млн долларов.

И вот, что мы видим сегодня: только за период H2 2020 — H1 2021 в андеграунде появилась **21 новая активная партнерская программа** и открылось **28 DLS**, на которых злоумышленники опубликовали данные **2 371 компаний-жертв**.

В этом исследовании мы рассмотрели ключевые причины и этапы развития индустрии программ-вымогателей, подробно разобрали деятельность некоторых партнерских программ изнутри и привели анализ по самым атакуемым странам и отраслям в мире.

КЛЮЧЕВЫЕ ТРЕНДЫ

ПОЯВЛЕНИЕ DLS С ЛОЖНЫМИ ДАННЫМИ

Впервые появился DLS с фейковыми данными об атаках.

НЕКОТОРЫЕ КОМПАНИИ СОГЛАШАЮТСЯ НА УСЛОВИЯ ШИФРОВАЛЬЩИКОВ

Около 30% компаний выплачивают выкуп злоумышленникам.

СПИСОК АТАКУЕМЫХ СТРАН НЕ МЕНЯЕТСЯ

По количеству жертв программ-вымогателей лидерами по-прежнему являются — США (49,2%) и Канада (5,6%). За ними следует Франция (5,2%), сменившая на этом месте Великобританию.

АТАКУЮТ САМЫЕ МОНЕТИЗИРУЕМЫЕ ОТРАСЛИ

Основные атакуемые отрасли: производство (9,6%), недвижимость (9,5%) и транспорт (8,2%).

НОВАЯ ТРОЙКА ЛИДЕРОВ СРЕДИ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Среди программ-вымогателей на первое место по проведенным атакам вышли Conti (16.5%), за ними Lockbit (11.5%) и Avaddon (7.5%). Группа Maze — лидер прошлого года — прекратила свое существование.

НЕ ВСЕ ДАННЫЕ ПУБЛИКУЮТСЯ НА DLS

На DLS выкладываются данные только 10% атакуемых компаний.

КОЛИЧЕСТВО НОВЫХ ПАРТНЕРСКИХ ПРОГРАММ ШИФРОВАЛЬЩИКОВ РАСТЕТ

Оно выросло на 23% (с 17 до 21) за период H2 2020 — H1 2021 по сравнению с H2 2019 — H1 2020.

УВЕЛИЧИВАЕТСЯ КОЛИЧЕСТВО DLS

Количество новых сервисов Data Leaks Sites для публикации выгружаемых данных из зашифрованных сетей жертв выросло на 115% (с 13 до 28) за период H2 2020 — H1 2021 по сравнению с H2 2019 — H1 2020.

КОЛИЧЕСТВО ЖЕРТВ НА DLS РАСТЕТ

Количество жертв, чьи данные были опубликованы на DLS, выросло на 935% (с 229 до 2371) за период H2 2020 — H1 2021 по сравнению с H2 2019 — H1 2020.

ПАРТНЕРСКИЕ ПРОГРАММЫ УХОДЯТ В ПРИВАТ

Большая часть партнерских (87%) программ уходит в приватную работу, однако в них по-прежнему можно вступить, если знать злоумышленников лично.

ВЫКУП НЕ СПАСАЕТ ОТ УТЕЧКИ ДАННЫХ

Когда компании-жертвы выплачивают выкуп, многие киберпреступники удаляют данные таких компаний с DLS, однако скомпрометированные файлы по-прежнему доступны по ссылкам.

ПРОГНОЗЫ

03

ПАРТНЕРСКИЕ ПРОГРАММЫ НЕ ИСЧЕЗНУТ ПОСЛЕ ЗАПРЕТА В АНДЕГРАУНДЕ

После запрета публичных партнерских программ на андеграундных форумах появился форум RAMP, где активность вымогателей была разрешена. Из этого можно предположить, что количество новых партнерских программ сохраняется.

DLS МОЖЕТ СТАТЬ ПЛОЩАДКОЙ ДЛЯ ПРОДАЖИ ДАННЫХ

Злоумышленники могут начать продавать данные скомпрометированных компаний на DLS. Такая активность была ранее, но пока не стала трендом.

ТОП-3 АТАКУЕМЫХ ОТРАСЛЕЙ ОСТАНЕТСЯ ПРЕЖНИМ

Основные атакуемые отрасли, скорее всего, не изменятся, так как они наиболее монетизируемые по мнению злоумышленников.

ЧИСЛО ЖЕРТВ ВЫМОГАТЕЛЕЙ И DLS БУДЕТ РАСТИ

Количество скомпрометированных данных компаний, публикуемых на публичных ресурсах операторов программ-вымогателей, будет расти. Также будет расти количество самих DLS.

ИСТОРИЯ РАЗВИТИЯ РЫНКА RAAS

HI-TECH CRIME TRENDS 2021/2022

GROUP-IB.RU

История развития киберимперии вымогателей: 1989 — 2021

Дата	Событие
01.1989	AIDS Trojan
04.2004	Появление первого известного локера ОС Krotten
12.2004	Появление первого псевдосовременного шифровальщика PGPcoder
03.2006	Появление шифровальщика через ZIP-архивы Cryzip
06.2006	Первые гайды по написанию шифровальщиков в андеграунде
05.2009	Первое появление в продаже локера Winlocker на андеграундных форумах
06.2009	Всплеск продаж различных локеров на форумах
07.2009	Появление статей о разработке локеров в андеграунде
01.2010	Появление первых партнерских программ по локерам
12.2010	Возвращение шифровальщиков, публикация в свободном доступе билдера Encoder
07.2011	Продажи доработанного Encoder
01.2012	Появление локеров с функцией перезаписи MBR
09.2012	Начало серии атак шифровальщиков на Австралию
06.2013	Первая партнерская программа по шифровальщикам
09.2013	Партнерская программа и первые атаки Cryptolocker
12.2013	Известные пользователи андеграунда сообщают, что тренд на локеры умер, и наступила эпоха криптолокеров
01.2014	Появление большого количества новых криптолокеров и партнерских программ
05.2015	Появление публичного криптолокера Tox Ransomware
11.2015	Шифровальщик Chimera атакует только юридические компании и угрожает опубликовать данные
11.2015	Появление первого шифровальщика для Linux Linux.Encoder
12.2015	На андеграундных форумах появляется множество тем, где злоумышленники обсуждают, что нужно атаковать исключительно юридические лица
02.2016	Старт одной из самых известных и крупнейших партнерских программ Cerber Ransomware
03.2016	Появление первого шифровальщика для MAC OS KeRanger
03.2016	Появление известного шифровальщика Petya с перезаписью MBR
11.2016	Некоторые программы-вымогатели начинают использовать Telegram как C&C
05.2017	Начало атак программ-вымогателей с функцией автораспространения WannaCry
06.2017	Появление программы-вымогателя NotPetya, который продолжил активность WannaCry

Дата	Событие
01.2018	Появление первой современной партнерской программы по программам-вымогателям, нацеленной на юридических лиц GandCrab
03.2019	Появление первой RaaS с техникой double extorsion Snatch
05.2019	Появление вредоносной программы-вымогателя Maze
12.2019	Появление первого DLS (maze)
06.2020	Всплеск появления новых партнерских программ RaaS
05.2021	“No more ransom!” – запрет публикации RaaS на форумах
07.2021	Появление Ramp – форума для Ransomware

Зарождение

2004—2008



PGPcoder, Cryzip, Archiveus

Ретроспективный анализ развития киберимперии вымогателей даст возможность оценить предпосылки к ситуации, с которой бизнес во всем мире столкнулся сегодня, теряя миллионы долларов из-за атак шифровальщиков.

Во-первых, определимся, что именно стоит понимать под расхожим термином «программа-шифровальщик» или «программа-вымогатель». Главной особенностью вредоносной активности этого типа является блокировка доступа к системе или файлам и требование денежного вознаграждения (выкупа) для восстановления этого доступа.

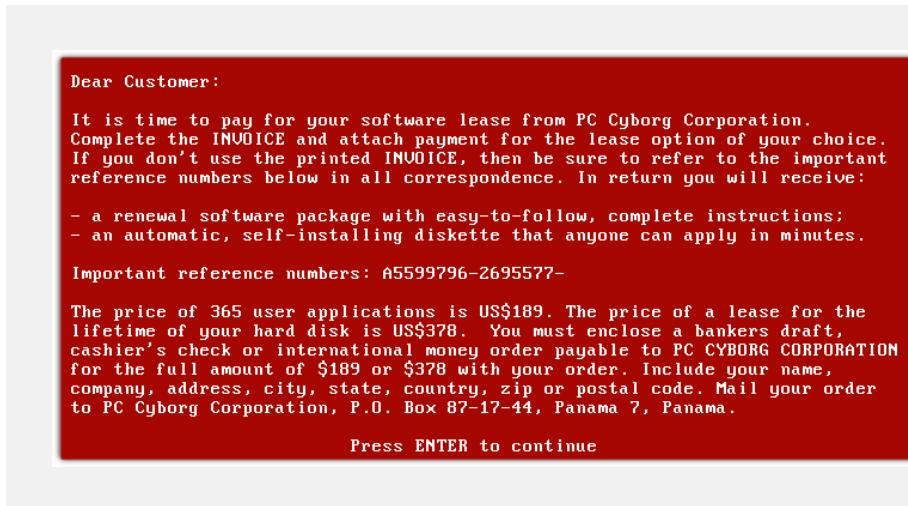
Сама идея требования выкупа позаимствована из другого типа угроз, который был особенно популярен в начале 2000-х — это всем известные DDoS-атаки. В то время злоумышленники высыпали жертвам письма с угрозами совершения DDoS-атаки на их ресурсы и требованием заплатить определенную сумму для того, чтобы этого не произошло. Шантаж приносил довольно неплохие доходы злоумышленникам: бизнес был не готов ни к простоям, ни к отражению подобных атак. Однако с появлением различных CDN-сервисов с интегрированными опциями защиты от DDoS, коммерческий потенциал таких инцидентов снизился. Злоумышленники начали искать новые способы атак с целью вымогательства.

Во-вторых, отметим, что фактически класс ВПО, который мы называем программы-вымогатели, всегда делился на два подтипа: локеры и шифровальщики.

- **Цель локера** — заблокировать доступ к самому устройству, например запретить жертве войти в MS Windows без ввода дополнительного пароля.
- **Цель шифровальщика** — найти и зашифровать ценные данные, которые удалось обнаружить на машине жертвы.

Интересно, что развитие рынка программ-вымогателей началось именно с шифровальщиков, потом все перешло на локеры, а теперь вновь вернулось обратно. Это можно проследить в таблице [выше](#).

В данном отчете мы не будем рассматривать самый первый «прото-шифровальщик» **AIDS Trojan**^[1], который распространялся через диски еще в **1989 году**. Напомним, что именно AIDS, также известный как Aids Info Disk или PC Cyborg Trojan, начал вымогать деньги пользователей, ссылаясь на некое лицензионное соглашение несуществующей корпорации PC Cyborg Corporation, которое необходимо оплатить, иначе AIDS скроет каталоги и зашифрует имена всех файлов на диске C:



Тут и далее можно перейти на страницу «Трояны» с подробным описанием

Рис. 1. Пример прототипа письма вымогателей от авторов AIDS Trojan, 1989 г.

Оставим за скобками семейство фейковых антивирусов типа **Spysheriff**, которые вымогали у пользователя деньги, запугивая заражением компьютера большим количеством вредоносов.

Один из самых первых относительно современных шифровальщиков появился в конце 2004 года. В то время на многих IT-ресурсах пользователи жаловались на то, что они «поймали» какое-то вредоносное ПО, зашифровавшее почти все их важные файлы по алгоритму **CRZ**. На машине каждой из жертв был сгенерирован специальный текстовый файл, который мы сегодня называем Ransom Note. Это сообщение вымогателей, объясняющее, что данные зашифрованы и для их расшифровки необходимо связаться с злоумышленниками по определенным email-адресам. Написав по указанным контактам, жертва получала ссылку на сайт злоумышленников, где можно было купить декодер **за 1000 рублей**. В начале каждого зашифрованного файла была подпись **PGPcoder**^[2], благодаря которому первый шифровальщик получил свое название. Отметим, что данное вредоносное ПО было в основном нацелено на жертв в России.

The screenshot shows a forum post titled 'ВНИМАНИЕ!!!.txt' (Attention!!!.txt). The post was made by 'borech Guest' on 10.12.2004 at 23:37:39. It asks for help with a file named 'ВНИМАНИЕ!!!.txt' that appeared on the user's computer. The user provides their email address (bm7814@yahoo.com) and another (ztc567@mail.ru) for decoding. They mention that many files were encrypted using the CRZ standard. Another user, 'Pig killer Administrator', responded on 11.12.2004 at 18:08:12, stating it's a typical virus and offering to help if the user can't handle it. The user replies that they need help with their files.

Рис. 2. Сообщение пользователя о зашифрованных PGPCoder файлах, 2004

Специалисты Group-IB отмечают несколько вредоносных кампаний с распространением PGPcoder. Одна была в декабре 2004, вторая — в июне 2005. Шифровальщик распространялся через рассылки в формате .DOC документов с вредоносными макросами. В 2006 году разработчик усовершенствовал алгоритм шифрования и перешел на RSA.

Именно PGPcoder положил начало первой волне троянов-шифровальщиков, которая, стартовав в 2004 году, продолжалась вплоть до 2008-го.

По традиции «полигоном» для оттачивания техник атак стала Россия: изначально целями трояна становились жертвы на территории России и постсоветского пространства и лишь затем, спустя 2 года, злоумышленники начали атаковать международные цели.

В марте 2006 появилось новое вредоносное ПО **Cryzip**¹, которое использовало более простую логику для шифрования файлов: архивировало каждый файл в защищенный паролем ZIP-архив и удаляло оригинал. Данное вредоносное ПО имело текстовый файл о выкупе на английском языке. Для разархивирования нужных жертве файлов требовался пароль, а за него злоумышленники просили выкуп. В качестве платежной системы в то время использовалась E-Gold.

После успешных кампаний **Cryzip** схема требования выкупа после шифрования стала популярной на андеграундных форумах.

Cryzip даже называли новым поколением троянов. Например, в июне 2006 на известном андеграундом форуме exploit.in, администратор решил опубликовать гайд, как написать вредоносное ПО на основе Cryzip¹.

¹ <https://forum.exploit.in/topic/3175/?tab=comments#comment-18200>

Рис. 3. Гайд, как шифровать данные трояном, 2006

A Fraud Archivator Engine

Автор: admin, 8 июня 2006 в Статьи & Видео

admin
<forum,status>
•••••

Админ
● 154
 6 913 публикаций
 Регистрация 18.02.2005 (ID: 1)
 Деятельность другое / other

Опубликовано: 8 июня 2006

Fraud Archivator Engine или же Шифруем данные трояном и требуем за них выкуп

0x01| Интро
 Ежедневно компьютерные мошенники проводят различные fraud операции по всему миру. Кража кредитных карт, аккаунтов платежных систем и банков, услуги DDoS, рассыл спама и многое другое. Но далеко не всегда для совершения своих злодейний используют что-то новое. К примеру, рассмотрим кражу кредиток и аккаунтов. Здесь все сводится к одному - либо к взлому online-шопа с кредитками, либо к заражению компьютеров наглых буржуев. По поводу взломов можно говорить чуть ли не вечно, так, что опустим, к тому же тематика статьи другого плана, плана проникновения амеров. Итак, как же воруют кредитки? Чаще всего для этого используются специальное spyware, имена которым формгреберы и тангреберы - это программы, которые перехватывают введенные веб-формы данные. К примеру, ты залогинился в админке своего сайта - тут на твоем компьютере сработал троян и перехватил логин и пароль для админки. Делается это чаще всего через перевызов WinInet API, но мы не об этом. В принципе, ничем формгребер от тангребера не отличаются, просто в тангребере уже прописаны хосты, откуда воровать эти самые данные. Такого типа spyware - пруд пруди. Вообщем, не буду тянуть кота за хвост и расскажу, что мы будем делать сегодня. Сидел я как-то в аське и n4nbit подкинули линк. Заходя на страницу я увидел описание работы нового трояна:

.....// Zippo.A Trojan //.....
 [>>] Троянская программа Zippo шифрует данные и требует у жертвы выкуп.

 Сообщается о троянской программе, которая шифрует данные на ПК пользователя -жертвы и затем пытается получить выкуп в 300 долларов за их восстановление. Этот троян под названием Troj/Zippo-A (также известный и как CryZip), ищет на ПК файлы, такие, как документы Word, базы данных, электронные таблицы, собирает их затем в зашифрованные ZIP-файлы. Собрав и зашифровав таким образом данные, троян создает еще один файл, с помощью которого пострадавший пользователь компьютера узнает, что, чтобы восстановить данные, ему нужно перевести 300 долларов на счет в системе E-Gold.
 Специалисты Sophos, изучив программный код Zippo, установили, что пароль шифрования выглядит как C:\Program Files\Microsoft Visual Studio\VC98
 Похоже, такой пароль был выбран автором троянской программы неслучайно.
 Так вирмейкер пытался провести аналитиков, которые могли принять эту строчку за путь доступа к каталогу.
// Zippo.A Trojan //.....

 Честно говоря, я впервый раз услышал о таком методе и мне стало интересно, как это все работает. А работает все очень просто. Именно отсутствие материалов на эту тему и новизна техники побудило меня написать эту статью. Сразу скажу, что написание и использование таких программ коряется всеми муслыми и немуслыми законами, а статья несет представления из себя лишь ознакомительный материал. Да, кстати. Особых навоков I33t-coding в тебе не понадобится, я все распишу как можно подробнее, начиная с самого автозапуска =). Поехали!

Интерес к ZIP-тロjanу Cryzip привел к появлению похожего ВПО – **Archiveus** (aka MayArchive), который использовал RSA-1024 для шифрования файлов.

Интересно, что в это время на форумах обсуждали, что один из самых сложных моментов такого вредоносного ПО – это получение денежных средств от жертвы, так как в то время еще не было BTC.

До этого подобное вредоносное ПО не появлялось в продаже на андеграундных форумах. Это означает, что либо оно распространялось в приватных сообществах, либо с ним работала только одна преступная группа, которая занималась и разработкой, и распространением.

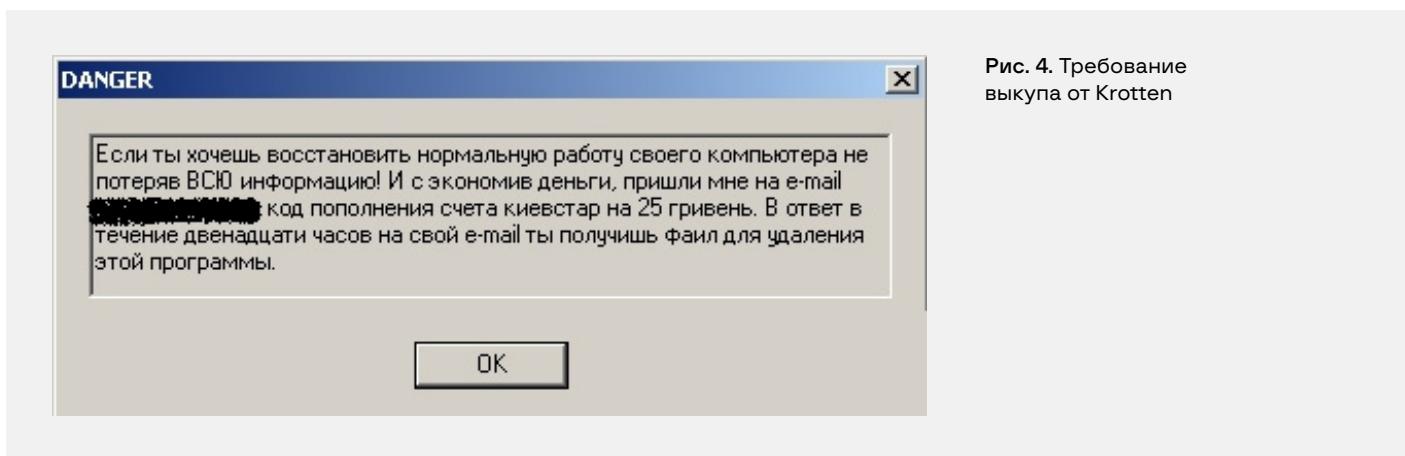
Время локеров, Winlock и первые партнерские программы

2009–2012



Krotten, Winlock

В то время был еще один известный троян **Krotten**^[4]. Он появился чуть позже PGCoder в 2005, однако использовал другую схему вымогательства. Он не зашифровал файлы, но редактировал реестр, приводя к невозможности нормального функционирования системы, а затем выводил сообщение с требованием выкупа. Данный троян можно отнести к типу локеров.



В этом же направлении пошли другие подобные трояны, которые также назывались SMS Lockers. Самым известным их представителем был троян с название **Winlock**^[5] (aka winlocker). До распространения данного вредоносного ПО среди пользователей была популярна программа **Winlock Pro**, которая выполняла похожие действия, а именно блокировала доступ к ОС по истечению определенного периода времени. Это приложение очень часто применялось в компьютерных клубах.

В 2009-м году появилось множество разновидностей подобных троянов, но их суть была одинаковой: они блокировали работу ОС с помощью системных функций, а затем выводили пользователю сообщение, что он может разблокировать свое устройство, заплатив атакующим выкуп. Часть троянов маскировались под баннеры с эротическим контентом, другие сообщали жертвам, что у них на устройстве было обнаружено нелицензионное ПО.

Самое важное в появлении Winlock то, что это было первое вредоносное ПО, которое стали продавать и распространять на андеграундных форумах. Это привело к небывалому всплеску атак с использованием данного трояна.

Впервые Winlock появился в продаже на андеграундных форумах в конце мая 2009 года:

Рис. 5. Сообщение о продаже Winlock, 2009

Столичный отметить, что данный Winlock стоил довольно дешево, учитывая тот факт, что даже исходные коды трояна в 2009 году продавались всего за \$50. Позже на форумах появляется множество запросов на разработку подобных локеров под ключ.

И уже в июле 2009 на форуме exploit.in появляется статья, как написать такой локер самостоятельно:

Рис. 6. Гайд по созданию локера, 2009

Исходя из сообщений на форумах, основной проблемой в то время было поиск подходящего абузоустойчивого биллинга, который готов был бы принимать платные СМС для разблокировки локеров.

Рис. 7. Поиск СМС-биллинга для локера, 2010

The screenshot shows a forum post titled "sms биллинг" (SMS Billing) from 08.01.2010 at 00:00. The post has 3 replies and 5 attachments. It includes a message from "Stark" asking for advice on how to get SMS billing for a WinLocker. The message details section shows Stark's profile and the topic message content.

The screenshot shows a forum post by "K-Frog" titled "sms биллинг" (SMS Billing) from 29 января 2010. The post discusses getting SMS billing for a WinLocker and includes a link to another topic. It also features a reply from "KIDALA" with a red "КИДАЛА" stamp.

Именно Winlocker начал развивать **первые партнерские программы по вымогателям**. Одна из первых партнерских программ по локерам появилась **в январе 2010 года**:

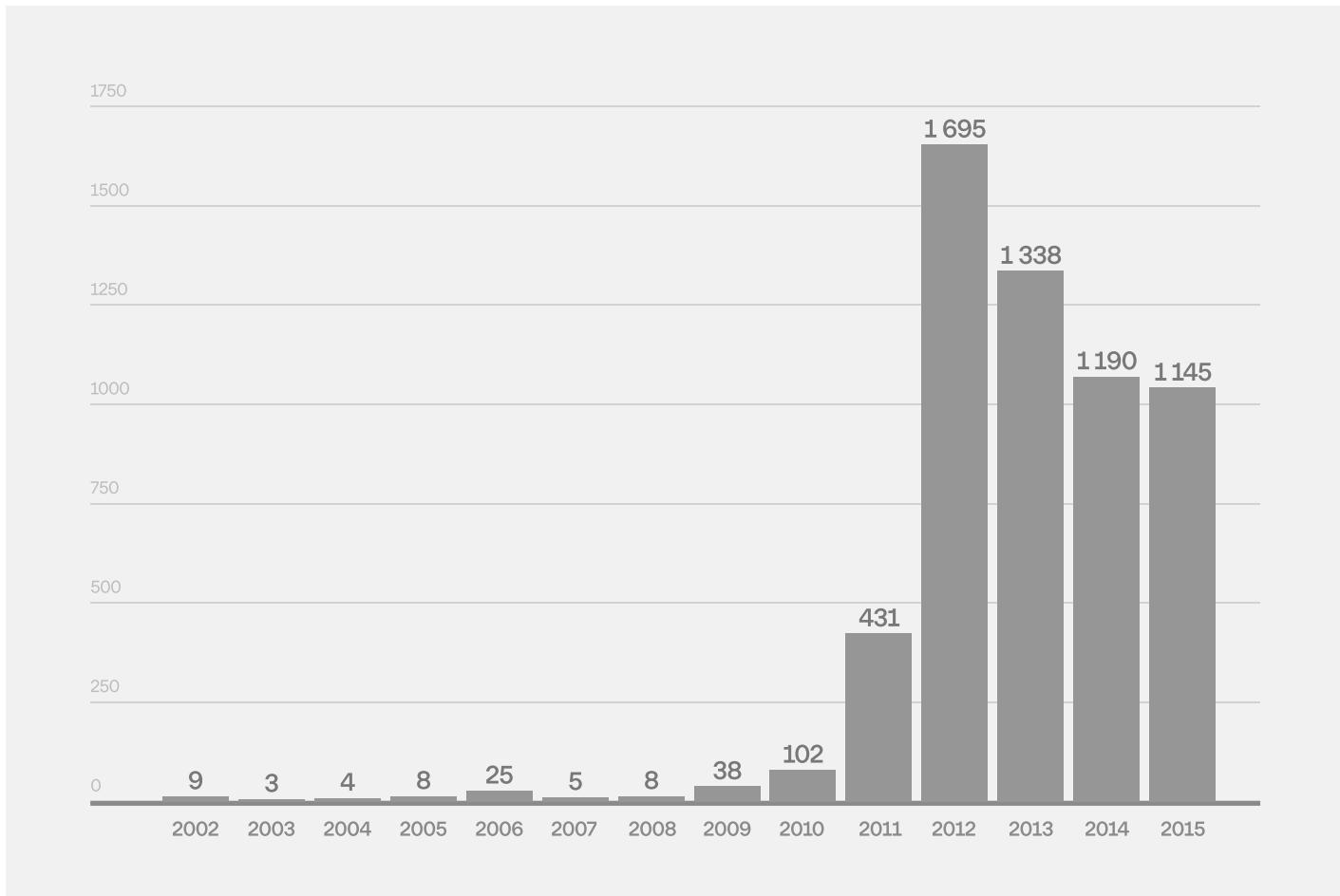
The screenshot shows a forum post by "duh_9" titled "Партнерская программа, смс, адваре" (Partner program, SMS, Adware) from 19 января 2010. The post describes a profit-sharing scheme for lockers and includes a reply from "duh_9" with a red "КИДАЛА" stamp.

Основная идея этих «партнерок» заключалась в том, что участнику выдавался троян, который он должен был распространять среди жертв и получать процент от прибыли за разблокировку, а точнее за отправленные СМС.

Рис. 9. Поиск СМС-биллинга для локера продолжается, 2010

Исходя из анализа сообщений, опубликованных на андеграундных форумах и связанных с обсуждением локеров, была построена следующая гистограмма:

Рис. 10. Гистограмма упоминаний локеров на форумах, 2002 – 2015 гг



На гистограмме очень хорошо видно, что популярность локеров началась с 2009 года, а пик славы пришелся на 2012 год, затем популярность начала спадать. Стоит также отметить, что начиная с 2011 года, локеры стали атаковать не только российский сегмент рынка. Более того, часть партнерских программ стала искать людей исключительно для работы по иностранным странам:

Рис. 11. Поиск людей для партнерской программы, 2012

Сообщение от пользователя **djekh** (11 апреля 2012):

Автор: djekh, 11 апреля 2012 в [Разное] - все остальное

 Просьба верифицировать аккаунт!

 ищу партнеров на локер. могу намутить локер грамотный с статьей и админкой. с вас траф и лоады. я могу налить) страна пофикс ток не ру

 Создать тему Ответить в тему

 djekh Опубликовано: 11 апреля 2012

ищу партнеров на локер. могу намутить локер грамотный с статьей и админкой. с вас траф и лоады. я могу налить) страна пофикс ток не ру

 Жалоба

 Цитата

 djekh Просьба верифицировать аккаунт. Для разбана обратитесь к администрации (для проверки аккаунта на угон).

 // С уважением,
 // администрация

 Деконтирошин 201 публикация

Регистрация 19.03.2011 (ID: 36589)

Деятельность другое

Первые современные шифровальщики и продолжение господства локеров

2011—2013

2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021

Encoder, Ulocker, Reveton, Citadel

Не успела популярность винлокеров сойти на нет, как на андеграундные форумы вернулись трояны, которые позволяли злоумышленникам шифровать данные пользователей и требовать у них выкуп. Наступила эпоха шифровальщиков.

В конце 2010 года на хакерских форумах появился **Encoder**^[6] (aka xorist), который стал первым известным трояном, работающим по этой схеме.

Рис. 12. Описание трояна xorist, 2010

Parallel Forum of VaZoNeZ » Phorum » P :: Diabolic » **Encoder Builder [bin + src]**

Страницы: [1] 2 3 « предыдущая тема следующая тема » ПЕЧАТЬ

Автор Тема: **Encoder Builder [bin + src]** (Прочитано 1314 раз)

0 Пользователей и 1 Гость просматривают эту тему.

vazonez
Администратор
[1000:0000:0000h]

Encoder Builder [bin + src]
« : 05 Декабрь 2010, 23:20:23 »

Собственно, энкодер, он же xorist. Шифрует выбранные файлы и просит деньги (или что еще захотите) за восстановление данных. В комплекте: сорцы и бинарники энкодера и его билдера.

Особенности:
Шифрование файлов с помощью XOR и TEA
Конфигурация расширений файлов, которые нужно обрабатывать
Куча всяких разных настроек, вроде количества попыток ввода пароля (см. скрин)
Сам энкодер написан на masm'e
Размер готового билда - 10.5 КБ, а после UPX'a - всего 6.5
Пароль для декрипта не хранится в открытом виде, в билде хранится его MD5x5-хеш.

Скрин:

Линк на сайте:
Вам запрещено просматривать ссылки. Зарегистрируйтесь или Войдите

Прямой линк на софт:
Вам запрещено просматривать ссылки. Зарегистрируйтесь или Войдите : vazonez

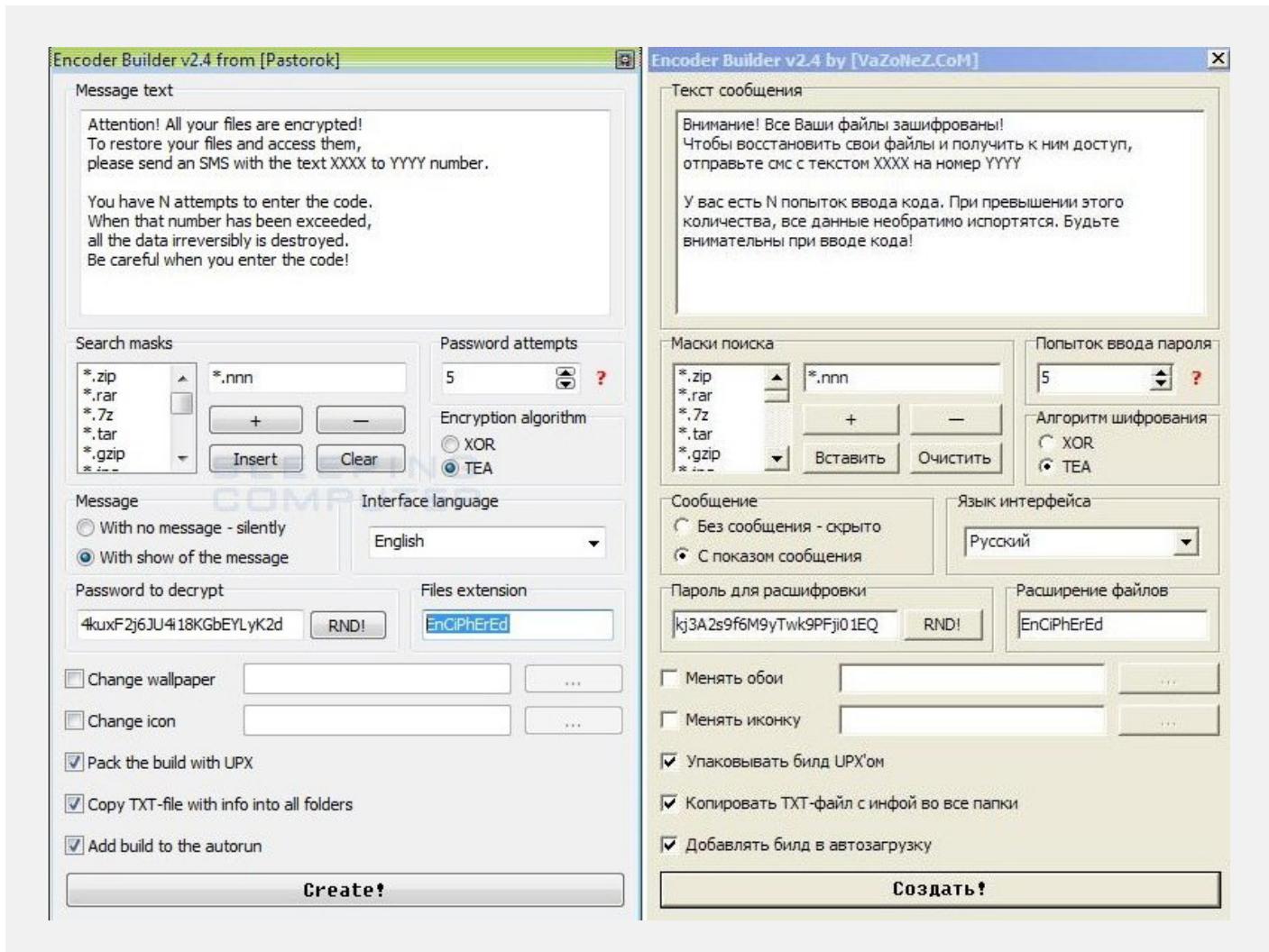
Информация должна быть свободной :) Заставим спермских и въебовцев работать, пусть делают свои никчёмные декодеры. Достаточно изменить в сорце совсем немного - и все они уйдут лесом ;)
« Последнее редактирование: 25 Декабрь 2010, 13:52:47 от vazonez »

You know what you are. What you're made of. Code is in your blood. Don't fight it. You didn't code for your country. You coded for yourself. God's never gonna make that go away. When you're pushed, coding's as easy as breathing.

Разработчиком данного трояна был хакер под псевдонимом **VaZoNeZ**.

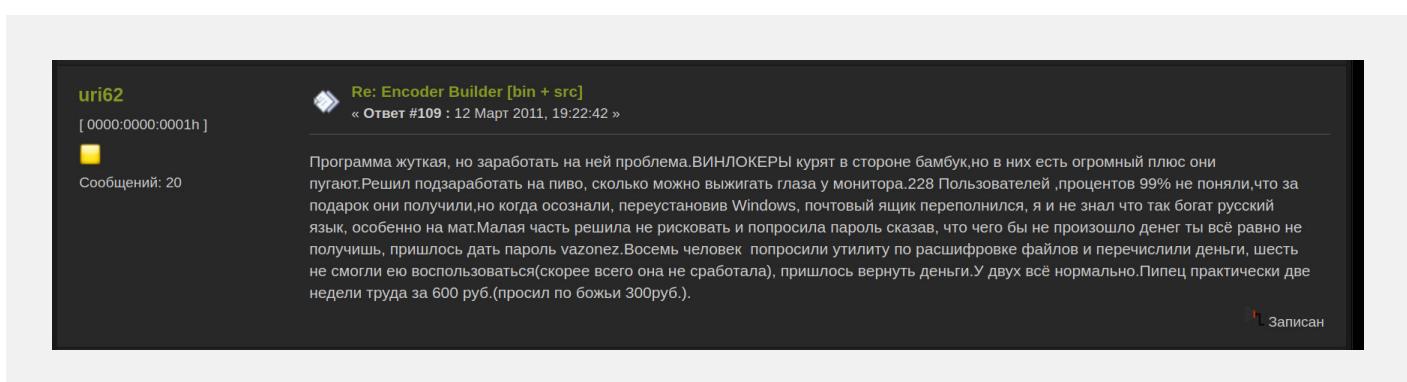
Автор трояна выложил не только исходные коды вредоносного ПО, но и билдер, что позволяло пользователям автоматически генерить вредоносные сэмплы со своими настройками.

Рис. 13. Билдер трояна Encoder, 2010



Что интересно, злоумышленники, которые тестировали данное ПО, считали, что у него слишком низкая конвертация.

Рис. 14. Жалобы на низкую конвертацию Encoder, 2011



Изначально проблема заключалась в том, что жертвы не совсем понимали, что именно произошло, а также как именно работать с декодером.

Локеры и шифровальщики поначалу были крайне не популярны среди злоумышленников. Последние считали, что этот тип ВПО привлекает слишком много внимания. Второй проблемой в то время оставался вопрос, куда именно надо принимать денежные средства.

AluAdib
Прошу верифицировать
аккаунт!


Деятельность
120
1.235 публикаций
Регистрация
16.03.2009 (ID: 19 114)
Деятельность
другое

Опубликовано: 16 декабря 2010
Трои, формграббери, стиллеры и т.д. это в некотором роде пассивный софт, но стянут пароль от почты пользователь вернет и не особо пострадает не морально, не материально а софт типа рэндом шиффаторы и блокаторы это агрессивный софт требующий активного участия пользователя и вопрос всегда ставиться ребром, тут всегда будут проблемы, пользователи будут активно жаловаться и разбираться.

Цитата
Поймают и оторвут башку, у этого вида мошенничества хороший показатель раскрываемости дел в РУ насколько позволяет судить интернет-пресса.
да, да и это тоже.

Цитата

Рис. 15. Обсуждение, куда принимать доход от локеров, 2010

Quake3
генератор Эла


Модератор
1460
2 166 публикаций
Регистрация
01.09.2010 (ID: 32 399)
Деятельность
кодинг / софт
депозит
0.983721 B

Опубликовано: 17 декабря 2010
AluAdib, exirkin, понятно все.. Ну тогда можно использовать софт для единичной мести кому-нибудь, или просто для изучения асма. Интересно, а если заказать загрузки по другим странам, скажем Германия или еще где, риск что поймавт умешится?
Тут, по моему, огромный минус один - куда принимать деньги. Платежи маленькие - т.е. WU и прочее не покатят, возникнут подозрения; вебмани не у всех есть, а смс биллинги - не очень надежно + большой риск что поймают + иностранные тяжело найти.

Цитата
а расшифровывать уже пробовал... работает?
да, попробовал - все отлично работает, шифрут и расшифровывает.

Цитата
[Не работают ни по каким темам!](#) (на заках не пишу, малварь не продаду, никого не знаю кто пишет/продает)

Рис. 16. Обсуждение, куда принимать доход от локеров, 2010

В июле 2011 пользователь **Galahem** начал продажи доработанного шифровальщика.

Galahem
Прошу верифицировать
аккаунт!
•

Деятельность
10 публикаций
Регистрация
14.07.2011 (ID: 28 659)
Деятельность
другое

Опубликовано: 21 июля 2011 (изменено)
Доброго времени суток форумчиче!
Продам шифровальщика файлов (энкодер).

Что это такое? Это маленькая программа, которая запустившись, на компьютере жертвы, начинает искать файлы жертвы по популярным маскам расширений (doc, gif, zip и тд) и шифровать их, пусть не уникальным, но надежным способом. После всех этих действий выдвигает требование жертвы о выкупе его файлов.

Особенности продукта:

- 1) Расшифровать нельзя, не зная пароля заданного при шифровке, невозможно, разве только перебором.
- 2) Работает под всеми популярными ОС семейства microsoft (XP Vista, 7)
- 3) Пока не обходит UAC, но при первом же запуске успешно отключает его.
- 4) Генерирует случайную строку загрузки на 32 байта, для увеличения плавающих ресурсов, с которых грузится энкодер.
- 5) Состоит из двух частей, криптор и декротор. После криптования криптор самоподвигается. Это повышает надежность того, что ваш криптор не скроется и не вытащат пароль (так или иначе, пароль хранится в хэше).
- 6) После себя оставляет очи зашифрованных файлов, сино с требованием, которое выполняет каждые 15 минут и текстовый файл на рабочем столе, с тем же текстом что и в окне, на случай, если AD или жертва снесет недородливое окно.
- 7) Помимо манипуляций с файлами, подсчитывает их и отдает данные в мини админку.
- 8) Имеется мини админка, в которой отображаются: время, IP, страна и количество зашифрованных файлов. (отступ в админку разовый, в случае недоступности интернета на момент попытки отступа, повторного отступа не будет).
- 9) 50 масок расширений по которым идет поиск файлов для шифровки.
- 10) Вес бинара 5765.
- 11) Повторно не запускается в виде, на которой уже побывала.
- 12) Написан на c++ и Windows API

Поставляется с админкой и декротором под ваш билд.

От вас нужен текст не более 2,5 тысяч символов вместе с проблемами. Урл где будет лежать админка и желаемый пароль, не более 100 символов. Сам файл палится AB, но можно криптовать (жалательно упаковщиком). Могу дать контакт человека который криптует. Процесс не палится, и не будет палится, так как используются родные средства Windows.

Стоимость билда 50\$.

Рис. 17. Продажа шифровальщика, 2011

Популярностью данное ВПО не пользовалось. Судя по сообщениям на андеграундных форумах, злоумышленники продолжали интересоваться исключительно винлокерами, потому что их было проще монетизировать, в том числе, благодаря партнерским программам. Для приема платежей злоумышленники начали использовать **Ukash** и ваучеры **Paysafecard**. Новые винлокеры работали по огромному количеству стран, но не работали «по ру» — то есть по России и СНГ. Уже в то время появилась практика не работать по этим странам для минимизации риска быть обнаруженными.

Например, в июле 2012 появился новый локер под названием **Ulocker**¹⁷. Исходя из описания, он работал по следующим странам:



This screenshot shows a forum post from a Russian-speaking community. The post is titled "ULocker" and discusses a new ransomware variant. It includes a link to a file sharing site where the malware's source code is available. The post lists various features of the ransomware, such as file encryption, system keylogging, and the ability to change language settings. It also mentions the use of the Ukash payment method. The post is dated November 11, 2011, and has received several replies.

Рис. 18. Сообщение о появлении Ulocker, 2011

Также у Ulocker'а были очень продвинутые лендинги, которые позволяли отображать изображение с веб-камеры, перехваченное вредоносным ПО.

This screenshot shows a sophisticated ransomware landing page. At the top, it features the International Police Association - IAC logo and a message stating that all activity on the computer is recorded. Below this is a large image of the European Union flag. A prominent green banner at the bottom left displays a warning message: "Your Computer has been hacked". The main content area contains a live video feed from a victim's webcam, showing a view of a car's interior. To the right of the video, there is a payment interface for Ukash, with options for 50 or 100 Euro. A note specifies that payment must be made within 48 hours. The page also includes a "Please note" section about the fine and a "Please note" about the stored photo for identification.

Рис. 19. Сообщение о появлении Ulocker, 2011



Рис. 20. Сообщение Ulocker о требовании оплаты за разблокировку, 2012.

В 2012 году некоторые локеры стали использовать новую тактику: они перезаписывали Master Boot Record (MBR), что в итоге приводило к тому, что жертва не могла запустить даже операционную систему.

В то же время появляется еще один один известный локер **Reveton**. Он тоже блокировал операционную систему жертвы и требовал выплатить штраф в размере \$100. Лендинг был выполнен в виде требования Министерства юстиции США. Распространялся он через известное в то время вредоносное ПО **Citadel**^[8].

Из-за популярности Citadel, многие злоумышленники подгружали его к своей полезной нагрузке в зараженные машины.

Старый шифровальщик **GPCode** также продолжал развиваться, но его жертвами по-прежнему оставались обычные физические лица.

Со второй половины 2012 начались изменения. Жертвами атак шифровальщиков стали четыре австралийских компании:

Компания	Когда атаковали	Сумма выкупа	Отрасль
TDC Refrigeration and Electrical	Сентябрь 2012	3000	Производство
Byron Community Primary School	Октябрь 2012	5000	Образование
Deanes Buslines	Ноябрь 2012	3000	Перевозки
Gold Coast medical centre	Декабрь 2012	4000	Здравоохранение

Злоумышленники просили за расшифровку данных крайне небольшие денежные суммы по сравнению с текущими цифрами. Однако именно в 2012 году стало ясно, что атаки на бизнес могут быть гораздо более эффективными, чем атаки на физические лица. Также злоумышленники заметили, что обычные локеры перестали приносить прибыль и что пора переходить на криптолокеры. В конце 2013 года известный пользователь upO написал следующее:

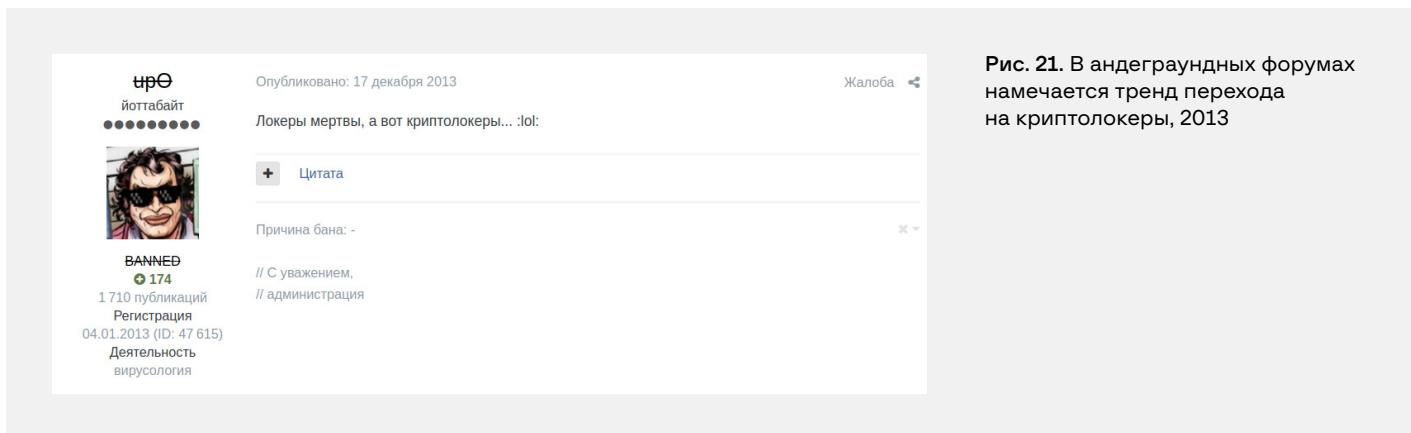
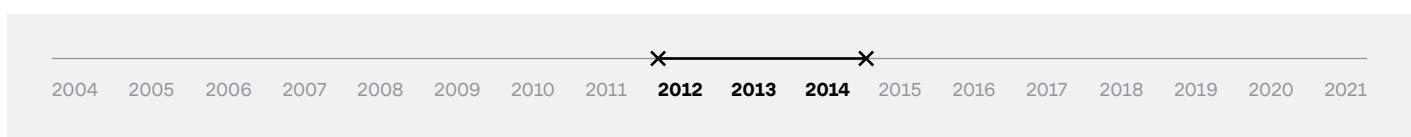


Рис. 21. В андеграундных форумах намечается тренд перехода на криптолокеры, 2013

Появление партнерских программ по шифровальщикам, партнерская программа и автор CryptoLocker

2012—2014



Одна из первых партнерских программ по локерам, связанная с шифрованием файлов, появилась в июне 2013 года на форуме antichat:

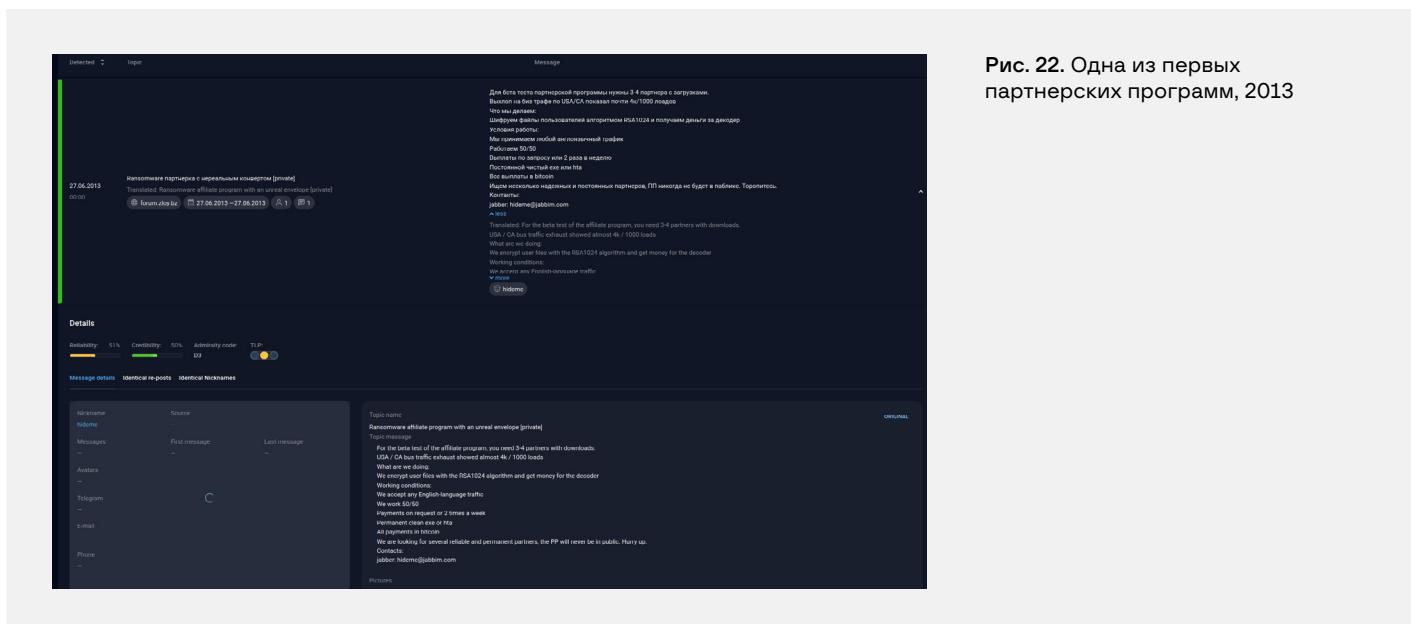


Рис. 22. Одна из первых партнерских программ, 2013

Как видно из описания, локер шифровал файлы по алгоритму RSA1024, а разработчики работали по схеме 50/50. К сожалению, ни названия, ни отзывов к данной партнерской программе обнаружено не было.

В сентябре 2013 появился один из самых известных шифровальщиков в то время с названием **CryptoLocker**¹⁹. Сейчас его название превратилось в устойчивый термин и используется для любого вредоносного ПО подобного типа, однако ранее их называли либо «локерами», либо «шифровальщиками», а также «вымогателями» или ransomware (без перевода на русский язык).

Первое упоминание этого термина появилось за полгода до известных атак на андеграундном форуме exploit:

The screenshot shows a forum post by user **max270** from March 26, 2013, in the [Работа] - поиск, выполнение работ category. The post title is "требуется кодер для написания локера" (A coder is needed to write a locker). The post content asks for a programmer with experience in writing cryptolockers, mentioning further support and development. The user's profile shows they are deactivated and have 14 publications. The post has 0 comments and 0 likes.

Рис. 23. Сообщение о поиске программиста, способного написать «локер», 2013

Как видно из данного скриншота, пользователь форума **max270** (aka max2 aka nyservol) искал людей для разработки криптологора с дальнейшей поддержкой. Если изучать последующие сообщения данного злоумышленника, то можно заметить, что в конце августа он сообщил, что у него резко увеличились объемы, связанные с обналичиванием денежных средств.

The screenshot shows a forum post by user **max270** from August 30, 2013, in the [Финансы] - биллинги, банки, акции, логи category. The post title is "МП инстантом 60-65, предоставлю гарантии." (MP instant 60-65, I will provide guarantees). The post content discusses increasing withdrawal volumes and mentions netted@jabbitm.cz. The user's profile shows they are deactivated and have 14 publications. The post has 0 comments and 0 likes.

Рис. 24. Сообщение об увеличении объемов обналичивания денег, 2013

В сентябре 2013 года на нескольких форумах публикуются предложения с новой партнерской программой, связанной с локером.

Ждем партнера с адапт трафом ЮС для локера

Автор: max270, 10 сентября 2013 в [Трафик] - трафик, загрузки, инсталлы, iframe

Создать тему Ответить в тему

max270
Прошу верифицировать аккаунт!

Опубликовано: 10 сентября 2013 Жалоба

Ваши 20% от грязного выхлопа в админке локера. т.е все зависит от качества вашего трафика, но не менее 30\$ с 1000 уникальных пользователей. Пусть с 1000 уникальных мы имеем 50 инсталлов, то получается около 50\$ вашей прибыли. Мы можем это себе позволить, т.к мы сами обналичиваем чеки в течение часа после потери % комиссии. Ваша выплата ежедневно. Доступ и отчет с админки по договоренности с каждым. Ищется 2-3 человека с нормальными потоками. Рассмотрим любые предложения. Рега на всех приватных форумах присутствует.

Deactivated ● 0
14 публикаций
Регистрация 09.07.2009 (ID: 22 507)
Деятельность другое

netted@jabbim.cz
+ Цитата

Прошу верифицировать аккаунт. Для разбана обратитесь к администрации (для проверки аккаунта на угон).
// С уважением,
// администрация

Рис. 25. Объявление о новой партнерской программе, 2013

Исходя из публичных исследований, кампания по распространению трояна CryptoLocker началась 5 сентября 2013 года, что позволяет предположить, что данная партнерская программа относится именно к этому вредоносному ПО.

Само окно трояна после заражения выглядело следующим образом:

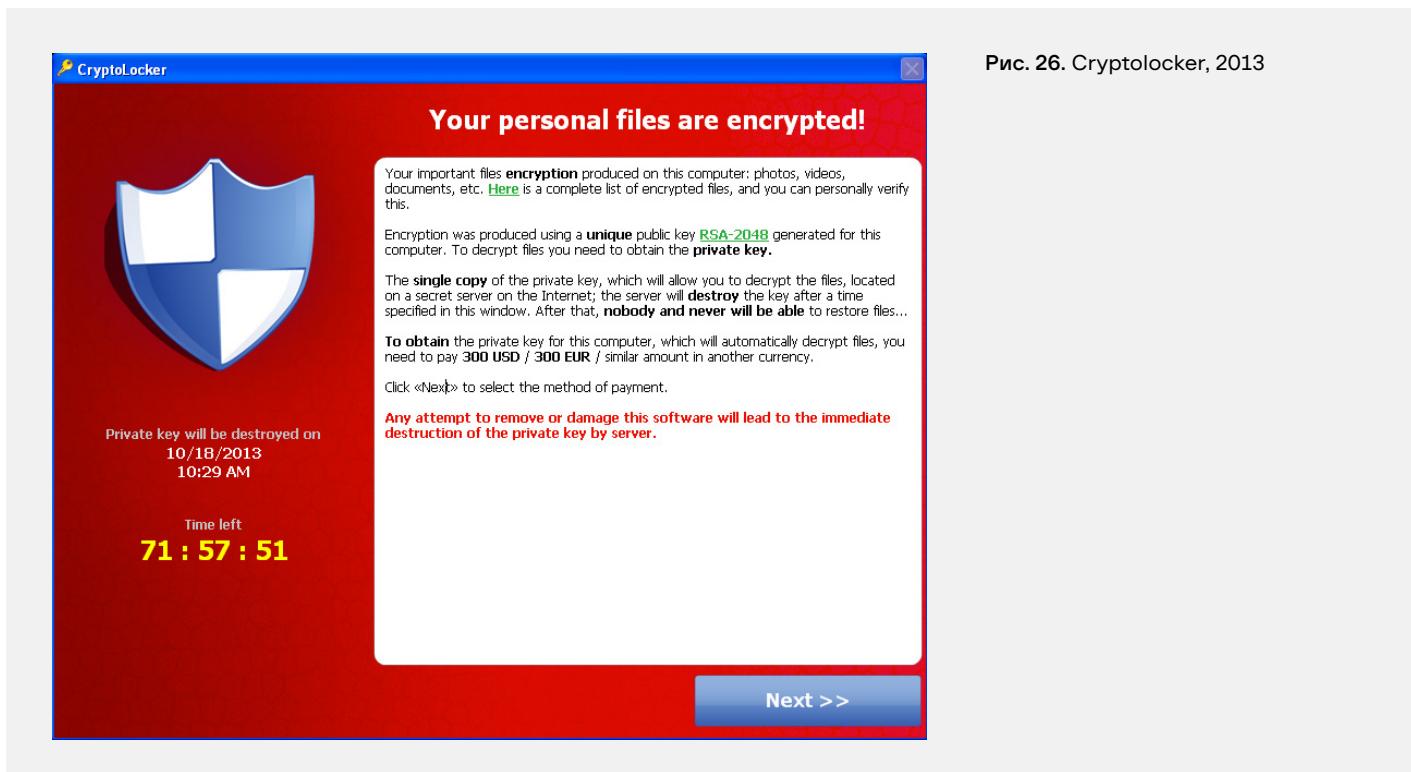


Рис. 26. Cryptolocker, 2013

Затем оно позволяло выбрать различные способы оплаты:

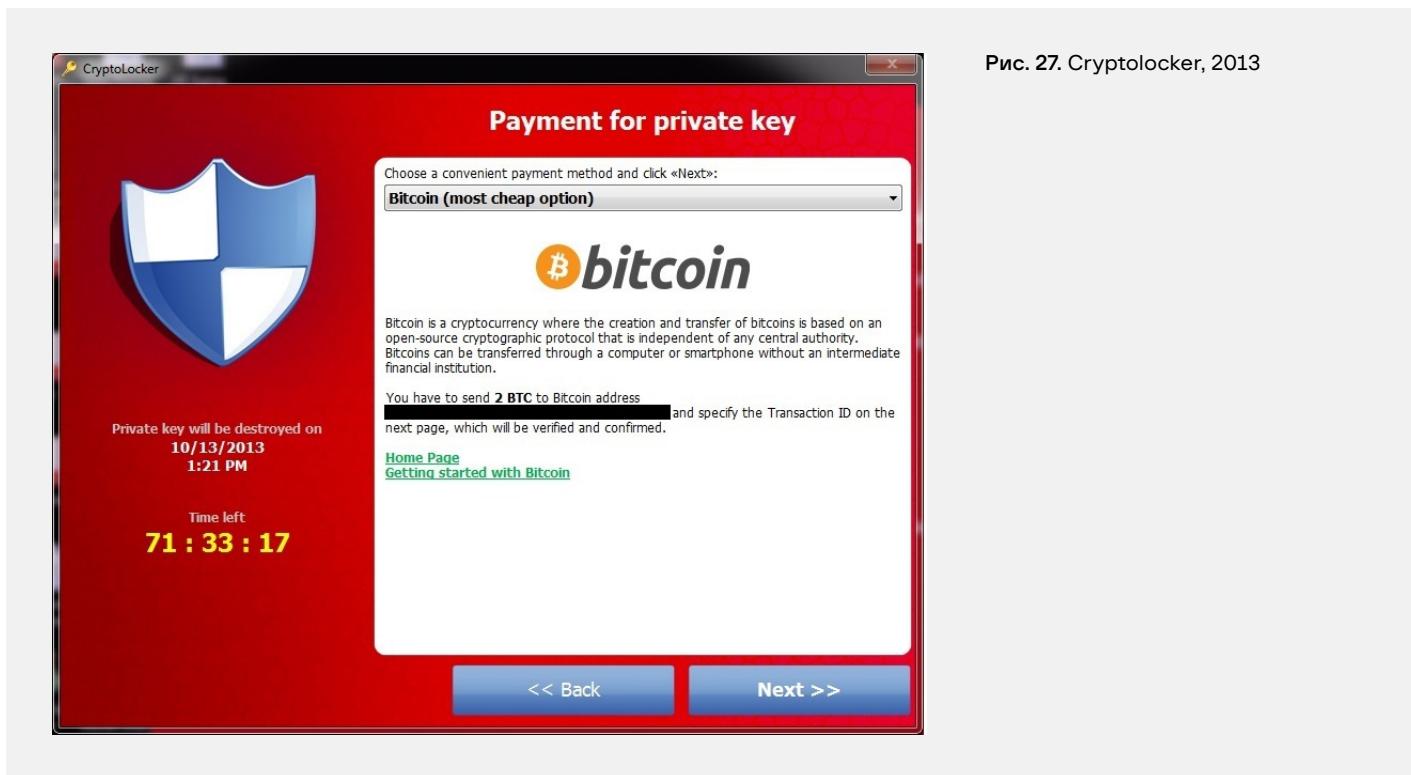


Рис. 27. Cryptolocker, 2013

Cryptolocker был одним из первых шифровальщиков, который заразил огромное количество жертв за крайне небольшой период. По словам исследователей, к середине декабря 2013 (за 3 месяца) было заражено больше 200 000 машин. Данный шифровальщик был активен до мая 2014 года, когда он был изолирован в ходе операции Tovar, был получен доступ к секретным ключам для шифрования и выпущено специальное ПО для расшифровки файлов без оплаты. Считается, что за все время участники партнерской программы заработали около \$3 000 000.

Развитие направления RaaS, смена фокуса на бизнес, угроза публикации файлов

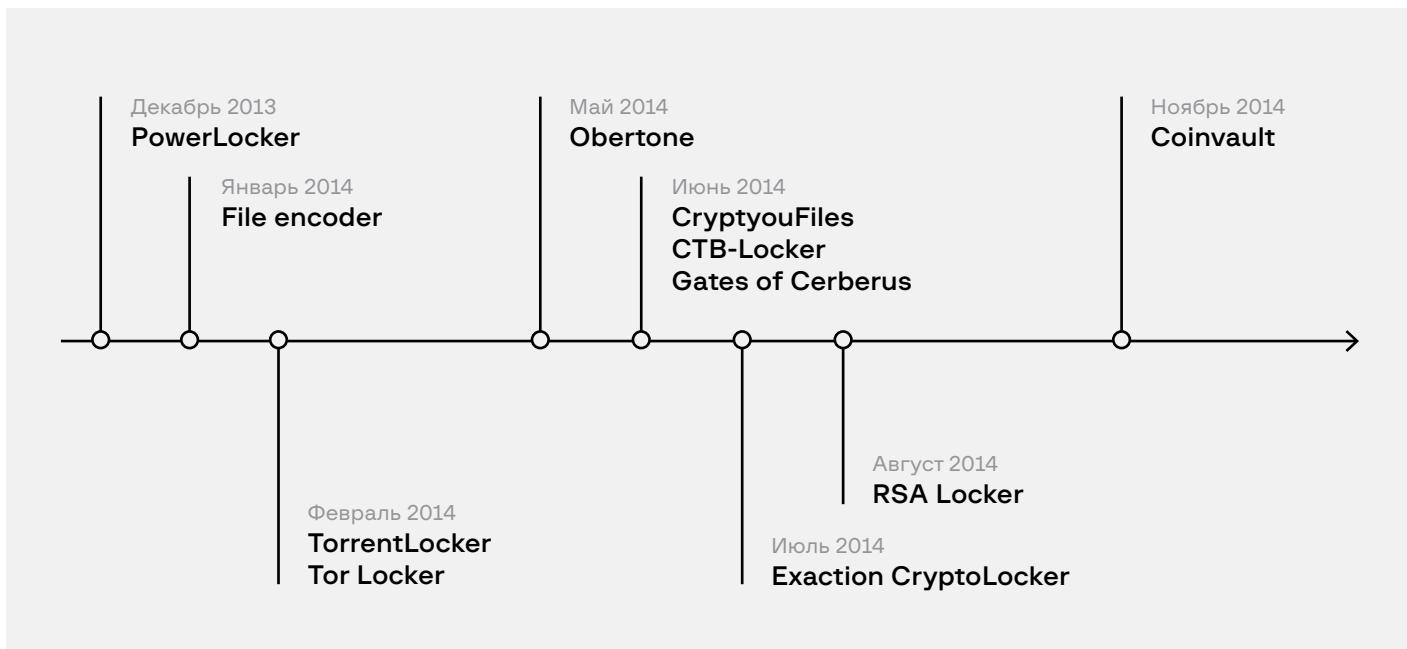
2014–2016



TorrentLocker, VaultCrypt, Tox Ransomware, LowLevel04, Chimera, Linux.Encoder, CryptoWall

Популярность шифровальщика Cryptolocker привела к тому, что на форумах увеличилось количество злоумышленников, которые продают различные версии вредоносного ПО с функцией шифрования файлов.

Трояны с функцией шифрования файлов, 2013-2014



Все эти трояны предлагались на различных андеграундных форумах. В основном они работали не по партнерской программе, а злоумышленники просто продавали билды трояна или подписку.

Самым распространенным криптолокером за 2014 год был признан **TorrentLocker^[10]**. По итогам 2014 его владельцы заработали около \$500 000.

Развитие обычных локеров тоже несколько видоизменяется – злоумышленники начинают продавать локеры для мобильных телефонов.

В феврале 2015 года начинается активность шифровальщика **VaultCrypt^[11]**. В основном кампания с ним была ориентирована на русскоязычных пользователей. В марте 2015 запускается полноценная партнерская программа по данному шифровальщику. Её стоит выделить отдельно, так как данное предложение уже очень похоже на современные партнерские программы.

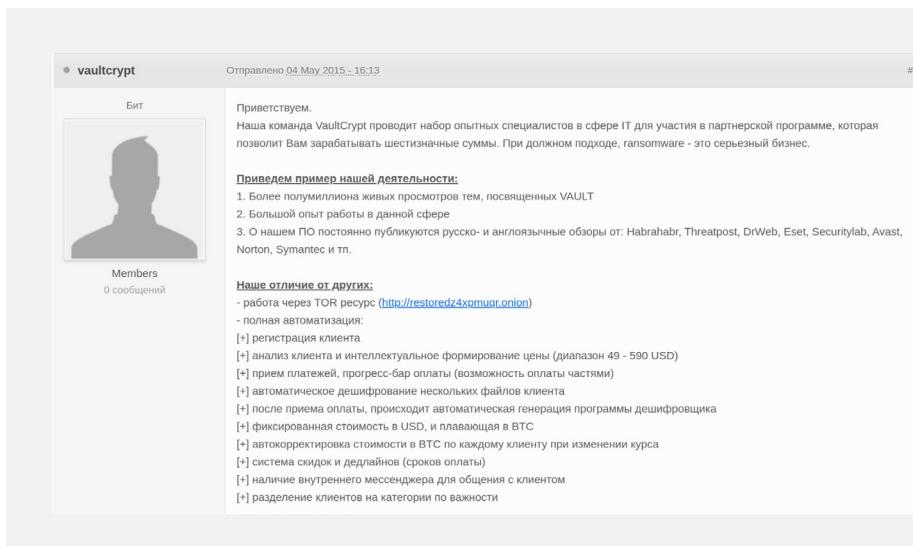


Рис. 28. Сообщение о партнерской программе VaultCrypt, 2015

Отдельно стоит отметить появление **Tox Ransomware** в мае 2015 года. По факту данная партнерская программа представляла онлайн-конструктор ВПО, доступный на определенном сайте в .onion.

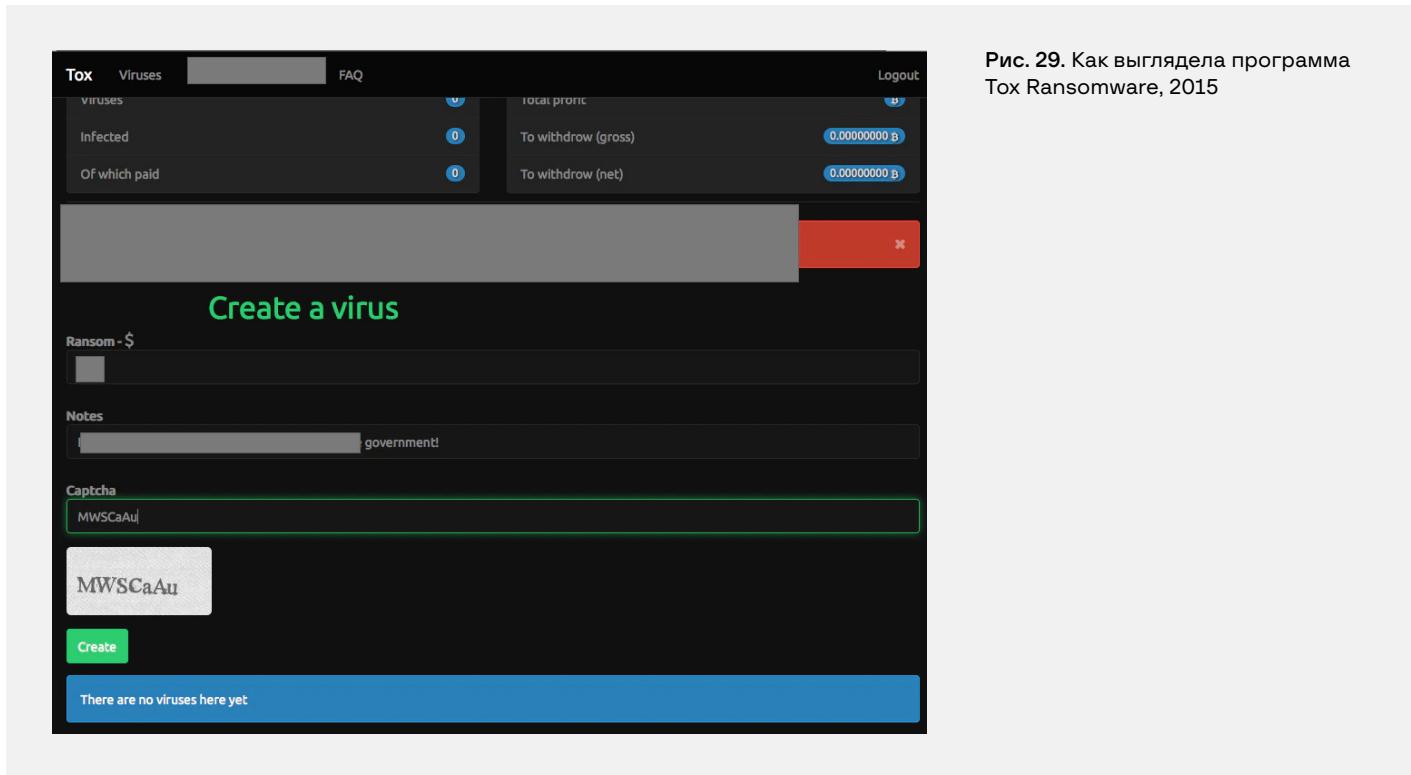


Рис. 29. Как выглядела программа Tox Ransomware, 2015

Любой пользователь мог сгенерировать себе сэмпл шифровальщика на данном сайте, указать сумму денежных средств для расшифровки и использовать его для получения прибыли.

Некоторые партнерские программы работали в привате, то есть они не имели объявления о наборе партнеров на андеграундных ресурсах. Однако периодически даже они появлялись на форумах, чтобы набрать новых людей в свои команды. Пример такой приватной партнерской программы был размещен в октябре 2015 года на форуме verified. И снова в явном виде прописано, что партнерская программа не предназначена для работы в России и странах СНГ:

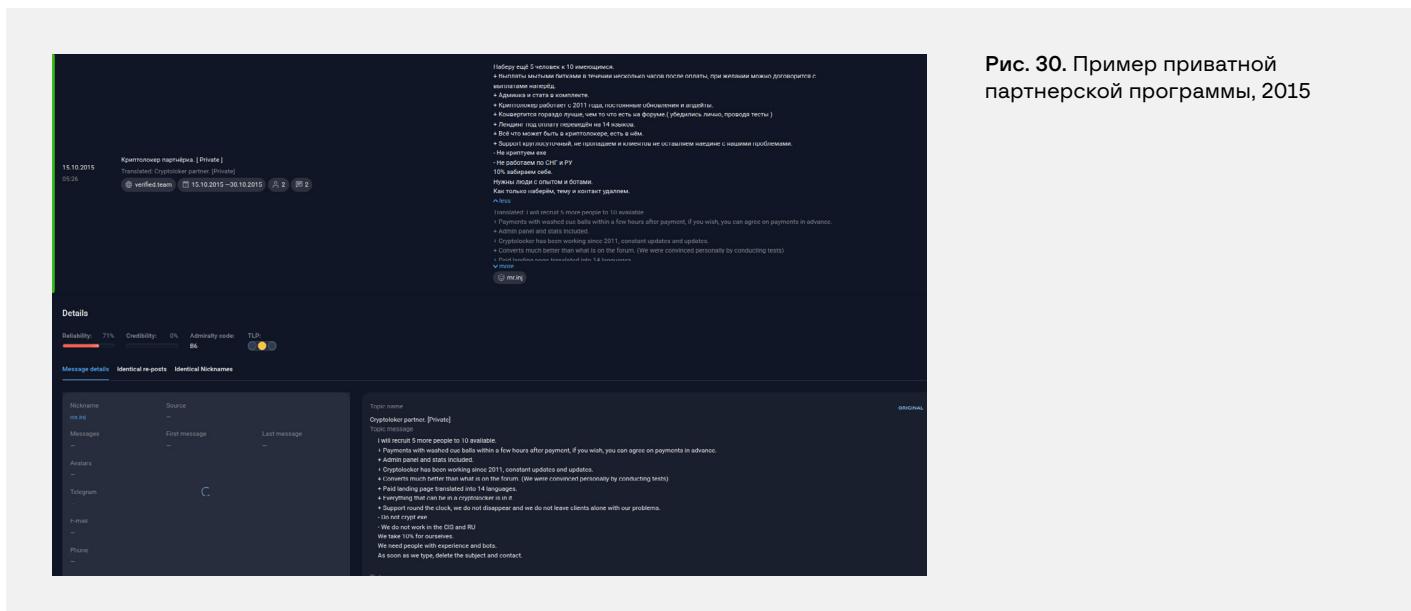


Рис. 30. Пример приватной партнерской программы, 2015

По словам автора, его партнерская программа работала еще с 2011 года. Однако учитывая то, что он заинтересовался криптолокерами только в 2014 году, его заявление выглядело как минимум сомнительно. Тем не менее, видно, что RaaS начинает набирать обороты.

В мае 2015 произошла довольно крупная атака шифровальщиков: компьютеры Министерства юстиции Вьетнама были заражены вредоносным ПО. Сумма выкупа названа не была. Однако в октябре 2015 года была зафиксирована атака на школьную компьютерную сеть Нью-Джерси, и тут злоумышленники требовали порядка \$124 000, что уже начинает напоминать текущие расценки известных групп, атакующих с помощью программ-вымогателей.

В октябре 2015 некоторые пользователи стали жаловаться на то, что их сервера под управлением Windows Server стали жертвами некоего вредоносного ПО **LowLevel04**. Тогда стало очевидно, что некоторые преступные группы начинали использовать современные тактики атак. В данном случае речь шла о брутфорс атаках на RDP. С этого момента жертвами шифровальщиков все чаще становятся юридические лица.

Отдельно стоит отметить шифровальщик **Chimera**^[12], который появился в ноябре 2015 года. У него было две отличительные особенности: с его помощью атаковали исключительно юридические лица и угрожали жертвам публикацией зашифрованных данных в открытом доступе.

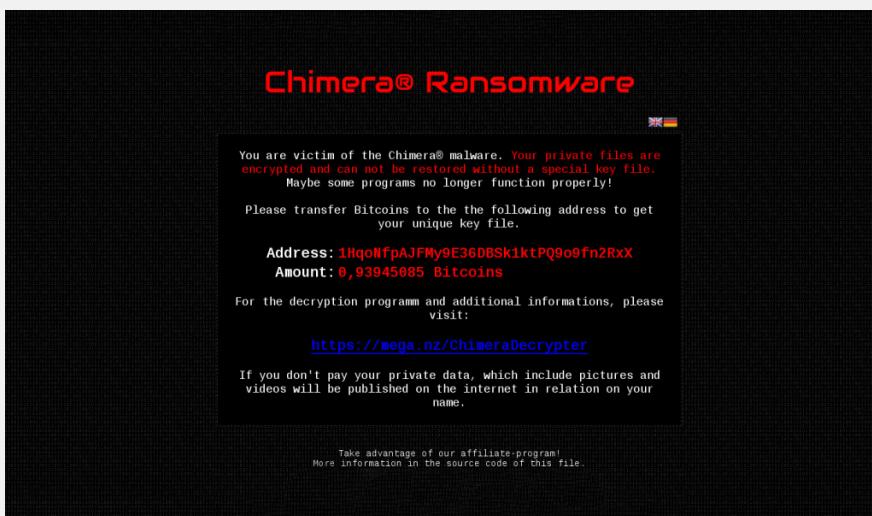


Рис. 31. Угроза публикации данных от Chimera, 2015

При этом злоумышленники не выполняли угрозу и не публиковали данные, но эту технику позже взяли на вооружение все современные группы операторов программ-вымогателей.

В ноябре 2015 также появляется шифровальщик, нацеленный на систему под управление Linux – **Linux.Encoder**. Основной его целью являются именно серверы под управлением Linux, которые скорее всего принадлежат компаниям, а не частным лицам.

Самым известным шифровальщиком за 2015 год стало вредоносное ПО под названием **CryptoWall**^[13]. Впервые его обнаружили еще весной 2014. По подсчетам экспертов за 2014 год, злоумышленники заработали \$18 000 000, а за 2015 – \$325 000 000.

Любопытно, что у них не было публичной партнерской программы, а за программу отвечала одна группировка – судя по использованию одних и тех же Bitcoin-кошельков.

2015 год становится переломным для развития шифровальщиков – фокус злоумышленников все чаще смещается в сторону бизнеса. Финансово мотивированные группы начинают осознавать, что атаковать юридические лица значительно выгоднее. Подобные обсуждения можно найти на андеграундных форумах:

mipse1
терабайт
•••••
M
Пользователь
0 34
210 публикаций
Регистрация
15.03.2015 (ID: 60 282)
Деятельность
кодинг

Опубликовано: 21 декабря 2015
ИМХО локер надо по юркам всяким отшугать, с них и просить можно куда больше. А обычным людям шифровать фоточки как-то низко.

+ Цитата

Ничего не продаю и не покупаю.

Рис. 32. Пример обсуждения с форума о выгоде атак на юридических лиц вместо пользователей, 2015

Дальнейшая популяризация вымогателей, WannaCry

2016—2018



Cerber Ransomware, KeRanger, Petya, Mischa, Satana, ZCryptor, CTB-Locker, Locky, TeslaCrypt

Как уже было сказано выше, в конце 2015 года злоумышленники переключились на атаки компаний. Это постоянно обсуждалось на форумах:

Syndicates
пятый
•••••
S
ЧАШНИК
0 11
470 публикаций
Регистрация
03.04.2014 (ID: 51 635)
Деятельность
безопасность

Опубликовано: 29 декабря 2015
Подскажите пожалуйста, где лучше конвертится криптолокер, в каких странах, какой сумму лучше просить и т.д.

+ Цитата

Причина баня: по собственному желанию.
// С уважением,
// администрация

RIPPER
•••••
RIPPER
0 95
490 публикаций
Регистрация
11.03.2015 (ID: 60 207)
Деятельность
безопасность

Опубликовано: 7 января 2016
таргет заражения юриков. просить \$ в зависимости от важности доков/файлов на зараженных машинах. на мой взгляд, это самый логичный вариант

+ Цитата

Блок: <https://forum.exploit.in/index.php?showtopic=105603>
// С уважением,
// администрация

Рис. 33. Пример обсуждения об использовании локера в отношении компаний, 2015

Злоумышленники начали собирать email-адреса различных корпораций и государственных учреждений для проведения атак:

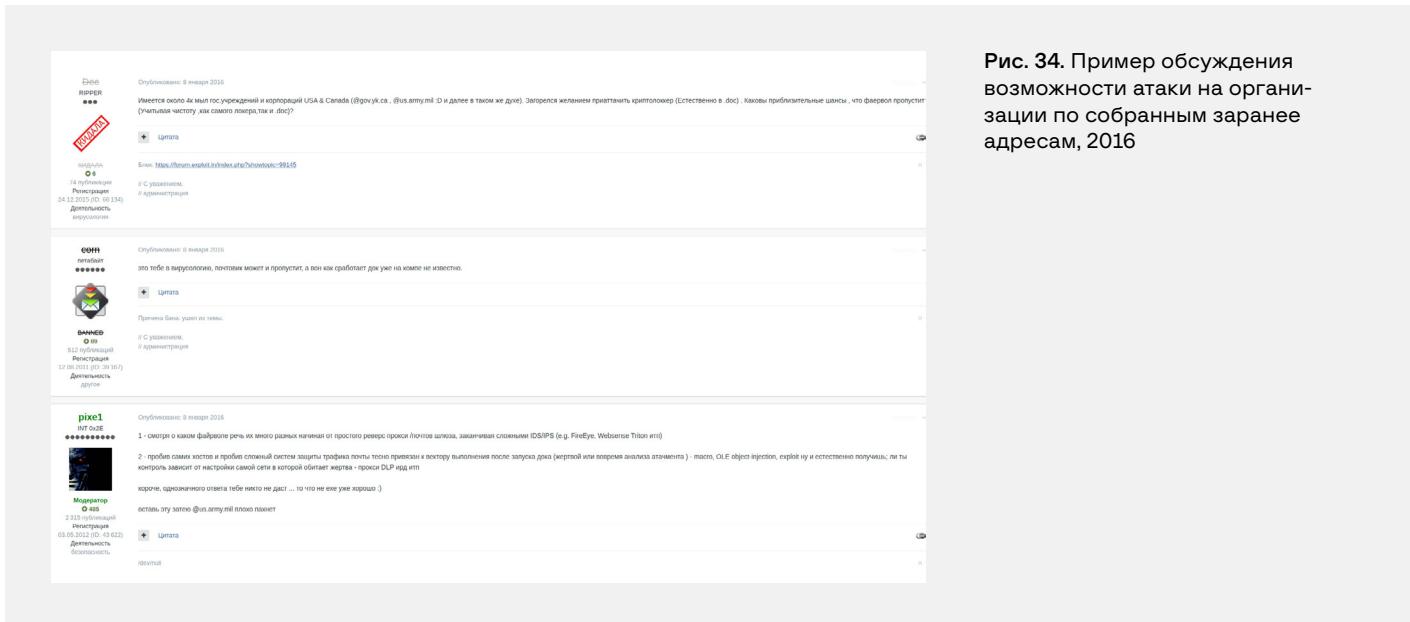


Рис. 34. Пример обсуждения возможности атаки на организации по собранным заранее адресам, 2016

Далее мы не будем останавливаться на каждом новом шифровальщике подробно, уделив внимание лишь самым интересным событиям, которые произошли за эти годы и повлияли на развитие киберимперии вымогателей в целом.

Итак, 24 февраля 2016 года стартует одна из самых известных и крупных партнерских программ по шифровальщикам на то время – **Cerber Ransomware**. За расшифровку вымогатели требуют \$500, для оплаты выкупа предлагают пройти на сайт, размещенный в сети Tor. В июле 2016 Cerber Ransomware становится самым распространенным вымогателем.

В марте 2016 года был зафиксирован первый полноценный шифровальщик для Mac OS X под названием **KeRanger**¹⁴¹. Для его распространения злоумышленники взломали ресурс известной программы **Transmission** и подменили его на свою копию.

Также в конце марта 2016 года появляется новый троян **Petya**. Помимо шифрования он использовал другую технику, которая в 2012 году применялась в обычных локерах – перезапись Master Boot Record (MBR), что в итоге приводило к тому, что жертва даже не могла запустить ОС. Чуть позднее вместе с этим локером начал распространяться локер **Mischa**, который шифровал файлы без MBR, если прав было недостаточно. В июле такую же технику начинает использовать другой шифровальщик – **Satana**.

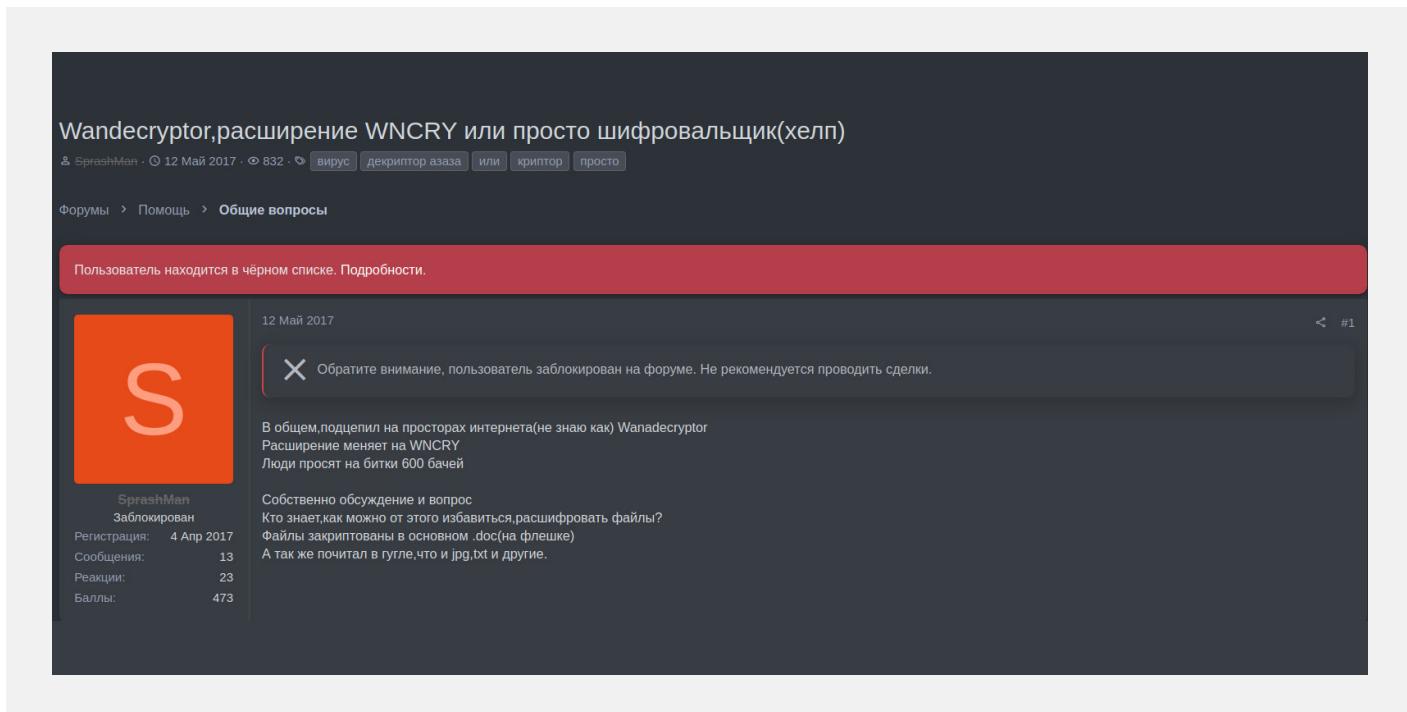
В мае 2016 появляется шифровальщик **ZCryptor**. Он обладал новой техникой, свойственной классическим вирусам – самораспространением на различные устройства.

В ноябре 2016 появились шифровальщики, которые использовали мессенджер Telegram в качестве управляющего сервера для своих троянов. Шифровальщик содержал API ключ бота в Telegram и сообщал об инфицировании и других действиях в определенные каналы или напрямую злоумышленникам. Сейчас такая техника очень часто используется в стилерах.

Самыми распространенными шифровальщиками за 2016 год стали **CTB-Locker**, **Locky** и **TeslaCrypt**.

12 мая 2017 года пользователи, в том числе на андеграундных форумах, начинают жаловаться, что их файлы зашифрованы новым шифровальщиком, который меняет расширение на WNCRY:

Рис. 35. Сообщение о новом шифровальщике WNCRY, 2017



В ходе атаки данного вредоносного ПО за короткое время было зашифровано около полутора миллионов машин. Основной причиной столь быстрого распространения было то, что троян имел способность к самораспространению с помощью эксплойта **EternalBlue** и последующей установки бэкдора **DoublePulsar**. Эта история показала злоумышленникам, что для массового распространения вредоносного ПО можно использовать известные уязвимости. Поэтому чуть позднее, а именно 27 июня 2017 года, другой шифровальщик **NotPetya** использовал ту же уязвимость для своих атак.

Формирование современных трендов RaaS: GandCrab

2018—2019



GandCrab, REvil, Mephistophilus

В январе 2018 года появляется одна из самых известных партнерских программ **GandCrab**. Считается, что исходные коды именно этого вредоносного ПО использовала группа **REvil** для разработки своего трояна. Данная партнерская программа прослужила прародителем практически всех основных трендов, которые до сих пор используются злоумышленниками.

GandCrab

Topic name: GandCrab Ransomware
Topic message:

Появился купон для тех, кто указывает информацию о компаниях и лицах, имеющих постоянный источник инфляции.)
Рады представить универсальный речевой конвертер качественных инструментов: GANDCRAB Ransomware.
Продукт написан на C/C++ с использованием WinAPI;
Не имеет никаких сторонних зависимостей.
Максимальное время работы - 10 минут.
Максимальное время работы - 10 минут.
Файл с ключом (PRIVATEKEY) создается отдельным потоком, шифрование файлов: свыше 1400 часов (с возможностью добавления новых). В ручную в админ-панели алгоритм AES с ключом в 256 бит - шифрование ключа происходит
Алгоритм шифрования AES режим шифрования CBC с использованием CSPNG, модуля SSE (Arnoldi);
При выполнении ИК или перегрузки начинает поиск и шифрование новых файлов и скрытых директорий;
Сезар фильтр обходит Anti-Malware решения на основе блокировок (.Сезар фильтр).
Применение шифрования алгоритмом: трафик между админ-панелью и ботом зашифрован, мета-данные, структура параметров файла опускаются, используется комбинация техник для
Продукт не работает по IP и странам: CH, AM, AZ, BY, GE, KG, KZ, MD, TJ, TM, UA, UZ;
Продукт определяет работать или нет на расширение изображения, но и другими параметрами. Таким образом, Китайские сервера с IP расшифровкой также находятся в зоне
ПАРТНЕРСКАЯ ПРОГРАММА.
Удобная администраторская панель агентов в сети TOR (онлайн).
Поддержка отдельных рекламодателей.
Поддержка информации о каждом объекте, возможность выбирать наборы данных.
Ручной калькулятор: размер выплаты от страны, отдельных ботов, масок шифрования - все это настраивает Вы.
При выполнении ИК или перегрузки начинает поиск и шифрование новых файлов и скрытых директорий;
Технология демонстрации процесса шифрования для улучшения восприятия реального времени.
Обработка через поиск частичек у каждого изображения, для извлечения пикселей и пресетов генерации.
Обработка через извлечение пикселей изображения и инструкции к нему на пакете, в случае не успеть выкупить в определенный срок его разрыв заменяется автоматически.
Установка рекламодателей на пакетах.
1. Скорость работы;
2. Удобство использования;
3. Инвестиции в проект;

Мы работаем как Raid (Ransomware As-a-Service), поэтому партнёрам:
1. Добро пожаловать;
2. Поддержка и обновление продукта;
3. Техническая поддержка;
4. Партнерские соглашения;

1. Работаем без АИ, используем только техники, что возможны для удаления проприетарного продукта в Вашу сторону до 70%;
2. Применяем антивирусы и плагины, что не влияет на характеристики шифровального трафика и паролей* (наши методы анти-анти-вируса);
3. Бесплатная поддержка между ПТР и Администраторами и ПТ (платят);
4. Секьюрити и институт способствуют изучению и разработке новых методов;

1. запрещено заниматься, эта фишь на миграционные изменения (которые передаются скрипты AB в лаборатории);
2. запрещена любая попытка работы по СНГ странам (AM, AZ, BY, GE, KG, KZ, MD, RU, TJ, TM, UA, UZ);
3. запрещены любые попытки взлома и смены логинов;
4. запрещены попытки взлома и смены паролей.
За нарушение этих правил выходит удаление без последующих выплат.
Приносим извинения из-за временного отсутствия работы из-за перебоев в интернете.
Приносим извинения из-за временного отсутствия работы из-за перебоев в интернете и изменений политики трафика в сети.

С уважением, администрация GANDCRAB

Рис. 36. Описание партнерской программы GANDCRAB, 2018

GANDCRAB подробно описывала, как именно стоит атаковать своих жертв и указала крайне популярный на данный момент способ с фреймворком Cobalt Strike.

GandCrab

Topic name: GANDCRAB Ransomware
Topic message:

We appeared on 01/28/2018 and are already working in the following areas:
1. RIG_EK
2. GrandSoft_EK
3. Neurs botnet
4. Fifttest popups
5. Cobalt (APT soft)
6. Cobalt (APT soft)
7. Cobalt (APT soft)
8. Cobalt (APT soft)
9. Cobalt (APT soft)
10. Cobalt (APT soft)
11. Cobalt (APT soft)
12. Cobalt (APT soft)
13. Cobalt (APT soft)
14. Cobalt (APT soft)
15. Cobalt (APT soft)
16. Cobalt (APT soft)
17. Cobalt (APT soft)
18. Cobalt (APT soft)
19. Cobalt (APT soft)
20. Cobalt (APT soft)
21. Cobalt (APT soft)
22. Cobalt (APT soft)
23. Cobalt (APT soft)
24. Cobalt (APT soft)
25. Cobalt (APT soft)
26. Cobalt (APT soft)
27. Cobalt (APT soft)
28. Cobalt (APT soft)
29. Cobalt (APT soft)
30. Cobalt (APT soft)
31. Cobalt (APT soft)
32. Cobalt (APT soft)
33. Cobalt (APT soft)
34. Cobalt (APT soft)
35. Cobalt (APT soft)
36. Cobalt (APT soft)
37. Cobalt (APT soft)
38. Cobalt (APT soft)
39. Cobalt (APT soft)
40. Cobalt (APT soft)
41. Cobalt (APT soft)
42. Cobalt (APT soft)
43. Cobalt (APT soft)
44. Cobalt (APT soft)
45. Cobalt (APT soft)
46. Cobalt (APT soft)
47. Cobalt (APT soft)
48. Cobalt (APT soft)
49. Cobalt (APT soft)
50. Cobalt (APT soft)
51. Cobalt (APT soft)
52. Cobalt (APT soft)
53. Cobalt (APT soft)
54. Cobalt (APT soft)
55. Cobalt (APT soft)
56. Cobalt (APT soft)
57. Cobalt (APT soft)
58. Cobalt (APT soft)
59. Cobalt (APT soft)
60. Cobalt (APT soft)
61. Cobalt (APT soft)
62. Cobalt (APT soft)
63. Cobalt (APT soft)
64. Cobalt (APT soft)
65. Cobalt (APT soft)
66. Cobalt (APT soft)
67. Cobalt (APT soft)
68. Cobalt (APT soft)
69. Cobalt (APT soft)
70. Cobalt (APT soft)
71. Cobalt (APT soft)
72. Cobalt (APT soft)
73. Cobalt (APT soft)
74. Cobalt (APT soft)
75. Cobalt (APT soft)
76. Cobalt (APT soft)
77. Cobalt (APT soft)
78. Cobalt (APT soft)
79. Cobalt (APT soft)
80. Cobalt (APT soft)
81. Cobalt (APT soft)
82. Cobalt (APT soft)
83. Cobalt (APT soft)
84. Cobalt (APT soft)
85. Cobalt (APT soft)
86. Cobalt (APT soft)
87. Cobalt (APT soft)
88. Cobalt (APT soft)
89. Cobalt (APT soft)
90. Cobalt (APT soft)
91. Cobalt (APT soft)
92. Cobalt (APT soft)
93. Cobalt (APT soft)
94. Cobalt (APT soft)
95. Cobalt (APT soft)
96. Cobalt (APT soft)
97. Cobalt (APT soft)
98. Cobalt (APT soft)
99. Cobalt (APT soft)
100. Cobalt (APT soft)
101. Cobalt (APT soft)
102. Cobalt (APT soft)
103. Cobalt (APT soft)
104. Cobalt (APT soft)
105. Cobalt (APT soft)
106. Cobalt (APT soft)
107. Cobalt (APT soft)
108. Cobalt (APT soft)
109. Cobalt (APT soft)
110. Cobalt (APT soft)
111. Cobalt (APT soft)
112. Cobalt (APT soft)
113. Cobalt (APT soft)
114. Cobalt (APT soft)
115. Cobalt (APT soft)
116. Cobalt (APT soft)
117. Cobalt (APT soft)
118. Cobalt (APT soft)
119. Cobalt (APT soft)
120. Cobalt (APT soft)
121. Cobalt (APT soft)
122. Cobalt (APT soft)
123. Cobalt (APT soft)
124. Cobalt (APT soft)
125. Cobalt (APT soft)
126. Cobalt (APT soft)
127. Cobalt (APT soft)
128. Cobalt (APT soft)
129. Cobalt (APT soft)
130. Cobalt (APT soft)
131. Cobalt (APT soft)
132. Cobalt (APT soft)
133. Cobalt (APT soft)
134. Cobalt (APT soft)
135. Cobalt (APT soft)
136. Cobalt (APT soft)
137. Cobalt (APT soft)
138. Cobalt (APT soft)
139. Cobalt (APT soft)
140. Cobalt (APT soft)
141. Cobalt (APT soft)
142. Cobalt (APT soft)
143. Cobalt (APT soft)
144. Cobalt (APT soft)
145. Cobalt (APT soft)
146. Cobalt (APT soft)
147. Cobalt (APT soft)
148. Cobalt (APT soft)
149. Cobalt (APT soft)
150. Cobalt (APT soft)
151. Cobalt (APT soft)
152. Cobalt (APT soft)
153. Cobalt (APT soft)
154. Cobalt (APT soft)
155. Cobalt (APT soft)
156. Cobalt (APT soft)
157. Cobalt (APT soft)
158. Cobalt (APT soft)
159. Cobalt (APT soft)
160. Cobalt (APT soft)
161. Cobalt (APT soft)
162. Cobalt (APT soft)
163. Cobalt (APT soft)
164. Cobalt (APT soft)
165. Cobalt (APT soft)
166. Cobalt (APT soft)
167. Cobalt (APT soft)
168. Cobalt (APT soft)
169. Cobalt (APT soft)
170. Cobalt (APT soft)
171. Cobalt (APT soft)
172. Cobalt (APT soft)
173. Cobalt (APT soft)
174. Cobalt (APT soft)
175. Cobalt (APT soft)
176. Cobalt (APT soft)
177. Cobalt (APT soft)
178. Cobalt (APT soft)
179. Cobalt (APT soft)
180. Cobalt (APT soft)
181. Cobalt (APT soft)
182. Cobalt (APT soft)
183. Cobalt (APT soft)
184. Cobalt (APT soft)
185. Cobalt (APT soft)
186. Cobalt (APT soft)
187. Cobalt (APT soft)
188. Cobalt (APT soft)
189. Cobalt (APT soft)
190. Cobalt (APT soft)
191. Cobalt (APT soft)
192. Cobalt (APT soft)
193. Cobalt (APT soft)
194. Cobalt (APT soft)
195. Cobalt (APT soft)
196. Cobalt (APT soft)
197. Cobalt (APT soft)
198. Cobalt (APT soft)
199. Cobalt (APT soft)
200. Cobalt (APT soft)
201. Cobalt (APT soft)
202. Cobalt (APT soft)
203. Cobalt (APT soft)
204. Cobalt (APT soft)
205. Cobalt (APT soft)
206. Cobalt (APT soft)
207. Cobalt (APT soft)
208. Cobalt (APT soft)
209. Cobalt (APT soft)
210. Cobalt (APT soft)
211. Cobalt (APT soft)
212. Cobalt (APT soft)
213. Cobalt (APT soft)
214. Cobalt (APT soft)
215. Cobalt (APT soft)
216. Cobalt (APT soft)
217. Cobalt (APT soft)
218. Cobalt (APT soft)
219. Cobalt (APT soft)
220. Cobalt (APT soft)
221. Cobalt (APT soft)
222. Cobalt (APT soft)
223. Cobalt (APT soft)
224. Cobalt (APT soft)
225. Cobalt (APT soft)
226. Cobalt (APT soft)
227. Cobalt (APT soft)
228. Cobalt (APT soft)
229. Cobalt (APT soft)
230. Cobalt (APT soft)
231. Cobalt (APT soft)
232. Cobalt (APT soft)
233. Cobalt (APT soft)
234. Cobalt (APT soft)
235. Cobalt (APT soft)
236. Cobalt (APT soft)
237. Cobalt (APT soft)
238. Cobalt (APT soft)
239. Cobalt (APT soft)
240. Cobalt (APT soft)
241. Cobalt (APT soft)
242. Cobalt (APT soft)
243. Cobalt (APT soft)
244. Cobalt (APT soft)
245. Cobalt (APT soft)
246. Cobalt (APT soft)
247. Cobalt (APT soft)
248. Cobalt (APT soft)
249. Cobalt (APT soft)
250. Cobalt (APT soft)
251. Cobalt (APT soft)
252. Cobalt (APT soft)
253. Cobalt (APT soft)
254. Cobalt (APT soft)
255. Cobalt (APT soft)
256. Cobalt (APT soft)
257. Cobalt (APT soft)
258. Cobalt (APT soft)
259. Cobalt (APT soft)
260. Cobalt (APT soft)
261. Cobalt (APT soft)
262. Cobalt (APT soft)
263. Cobalt (APT soft)
264. Cobalt (APT soft)
265. Cobalt (APT soft)
266. Cobalt (APT soft)
267. Cobalt (APT soft)
268. Cobalt (APT soft)
269. Cobalt (APT soft)
270. Cobalt (APT soft)
271. Cobalt (APT soft)
272. Cobalt (APT soft)
273. Cobalt (APT soft)
274. Cobalt (APT soft)
275. Cobalt (APT soft)
276. Cobalt (APT soft)
277. Cobalt (APT soft)
278. Cobalt (APT soft)
279. Cobalt (APT soft)
280. Cobalt (APT soft)
281. Cobalt (APT soft)
282. Cobalt (APT soft)
283. Cobalt (APT soft)
284. Cobalt (APT soft)
285. Cobalt (APT soft)
286. Cobalt (APT soft)
287. Cobalt (APT soft)
288. Cobalt (APT soft)
289. Cobalt (APT soft)
290. Cobalt (APT soft)
291. Cobalt (APT soft)
292. Cobalt (APT soft)
293. Cobalt (APT soft)
294. Cobalt (APT soft)
295. Cobalt (APT soft)
296. Cobalt (APT soft)
297. Cobalt (APT soft)
298. Cobalt (APT soft)
299. Cobalt (APT soft)
300. Cobalt (APT soft)
301. Cobalt (APT soft)
302. Cobalt (APT soft)
303. Cobalt (APT soft)
304. Cobalt (APT soft)
305. Cobalt (APT soft)
306. Cobalt (APT soft)
307. Cobalt (APT soft)
308. Cobalt (APT soft)
309. Cobalt (APT soft)
310. Cobalt (APT soft)
311. Cobalt (APT soft)
312. Cobalt (APT soft)
313. Cobalt (APT soft)
314. Cobalt (APT soft)
315. Cobalt (APT soft)
316. Cobalt (APT soft)
317. Cobalt (APT soft)
318. Cobalt (APT soft)
319. Cobalt (APT soft)
320. Cobalt (APT soft)
321. Cobalt (APT soft)
322. Cobalt (APT soft)
323. Cobalt (APT soft)
324. Cobalt (APT soft)
325. Cobalt (APT soft)
326. Cobalt (APT soft)
327. Cobalt (APT soft)
328. Cobalt (APT soft)
329. Cobalt (APT soft)
330. Cobalt (APT soft)
331. Cobalt (APT soft)
332. Cobalt (APT soft)
333. Cobalt (APT soft)
334. Cobalt (APT soft)
335. Cobalt (APT soft)
336. Cobalt (APT soft)
337. Cobalt (APT soft)
338. Cobalt (APT soft)
339. Cobalt (APT soft)
340. Cobalt (APT soft)
341. Cobalt (APT soft)
342. Cobalt (APT soft)
343. Cobalt (APT soft)
344. Cobalt (APT soft)
345. Cobalt (APT soft)
346. Cobalt (APT soft)
347. Cobalt (APT soft)
348. Cobalt (APT soft)
349. Cobalt (APT soft)
350. Cobalt (APT soft)
351. Cobalt (APT soft)
352. Cobalt (APT soft)
353. Cobalt (APT soft)
354. Cobalt (APT soft)
355. Cobalt (APT soft)
356. Cobalt (APT soft)
357. Cobalt (APT soft)
358. Cobalt (APT soft)
359. Cobalt (APT soft)
360. Cobalt (APT soft)
361. Cobalt (APT soft)
362. Cobalt (APT soft)
363. Cobalt (APT soft)
364. Cobalt (APT soft)
365. Cobalt (APT soft)
366. Cobalt (APT soft)
367. Cobalt (APT soft)
368. Cobalt (APT soft)
369. Cobalt (APT soft)
370. Cobalt (APT soft)
371. Cobalt (APT soft)
372. Cobalt (APT soft)
373. Cobalt (APT soft)
374. Cobalt (APT soft)
375. Cobalt (APT soft)
376. Cobalt (APT soft)
377. Cobalt (APT soft)
378. Cobalt (APT soft)
379. Cobalt (APT soft)
380. Cobalt (APT soft)
381. Cobalt (APT soft)
382. Cobalt (APT soft)
383. Cobalt (APT soft)
384. Cobalt (APT soft)
385. Cobalt (APT soft)
386. Cobalt (APT soft)
387. Cobalt (APT soft)
388. Cobalt (APT soft)
389. Cobalt (APT soft)
390. Cobalt (APT soft)
391. Cobalt (APT soft)
392. Cobalt (APT soft)
393. Cobalt (APT soft)
394. Cobalt (APT soft)
395. Cobalt (APT soft)
396. Cobalt (APT soft)
397. Cobalt (APT soft)
398. Cobalt (APT soft)
399. Cobalt (APT soft)
400. Cobalt (APT soft)
401. Cobalt (APT soft)
402. Cobalt (APT soft)
403. Cobalt (APT soft)
404. Cobalt (APT soft)
405. Cobalt (APT soft)
406. Cobalt (APT soft)
407. Cobalt (APT soft)
408. Cobalt (APT soft)
409. Cobalt (APT soft)
410. Cobalt (APT soft)
411. Cobalt (APT soft)
412. Cobalt (APT soft)
413. Cobalt (APT soft)
414. Cobalt (APT soft)
415. Cobalt (APT soft)
416. Cobalt (APT soft)
417. Cobalt (APT soft)
418. Cobalt (APT soft)
419. Cobalt (APT soft)
420. Cobalt (APT soft)
421. Cobalt (APT soft)
422. Cobalt (APT soft)
423. Cobalt (APT soft)
424. Cobalt (APT soft)
425. Cobalt (APT soft)
426. Cobalt (APT soft)
427. Cobalt (APT soft)
428. Cobalt (APT soft)
429. Cobalt (APT soft)
430. Cobalt (APT soft)
431. Cobalt (APT soft)
432. Cobalt (APT soft)
433. Cobalt (APT soft)
434. Cobalt (APT soft)
435. Cobalt (APT soft)
436. Cobalt (APT soft)
437. Cobalt (APT soft)
438. Cobalt (APT soft)
439. Cobalt (APT soft)
440. Cobalt (APT soft)
441. Cobalt (APT soft)
442. Cobalt (APT soft)
443. Cobalt (APT soft)
444. Cobalt (APT soft)
445. Cobalt (APT soft)
446. Cobalt (APT soft)
447. Cobalt (APT soft)
448. Cobalt (APT soft)
449. Cobalt (APT soft)
450. Cobalt (APT soft)
451. Cobalt (APT soft)
452. Cobalt (APT soft)
453. Cobalt (APT soft)
454. Cobalt (APT soft)
455. Cobalt (APT soft)
456. Cobalt (APT soft)
457. Cobalt (APT soft)
458. Cobalt (APT soft)
459. Cobalt (APT soft)
460. Cobalt (APT soft)
461. Cobalt (APT soft)
462. Cobalt (APT soft)
463. Cobalt (APT soft)
464. Cobalt (APT soft)
465. Cobalt (APT soft)
466. Cobalt (APT soft)
467. Cobalt (APT soft)
468. Cobalt (APT soft)
469. Cobalt (APT soft)
470. Cobalt (APT soft)
471. Cobalt (APT soft)
472. Cobalt (APT soft)
473. Cobalt (APT soft)
474. Cobalt (APT soft)
475. Cobalt (APT soft)
476. Cobalt (APT soft)
477. Cobalt (APT soft)
478. Cobalt (APT soft)
479. Cobalt (APT soft)
480. Cobalt (APT soft)
481. Cobalt (APT soft)
482. Cobalt (APT soft)
483. Cobalt (APT soft)
484. Cobalt (APT soft)
485. Cobalt (APT soft)
486. Cobalt (APT soft)
487. Cobalt (APT soft)
488. Cobalt (APT soft)
489. Cobalt (APT soft)
490. Cobalt (APT soft)
491. Cobalt (APT soft)
492. Cobalt (APT soft)
493. Cobalt (APT soft)
494. Cobalt (APT soft)
495. Cobalt (APT soft)
496. Cobalt (APT soft)
497. Cobalt (APT soft)
498. Cobalt (APT soft)
499. Cobalt (APT soft)
500. Cobalt (APT soft)
501. Cobalt (APT soft)
502. Cobalt (APT soft)
503. Cobalt (APT soft)
504. Cobalt (APT soft)
505. Cobalt (APT soft)
506. Cobalt (APT soft)
507. Cobalt (APT soft)
508. Cobalt (APT soft)
509. Cobalt (APT soft)
510. Cobalt (APT soft)
511. Cobalt (APT soft)
512. Cobalt (APT soft)
513. Cobalt (APT soft)
514. Cobalt (APT soft)
515. Cobalt (APT soft)
516. Cobalt (APT soft)
517. Cobalt (APT soft)
518. Cobalt (APT soft)
519. Cobalt (APT soft)
520. Cobalt (APT soft)
521. Cobalt (APT soft)
522. Cobalt (APT soft)
523. Cobalt (APT soft)
524. Cobalt (APT soft)
525. Cobalt (APT soft)
526. Cobalt (APT soft)
527. Cobalt (APT soft)
528. Cobalt (APT soft)
529. Cobalt (APT soft)
530. Cobalt (APT soft)
531. Cobalt (APT soft)
532. Cobalt (APT soft)
533. Cobalt (APT soft)
534. Cobalt (APT soft)
535. Cobalt (APT soft)
536. Cobalt (APT soft)
537. Cobalt (APT soft)
538. Cobalt (APT soft)
539. Cobalt (APT soft)
540. Cobalt (APT soft)
541. Cobalt (APT soft)
542. Cobalt (APT soft)
543. Cobalt (APT soft)
544. Cobalt (APT soft)
545. Cobalt (APT soft)
546. Cobalt (APT soft)
547. Cobalt (APT soft)
548. Cobalt (APT soft)
549. Cobalt (APT soft)
550. Cobalt (APT soft)
551. Cobalt (APT soft)
552. Cobalt (APT soft)
553. Cobalt (APT soft)
554. Cobalt (APT soft)
555. Cobalt (APT soft)
556. Cobalt (APT soft)
557. Cobalt (APT soft)
558. Cobalt (APT soft)
559. Cobalt (APT soft)
560. Cobalt (APT soft)
561. Cobalt (APT soft)
562. Cobalt (APT soft)
563. Cobalt (APT soft)
564. Cobalt (APT soft)
565. Cobalt (APT soft)
566. Cobalt (APT soft)
567. Cobalt (APT soft)
568. Cobalt (APT soft)
569. Cobalt (APT soft)
570. Cobalt (APT soft)
571. Cobalt (APT soft)
572. Cobalt (APT soft)
573. Cobalt (APT soft)
574. Cobalt (APT soft)
575. Cobalt (APT soft)
576. Cobalt (APT soft)
577. Cobalt (APT soft)
578. Cobalt (APT soft)
579. Cobalt (APT soft)
580. Cobalt (APT soft)
581. Cobalt (APT soft)
582. Cobalt (APT soft)
583. Cobalt (APT soft)
584. Cobalt (APT soft)
585. Cobalt (APT soft)
586. Cobalt (APT soft)
587. Cobalt (APT soft)
588. Cobalt (APT soft)
589. Cobalt (APT soft)
590. Cobalt (APT soft)
591. Cobalt (APT soft)
592. Cobalt (APT soft)
593. Cobalt (APT soft)
594. Cobalt (APT soft)
595. Cobalt (APT soft)
596. Cobalt (APT soft)
597. Cobalt (APT soft)
598. Cobalt (APT soft)
599. Cobalt (APT soft)
600. Cobalt (APT soft)
601. Cobalt (APT soft)
602. Cobalt (APT soft)
603. Cobalt (APT soft)
604. Cobalt (APT soft)
605. Cobalt (APT soft)
606. Cobalt (APT soft)
607. Cobalt (APT soft)
608. Cobalt (APT soft)
609. Cobalt (APT soft)
610. Cobalt (APT soft)
611. Cobalt (APT soft)
612. Cobalt (APT soft)
613. Cobalt (APT soft)
614. Cobalt (APT soft)
615. Cobalt (APT soft)
616. Cobalt (APT soft)
617. Cobalt (APT soft)
618. Cobalt (APT soft)
619. Cobalt (APT soft)
620. Cobalt (APT soft)
621. Cobalt (APT soft)
622. Cobalt (APT soft)
623. Cobalt (APT soft)
624. Cobalt (APT soft)
625. Cobalt (APT soft)
626. Cobalt (APT soft)
627. Cobalt (APT soft)
628. Cobalt (APT soft)
629. Cobalt (APT soft)
630. Cobalt (APT soft)
631. Cobalt (APT soft)
632. Cobalt (APT soft)
633. Cobalt (APT soft)
634. Cobalt (APT soft)
635. Cobalt (APT soft)
636. Cobalt (APT soft)
637. Cobalt (APT soft)
638. Cobalt (APT soft)
639. Cobalt (APT soft)
640. Cobalt (APT soft)
641. Cobalt (APT soft)
642. Cobalt (APT soft)
643. Cobalt (APT soft)
644. Cobalt (APT soft)
645. Cobalt (APT soft)
646. Cobalt (APT soft)
647. Cobalt (APT soft)
648. Cobalt (APT soft)
649. Cobalt (APT soft)
650. Cobalt (APT soft)
651. Cobalt (APT soft)
652. Cobalt (APT soft)
653. Cobalt (APT soft)
654. Cobalt (APT soft)
655. Cobalt (APT soft)
656. Cobalt (APT soft)
657. Cobalt (APT soft)
658. Cobalt (APT soft)
659. Cobalt (APT soft)
660. Cobalt (APT soft)
661. Cobalt (APT soft)
662. Cobalt (APT soft)
663. Cobalt (APT soft)
664. Cobalt (APT soft)
665. Cobalt (APT soft)
666. Cobalt (APT soft)
667. Cobalt (APT soft)
668. Cobalt (APT soft)
669. Cobalt (APT soft)
670. Cobalt (APT soft)
671. Cobalt (APT soft)
672. Cobalt (APT soft)
673. Cobalt (APT soft)
674. Cobalt (APT soft)
675. Cobalt (APT soft)
676. Cobalt (APT soft)
677. Cobalt (APT soft)
678. Cobalt (APT soft)
679. Cobalt (APT soft)
680. Cobalt (APT soft)
681. Cobalt (APT soft)
682. Cobalt (APT soft)
683. Cobalt (APT soft)
684. Cobalt (APT soft)
685. Cobalt (APT soft)
686. Cobalt (APT soft)
687. Cobalt (APT soft)
688. Cobalt (APT soft)
689. Cobalt (APT soft)
690. Cobalt (APT soft)
691. Cobalt (APT soft)
692. Cobalt (APT soft)
693. Cobalt (APT soft)
694. Cobalt (APT soft)
695. Cobalt (APT soft)
696. Cobalt (APT soft)
697. Cobalt (APT soft)
698. Cobalt (APT soft)
699. Cobalt (APT soft)
700. Cobalt (APT soft)
701. Cobalt (APT soft)
702. Cobalt (APT soft)
703. Cobalt (APT soft)
704. Cobalt (APT soft)
705. Cobalt (APT soft)
706. Cobalt (APT soft)
707. Cobalt (APT soft)
708. Cobalt (APT soft)
709. Cobalt (APT soft)
710. Cobalt (APT soft)
711. Cobalt (APT soft)
712. Cobalt (APT soft)
713. Cobalt (APT soft)
714. Cobalt (APT soft)
715. Cobalt (APT soft)
716. Cobalt (APT soft)
717. Cobalt (APT soft)
718. Cobalt (APT soft)
719. Cobalt (APT soft)
720. Cobalt (APT soft)
721. Cobalt (APT soft)
722. Cobalt (APT soft)
723. Cobalt (APT soft)
724. Cobalt (APT soft)
725. Cobalt (APT soft)
726. Cobalt (APT soft)
727. Cobalt (APT soft)
728. Cobalt (APT soft)
729. Cobalt (APT soft)
730. Cobalt (APT soft)
731. Cobalt (APT soft)
732. Cobalt (APT soft)
733. Cobalt (APT soft)
734. Cobalt (APT soft)
735. Cobalt (APT soft)
736. Cobalt (APT soft)
737. Cobalt (APT soft)
738. Cobalt (APT soft)
739. Cobalt (APT soft)
740. Cobalt (APT soft)
741. Cobalt (APT soft)
742. Cobalt (APT soft)
743. Cobalt (APT soft)
744. Cobalt (APT soft)
745. Cobalt (APT soft)
746. Cobalt (APT soft)
747. Cobalt (APT soft)
748. Cobalt (APT soft)
749. Cobalt (APT soft)
750. Cobalt (APT soft)
751. Cobalt (APT soft)
752. Cobalt (APT soft)
753. Cobalt (APT soft)
754. Cobalt (APT soft)
755. Cobalt (APT soft)
756. Cobalt (APT soft)
757. Cobalt (APT soft)
758. Cobalt (APT soft)
759. Cobalt (APT soft)
760. Cobalt (APT soft)
761. Cobalt (APT soft)
762. Cobalt (APT soft)
763. Cobalt (APT soft)
764. Cobalt (APT soft)
765. Cobalt (APT soft)
766. Cobalt (APT soft)
767. Cobalt (APT soft)
768. Cobalt (APT soft)
769. Cobalt (APT soft)
770. Cobalt (APT soft)
771. Cobalt (APT soft)
772. Cobalt (APT soft)
773. Cobalt (APT soft)
774. Cobalt (APT soft)
775. Cobalt (APT soft)
776. Cobalt (APT soft)
777. Cobalt (APT soft)
778. Cobalt (APT soft)
779. Cobalt (APT soft)
780. Cobalt (APT soft)
781. Cobalt (APT soft)
782. Cobalt (APT soft)
783. Cobalt (APT soft)
784. Cobalt (APT soft)
785. Cobalt (APT soft)
786. Cobalt (APT soft)
787. Cobalt (APT soft)
788. Cobalt (APT soft)
789. Cobalt (APT soft)
790. Cobalt (APT soft)
791. Cobalt (APT soft)
792. Cobalt (APT soft)
793. Cobalt (APT soft)
794. Cobalt (APT soft)
795. Cobalt (APT soft)<br

Это не остановило злоумышленников и уже 7 марта 2018 года они перезапускают партнерскую программу, отметив, что теперь хранят ключи на отдельном от административной панели сервере.

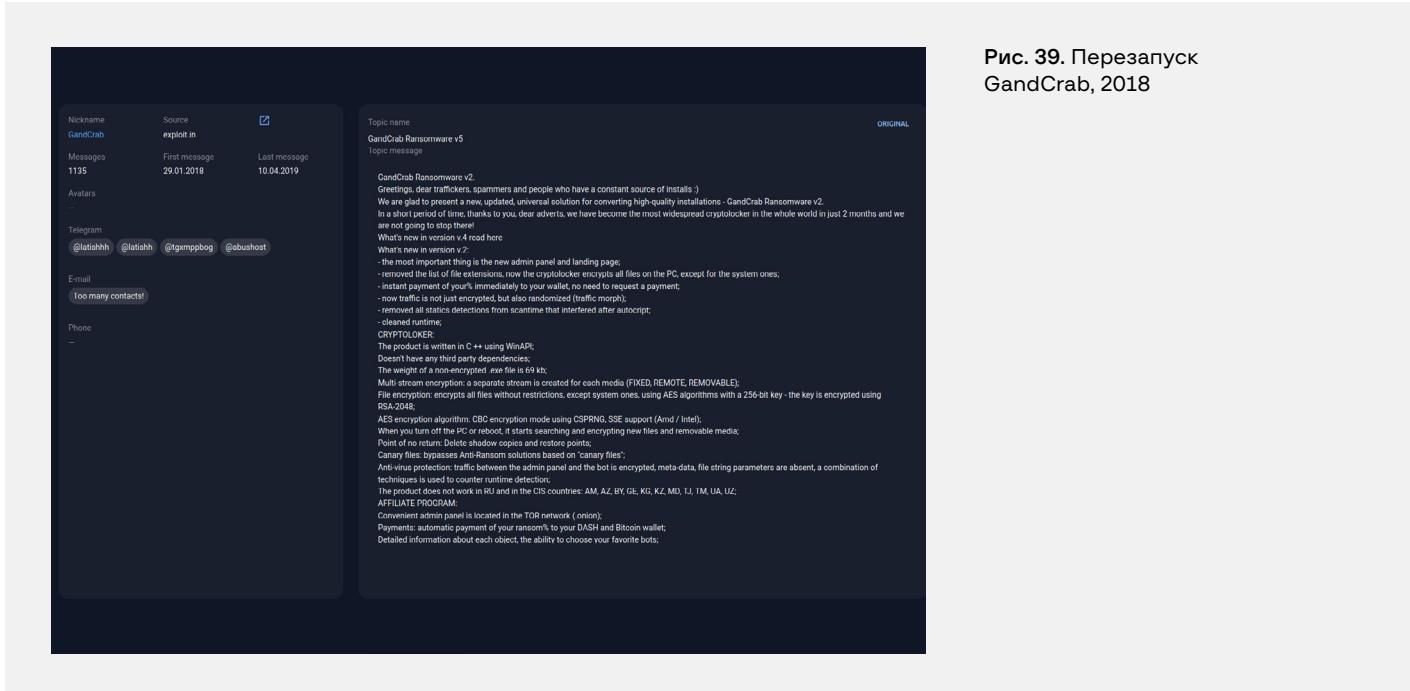


Рис. 39. Перезапуск
GandCrab, 2018

Данная партнерская программа отличалась от остальных продуманной работой с партнёрами, постоянными улучшениями вредоносного ПО и поиском новых технологий с целью повышения конвертации загрузок в выплаты от клиентов. Например, еще в феврале 2018 они первыми вводят прием оплаты в криптовалюте DASH.

Они сами подробно изучали разные методы получения доступа в сеть. Кроме таких стандартных фреймворков, как **Cobalt Strike** и **MSF**, они использовали разные приложения, позволяющие использовать социальную инженерию как основной вектор атаки. К примеру, **Mephistophilus** – систему для целевых фишинговых атак.

Также GandCrab были первыми, кто официально заявил, что они заключают договоры с Recovery компаниями по восстановлению данных:

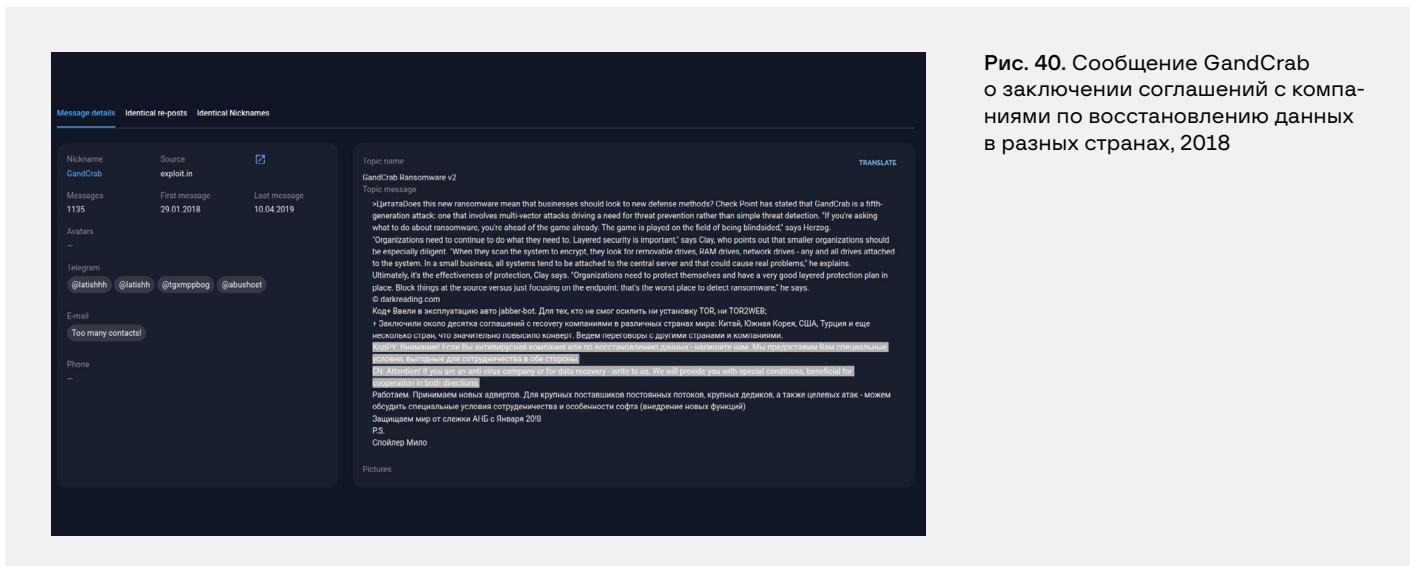


Рис. 40. Сообщение GandCrab
о заключении соглашений с компа-
ниями по восстановлению данных
в разных странах, 2018

В апреле 2018 года они снова создают новый тренд – скупают доступы к выделенным серверам для дальнейшего развития атаки с целью получения полного контроля над внутренней сетью компании.

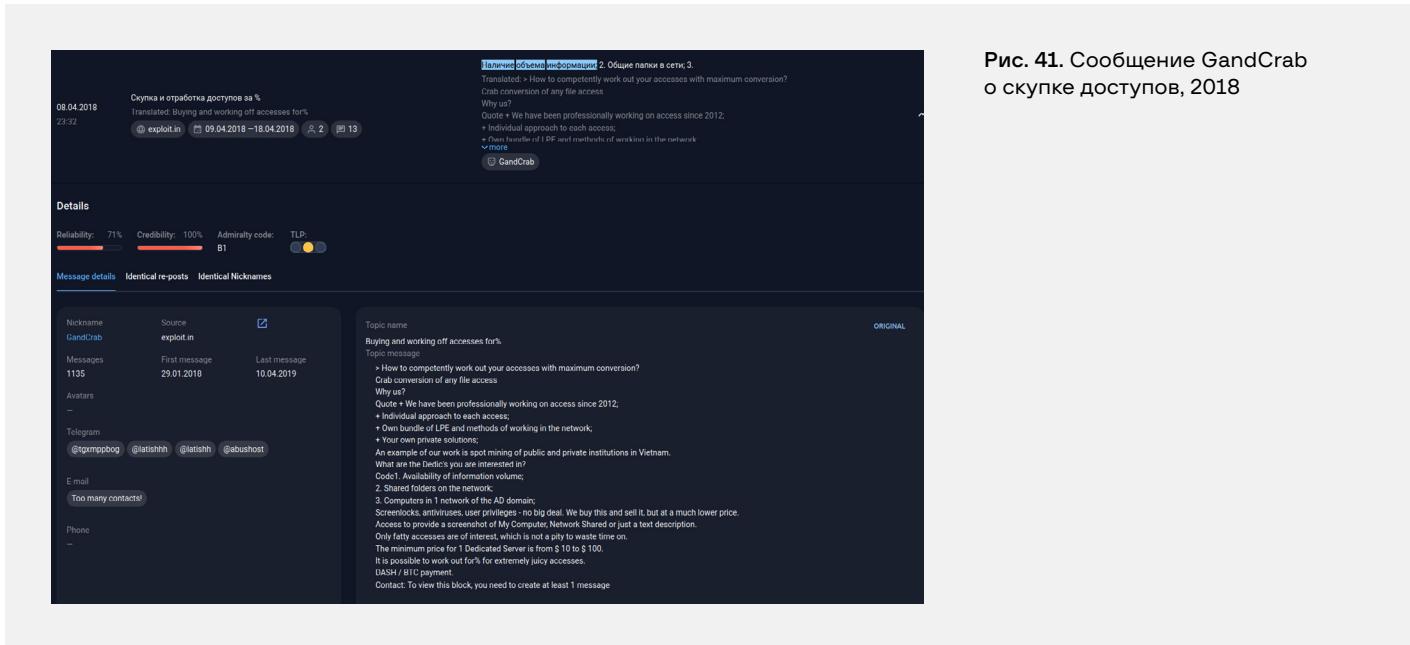


Рис. 41. Сообщение GandCrab о скупке доступов, 2018

По словам GandCrab, на момент апреля 2018 года их недельный оборот составлял более 100 тысяч долларов. В мае преступная группа приводит статистику по своим партнерам и показывает, что некоторые из них зарабатывают от 100 до 200 тысяч долларов в месяц. В июне 2018 они также приводят статистику, что за месяц было инфицировано 315 365 компьютеров. Также они настаивают на том, что ищут АРТ-команду² для получения целевых доступов к крупным компаниям.

В июле 2018 году они заключили 210 контрактов с компаниями по восстановлению данных по всему миру. В этом же месяце вышла новая версия GandCrab, в которой было автоматическое шифрование сетевых дисков. В дальнейшем эта особенность использовалась в других шифровальщиках. После того, как один из самых первых Initial Access Brokers ушел с публичного рынка доступов, на форумах появилось огромное количество новых предложений о продаже доступов. Подробнее об этом читайте в отчете **«Незванные гости: продажа доступов в сети компаний»**. GandCrab были первой группировкой, которая начала постоянно скупать доступы таких пользователей.

В августе 2018 GandCrab меняет логику приема новых партнеров – теперь для участия в программе необходимо пройти собеседование. Подобная практика будет затем перенята другими злоумышленниками.

Исходя из других сообщений данной преступной группы, в качестве связки эксплойтов для получения доступа они использовали Fallout.

В сентябре 2018 года выходит очередное обновление GandCrab, и злоумышленники заявляют, что их месячный доход составил более 1 млн долларов. Из новаторских особенностей, в административной панели новой версии появился билдер скрипта **PowerShell**, который позволял прогружать полезную нагрузку в обход антивирусных систем. Из других интересных особенностей стоит отметить то, что теперь зашифрованные файлы имели динамическое расширение, то есть они менялись от машины к машине. Так же GandCrab начали работать напрямую с крипт-сервисом **NTCrypt**.

² Advanced Persistent Threat – устойчивая угроза, целевая атака; как правило, АРТ-группа связана с работой на государство, т.е. проправительственная хакерская группа

Незванные гости: продажа доступов в сети компаний



В очередном октябрьском обновлении разработчики решили внедрить Mimikatz в свое решение для автоматизации сбора учетных записей. А также они открыто объявили борьбу другим шифровальщикам: они считали неприемлемым шифровать жертв дважды.

17 октября 2018 года злоумышленники заявили, что предоставляют гражданам Сирии бесплатный декриптор. В результате 27 октября антивирусным компаниям удалось получить мастер-ключ путем анализа сгенерированных ключей и сделать универсальный декриптор. В связи с этим 28 октября злоумышленники сделали новый мастер-ключ и стали переходить на новую схему шифрования, которая не зависела от него.

В обновлении от 31 октября у шифровальщика появилась функция сканирования RDP и брутфорса RDP внутри сети и использованием паролей, который достал **Mimikatz**.

В январе 2019 GandCrab открывает новый сервис по монетизации доступов других пользователей. То есть они начинают скупать доступы к RDP или VPN и предлагать продавцам реализацию за процент или выкуп доступа.

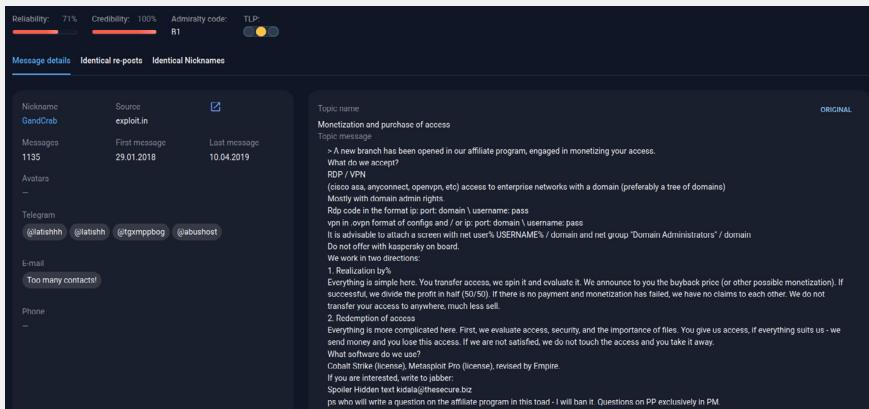


Рис. 42. Сообщение GandCrab о новом сервисе монетизации, 2019

В феврале 2019 была произведена очередная атака на сервера GandCrab, в ходе которой вновь удалось получить секретные ключи, что привело к появлению очередного декриптора.

Внезапно 31 мая 2019 GandCrab уходит с рынка.

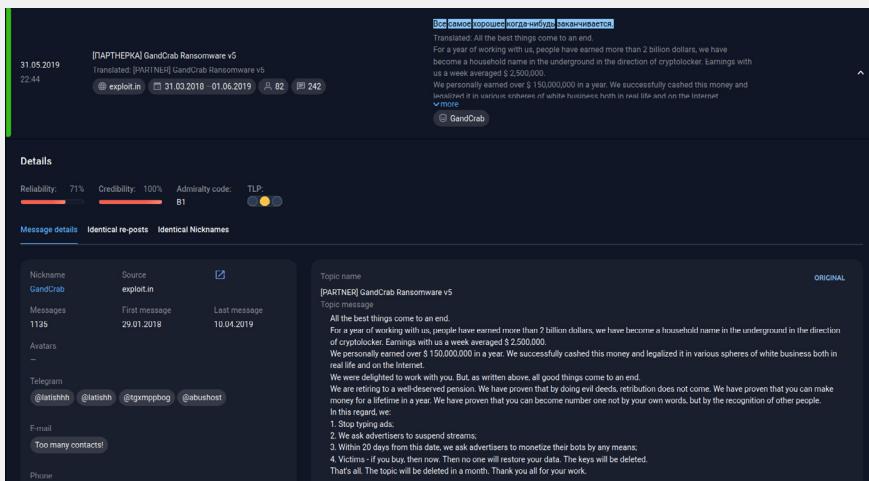


Рис. 43. Сообщение о прекращении деятельности GandCrab, 2019

В своем последнем сообщении владелец GandCrab просит удалить его аккаунты и все, что с ним связано.

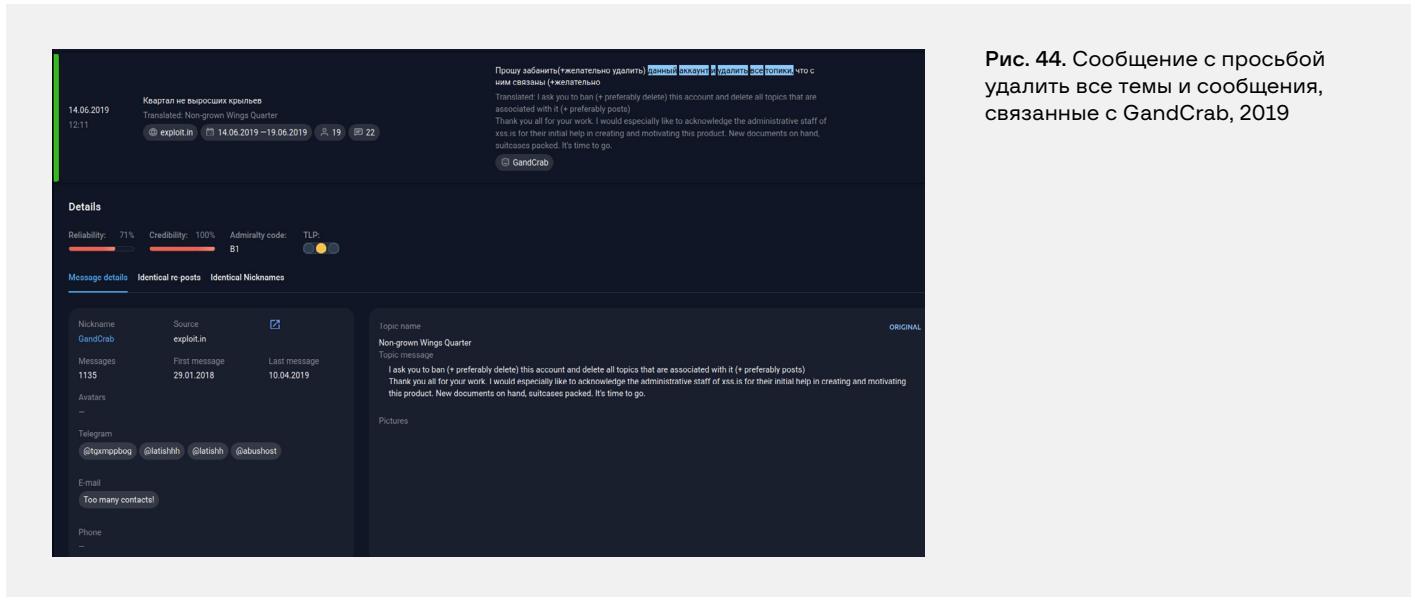


Рис. 44. Сообщение с просьбой удалить все темы и сообщения, связанные с GandCrab, 2019

Современные тренды: double extortion, появление DLS, запрет партнерских программ на форумах

2019—2021



Ransomware Snatch, ChaCha/Maze, REvil, Babuk

В марте 2019 на форуме exploit.in появляется реклама новой партнерской программы **Ransomware Snatch**:

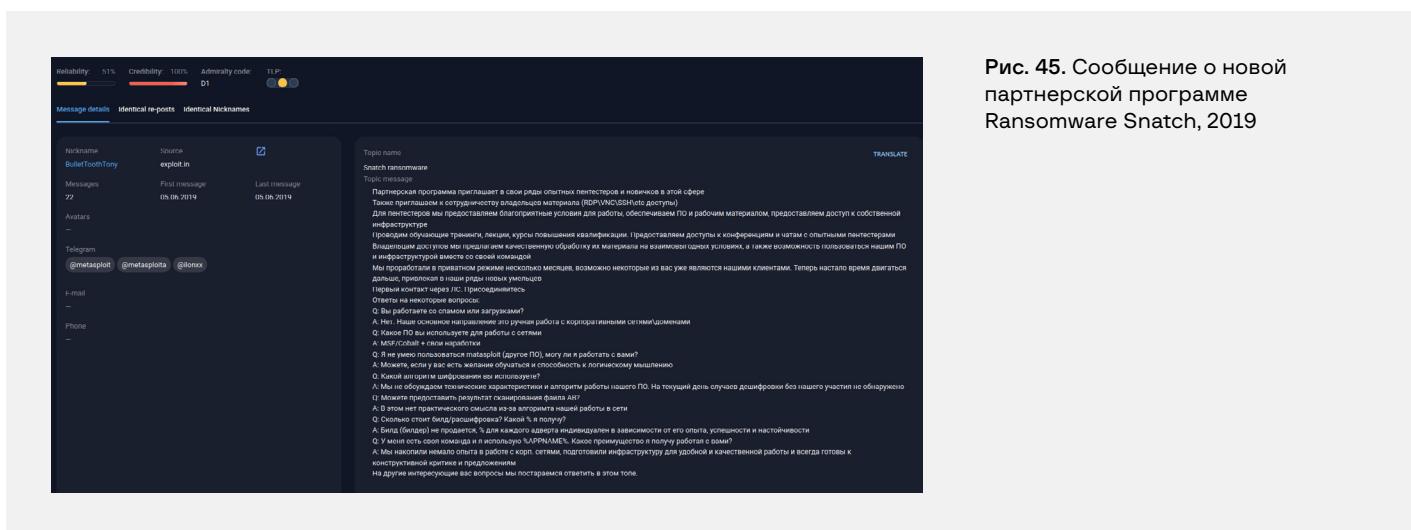
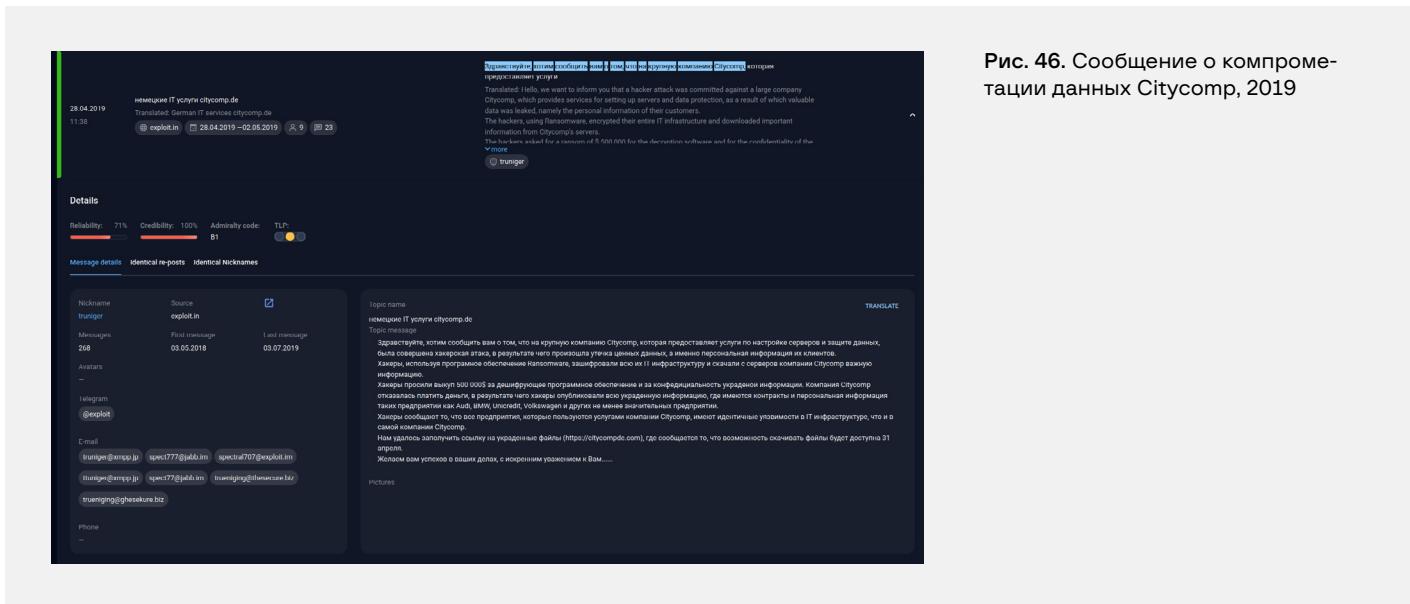


Рис. 45. Сообщение о новой партнерской программе Ransomware Snatch, 2019

Одной из отличительных особенностей данной партнерской программы было то, что в ней не работали с трафиком и загрузками, а сфокусировались исключительно на атаках на корпоративные сети.

28 апреля 2019 года некий пользователь под псевдонимом **truniger** публикует крайне интересный пост на форуме exploit.in, где он сообщает, что сеть компании **Citycomp** была взломана и зашифрована, а все данные были выгружены.



По словам злоумышленника, компания отказалась выплачивать деньги за расшифровку, поэтому некая группа решила выложить их данные в публичный доступ:

Who is a Citycomp?

As a multi-vendor service provider, today we maintain over 70,000 servers and storage systems of every type and size in 75 countries. We also support over 500,000 units of clients' hardware (PCs, workstations, printers, cash registers).

Our engineers are specialists in the field of servers and storage. We are also fully skilled in the networks and desktops field. Our engineers spent many years with different manufacturers servicing server and storage system hardware prior to joining CITYCOMP Service GmbH, and received first-class training.

We gradually won our clients' confidence through delivering proven quality and through being client-centred, and they responded by entrusting more and more of their systems to us. Many data-centre operators have appointed us as their strategic partner for safeguarding the operational status of their critical IT systems, and in on-site service situations our engineers deliver IMAC/D/R and rollout services.*

312 570 files in 51 025 folders, over 516 Gb data financial and private information on all clients, include VAG, Ericsson, Leica, MAN, Toshiba, UniCredit, British Telecom and etc..

Downloading of files will be available Apr, 31, 2019

Best regards: imboristheblade@protonmail.com

Permanent link: <http://snatchvwdns6zto.onion> (to open via TOR browser)

Рис. 46. Сообщение о компроматации данных Citycomp, 2019

Рис. 47. Данные Citycomp попали в открытый доступ, 2019

На ресурсе, где были опубликованы данные, был также указан .onion домен, на котором они собирались хранить утечку в будущем – snatchvwdns6zto.onion

В ходе обсуждения данной утечки пользователь уточнил, что данные и должны были быть опубликованы в случае отказа компании:

The screenshot shows a forum post from the XSS-IS forum. The post is titled "Немецкие IT услуги cityuscomp.de" (German IT services cityuscomp.de) and includes a link to a German exploit. The message content discusses a ransomware leak involving MySqliKits, mentioning a 500k ransom demand and a desire to publish the information to lower the company's reputation. The post has 28 messages and 22 attachments.

Рис. 48. «Эта информация была предназначена для публикации», 2019

В ходе дальнейшего изучения видно, что truniger занимается получением доступов к сетям и ранее работал в партнерской программе GandCrab. Вероятно, что после нее он стал работать в партнерской программе **Snatch**. В дальнейшем домен snatchvwddns6zto.onion стал использоваться для публикации данных о компаниях, которые отказались платить. Это был первый случай, когда группа программ-вымогателей решила оказать двойное давление на жертву. Однако другие группы не сразу подхватили эту технику.

В мае 2019 появляется новой шифровальщик, который изначально назвали **ChaCha** (по названию алгоритма шифрования), который распространялся через набор эксплойтов Fallout. Ранее его использовал также GandCrab. В июне 2019 операторы данного вредоносного ПО дали ему название **Maze**. Однако самое интересное произошло в ноябре 2019: преступная группа зарегистрировала аккаунт на андеграундном форуме XSS-IS и оставила сообщение о взломе и шифровании данных компании **Allied Universal**. Последние связались с ними, но отказались платить даже после предоставления доказательств. После этого злоумышленники решили выложить 10% полученных данных в открытый доступ на андеграундном форуме:

The screenshot shows a XSS-IS forum post from November 22, 2019, titled "[certificates, personal data, e-mail] Allied Universal". The message discusses the breach of Allied Universal security company, mentioning the extraction of sensitive data and the subsequent release of 10% of it on the forum. It also includes a short story about the company's history and its impact.

Рис. 49. Сообщение о компрометации Allied Universal, 2019

В этом же посте они сообщили, что передадут остальные 90% в сервис WikiLeaks, если компания не заплатит им. А также предупредили другие компании о том, что так будет со всеми, кто откажется платить.

В декабре 2019 Maze поняли, что лучшим способом для осуществления подобного давления будет создать собственный **Data leak Site (DLS)**, где они будут публиковать данные компаний, которые отказались от сотрудничества. В результате 9 декабря 2019 года они регистрируют домен mazenews.top, который Maze использует для публикации утечек. Первые публикации утечек там появляются 15 декабря.

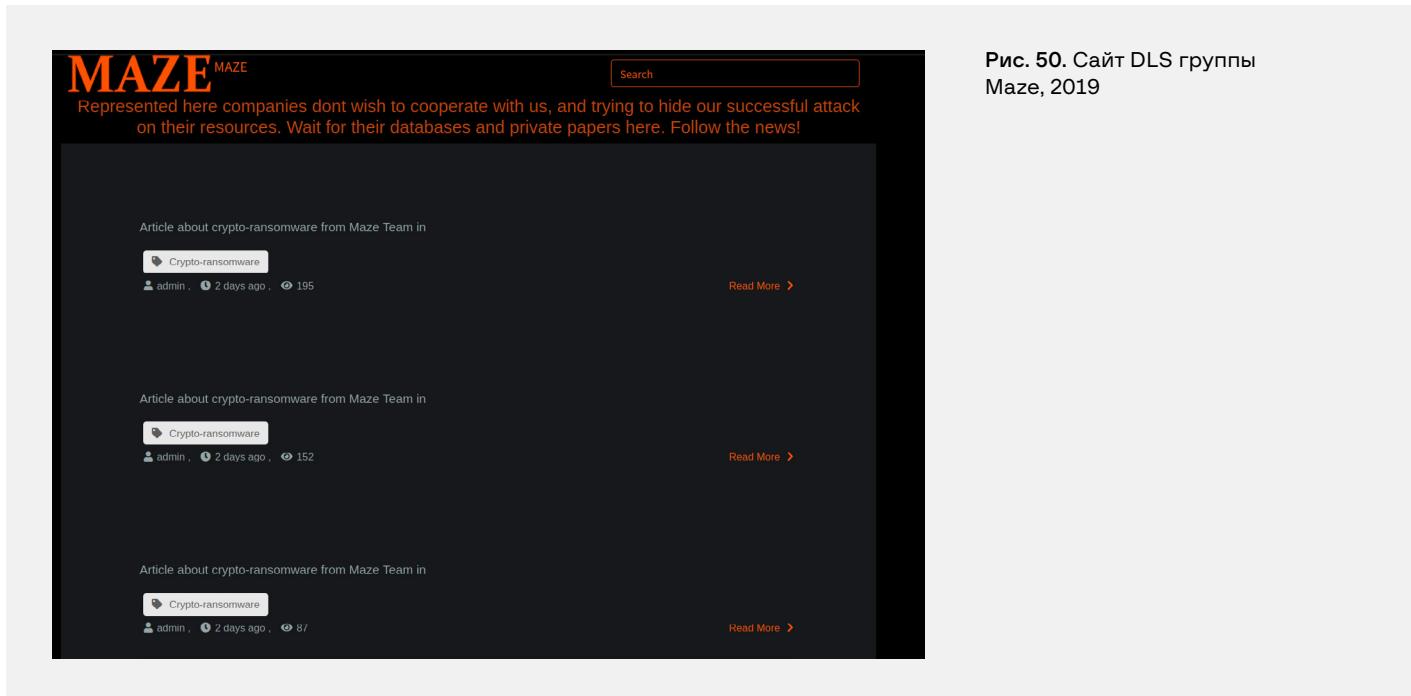


Рис. 50. Сайт DLS группы Maze, 2019

Далее практику преступных групп Maze и Snatch взяли себе на вооружение большинство из известных групп, атакующих с помощью программ-вымогателей.

Последнее значимое событие в развитии RaaS произошло в мае 2021. В связи с крупными атаками различных групп, в особенности группы **REvil**, владельцы форумов решили запретить распространение партнерских программ на андеграундных форумах. Так как, по их словам, это привлекает слишком много внимания к действиям других хакеров.

Рис. 51. Запрет на локеры на одном из андеграундных форумов, 2021

Днем позже к движению “No more ransom!” присоединяется другой крупный андеграундный форум exploit.in:

Рис. 52. Запрет на локеры на exploit.in, 2021

A Убрать партнерки локеров с форума.

Автор: admin, 14 мая в O Exploit.IN Site и Forum

[Подписаться](#) 6

[Создать тему](#)

1 2 3 4 5 6 [ВПЕРЕД](#) » Страница 1 из 10 *

admin <forum.status>
Опубликовано: 14 мая [Изменить](#) [Удалить](#)

Доброго времени суток,

Мы рады пентестерам, специалистам, кодерам.

Но не рады локерам, они привлекают очень много внимания. Сам вид деятельности нам не симпатичен ввиду того, что локается все подряд, мы считаем не целесообразным присутствие на нашем форуме, партнерок локеров.

Решено, убрать все партнерки и запретить как вид деятельности на нашем форуме.

Все топики связанные с локерами будут удалены.

Админ 1154
6 913 публикаций [Регистрация](#) 18.02.2005 (ID: 1)
Действительность другое / other

[7](#) [Сообщение](#)

* advertisement@exploit.im - заказ и оплата рекламы
* support@exploit.im - техническая поддержка форума
* oxygen@exploit.im - арбитр форума
* jabber_support@exploit.im - техническая поддержка jabber-сервера exploit.im

Однако это не остановило злоумышленников. В июле 2021 года на DLS странице группы **Babuk**, вместо данных скомпрометированных компаний появляется реклама нового форума под название RAMP:

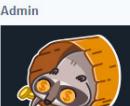
RAMP:)									
Мы заявляем что Ransomware как искусство.									
Index	User list	Rules	Search	Register	Login				
You are not logged in.					» Topics: Active Unanswered				
Index » Новости » Открытие площадки									
Pages: 1									
TetyaSluha Admin  Registered: Yesterday Posts: 3 Offline		Yesterday 12:49:06			#1				
		<p>Всех приветствую! В связи с недавними событиями запрета рансома на других площадках пришло время организовать свой ресурс, где успешные люди могли оставаться под защитой от кидалова. RaS сервисов</p> <p>И вообще создания коммюнити для общения, я как администратор данного ресурса Тетя Шлюха, начиная колонку авторских статей на тему тестирования на проникновения, освещать ту информацию которую вы не найдете на других площадках. Кто я такой вы можете поискать в интернете по кею bavuk.</p> <p>На данный момент отношения к команде bavuk не имею, так же данный продукт рекомендую внести в черный список всем секурути фирмам и датасекам.</p>							
Pages: 1									
Index » Новости » Открытие площадки									

Рис. 53. Новый форум RAMP без запрета на RaaS, 2021

Основной целью данного форума, по заявлению его создателей, является создание новой площадки для рекламы партнерских программ вымогателей. И новая площадка сработала, там довольно быстро появились следующие программы: **Lockbit v.2**, **Avos**, **Caodabi Locker**, **RTM**, **Hive**.

АНАЛИЗ ТЕКУЩИХ ТRENДОВ RAAS

HI-TECH CRIME TRENDS 2021/2022

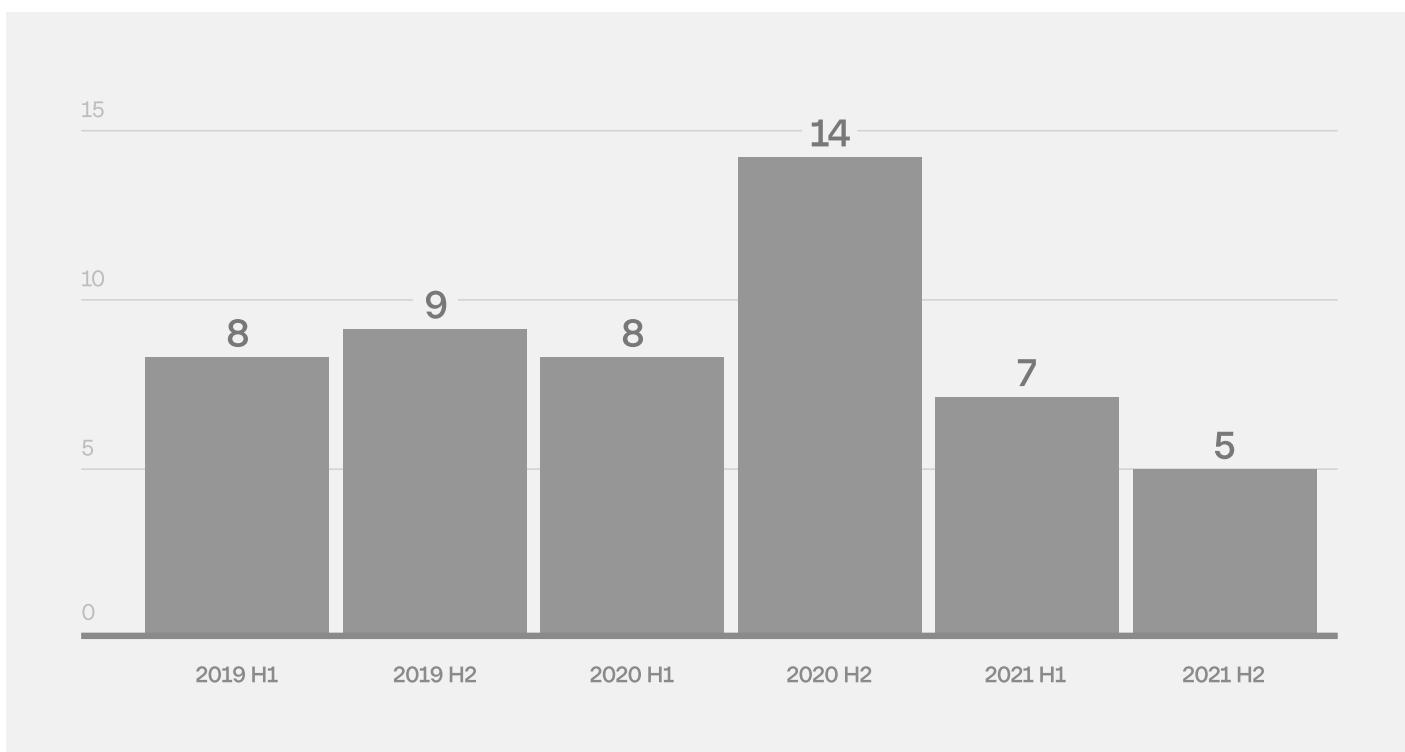
GROUP-IB.RU

Публичные партнерские программы

Как уже было сказано в главе выше, RaaS приобрели свою популярность еще в 2014-м году. Однако все современные партнерские программы стали появляться в свете славы преступной группы **GandCrab**.

Под публичной партнерской программой — RaaS — мы понимаем появление на форуме предложения присоединиться к группе, оперирующей программами-шифровальщиками, а именно заниматься распространением вредоносного ПО за процент от выкупа. Ранее такими «партнерами» были, в основном, злоумышленники, которые занимались трафиком и загрузками ВПО, сейчас, во времена Big Game Hunting, это профессиональные пентестеры (или Initial Access Brokers), которые получают доступ к сетям больших компаний с целью перепродажи или участия в партнерских программах вымогателей.

Рис. 54. Динамика появления новых партнерских программ на форумах в даркнете.



За последние годы — с 2019 по настоящее время — на андеграундных форумах было опубликовано **51 предложение различных партнерских программ — RaaS**. Среди них были «партнерки» крупных программ-вымогателей, такие как LockBit, Hive, SunCrypt или, например, Avaddon, но также и другие, которые так и не смогли стать популярными (realOnline Locker, Keystore Locker, Jingo Locker).

За анализируемый период (H2 2020 – H1 2021) появилось **21 новая партнерская программа на андеграундных форумах**, что на 19% больше чем появилось в прошлом периоде (H2 2019 – H1 2020), когда их было 17. Всего с 2020 по 2021 год появилось **34 новые партнерские программы**.

Стоит также отметить, что по-прежнему существуют скрытые партнерские программы для вступления в которые необходимо связаться с нужными людьми. Кроме этого некоторые партнерские программы находятся на стадии подготовки, так как разработчики оттачивают свое вредоносное ПО для шифрования данных компаний-жертв. Например, в 2021 году мы видим 12 новых партнерских программ на андеграундных форумах, 4 из них — **Babuk, Lockbit, Avos, Hive** — имеют известные DLS ресурсы для публикации данных. Однако за тот же период мы обнаружили еще 29 новых DLS ресурса (не включая вышеназванные), что позволяет предположить, что все они имеют скрытые партнерские программы.

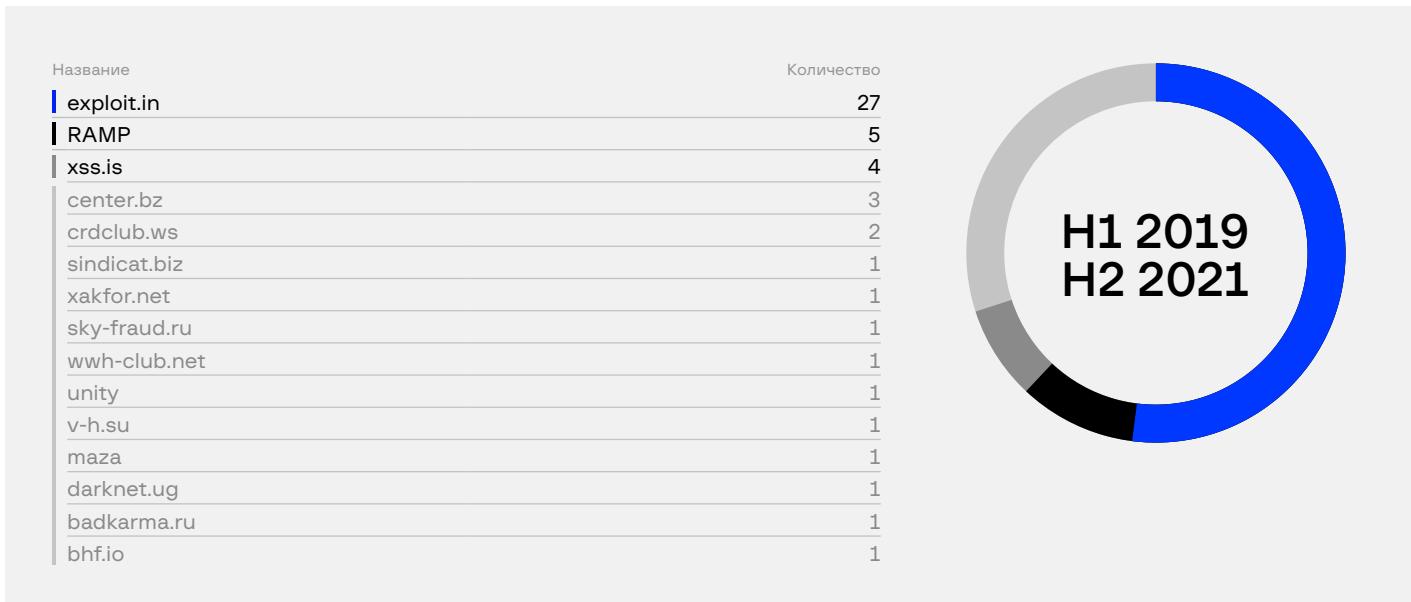
Как видно из графика выше, основная популярность новых партнерских программ пришла на второе полугодие 2020. В 2021 их количество резко снизилось, за первые три квартала этого года на форумах появилось только **12 новых партнерских программ, что на 14% меньше чем за второе полугодие 2021**.

Основными причинами снижения динамики появления DLS являются следующие:

1. Запрет публикации новых RaaS на основных андеграундных форумах.
2. В связи с тем, что многие продавцы доступов стали открыто продавать свой товар на андеграундных форумах, теперь группы, использующие программы-вымогатели, могут выбирать жертвы напрямую на форумах, как в магазине.

За это время (H1 2019 – H2 2021) не менее **15 даркнет-форумов**, которыми управляют русскоязычные администраторы, использовались для публикации RaaS программ. Основным из них был exploit.in (до запрета администраторами RaaS в мае 2021 года), также в топ-3 входят RAMP и XSS.is.

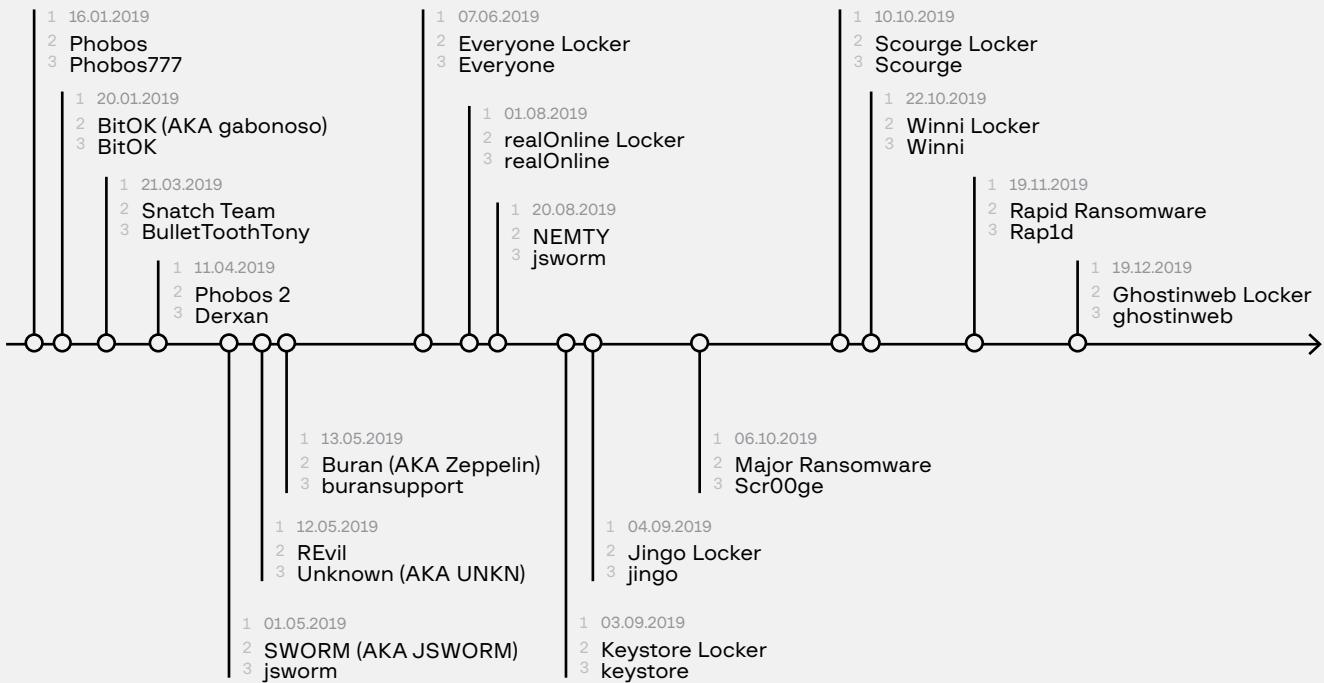
Рис. 55. Распределение RaaS на андеграундных форумах, 2019-2021



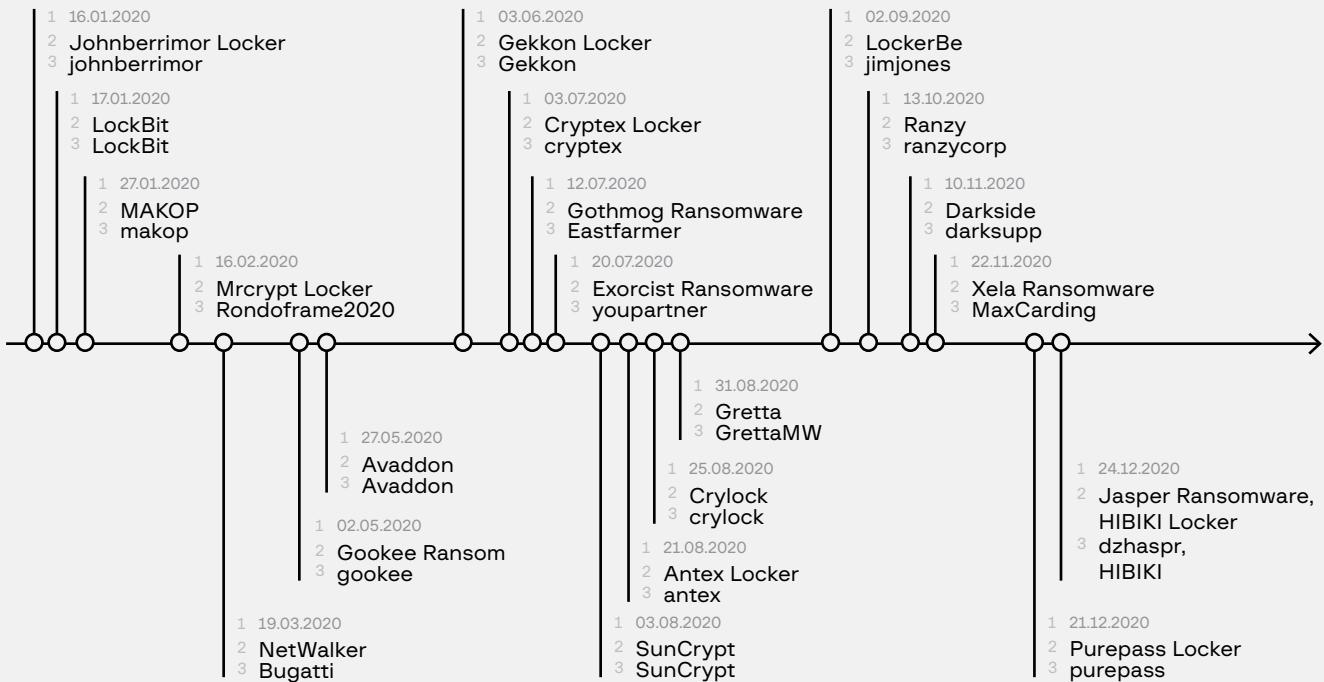
После запрета RaaS на exploit.in популярность быстро стал набирать RAMP. На диаграмме ниже показан таймлайн появления партнерских программ в даркнете начиная с 2019. В этот список не вошли приватные партнерские программы.

1 — Дата
2 — Имя
3 — Никнейм

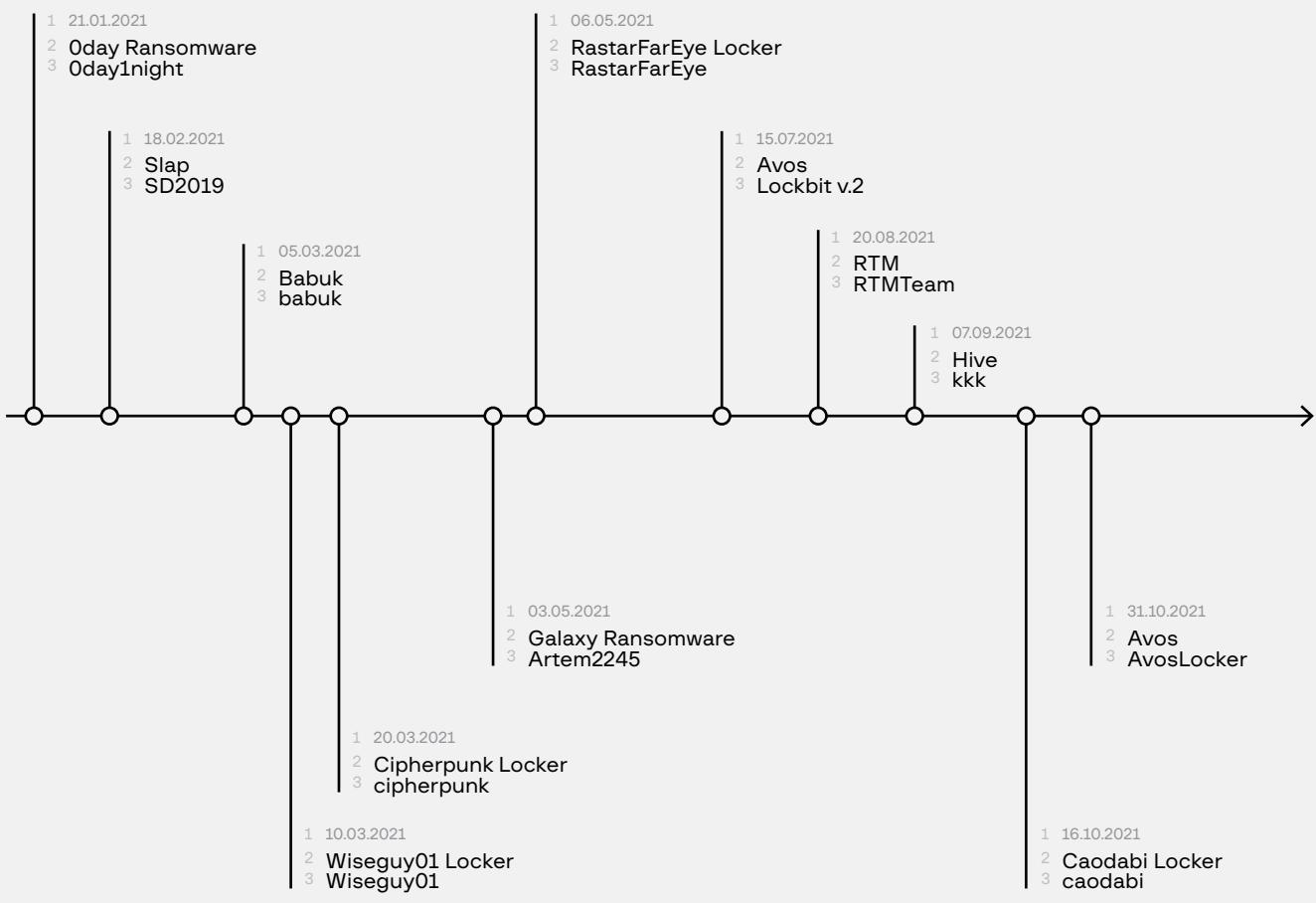
RaaS 2019



RaaS 2020



RaaS 2021



Анализ атак программ-вымогателей на основе компаний, опубликованных на DLS³

Как было отмечено в предыдущей главе, DLS используются операторами программ-вымогателей в качестве техники **double extortion** – то есть, с их помощью оказывается дополнительное давление на жертв для того, чтобы заставить их заплатить денежное вознаграждение. Как правило, после уплаты выкупа, операторы шифровальщиков обещают удалить скомпрометированные данные с DLS или не размещать их в публичном доступе.

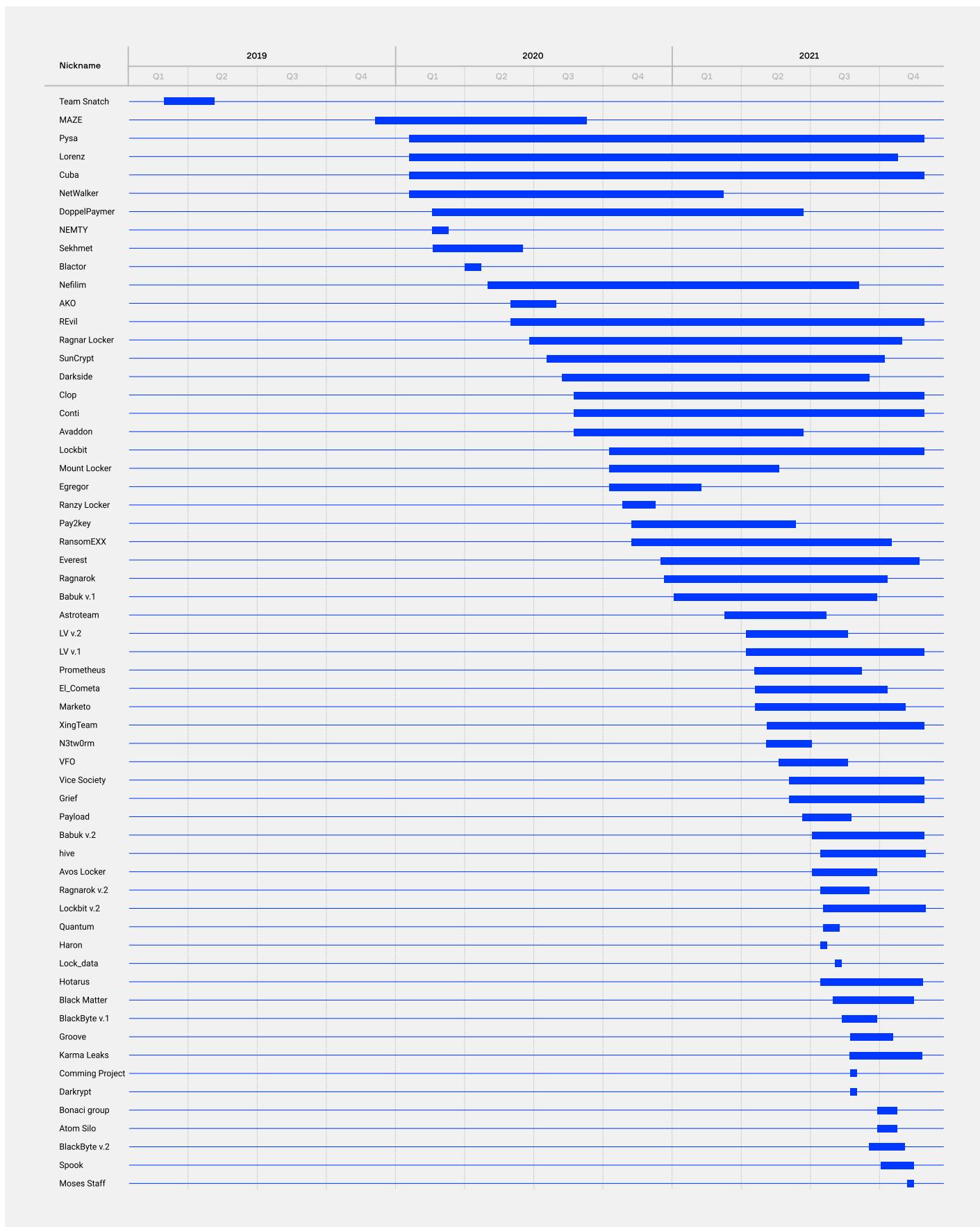
Однако, на практике все выглядит несколько иначе. Согласно исследованиям Group-IB, даже в случае удаления объявления с DLS, ссылки, которые ведут на сами скомпрометированные файлы, находящиеся на других серверах злоумышленников, остаются доступными.

Данная техника впервые была применена группой **Snatch**, но популярной стала после **Maze**. Вероятно, из-за того, что последняя была больше известна в широких кругах.

График ниже показывает, в каком порядке и какие группы операторов программ-вымогателей стали использовать DLS для публикации данных.

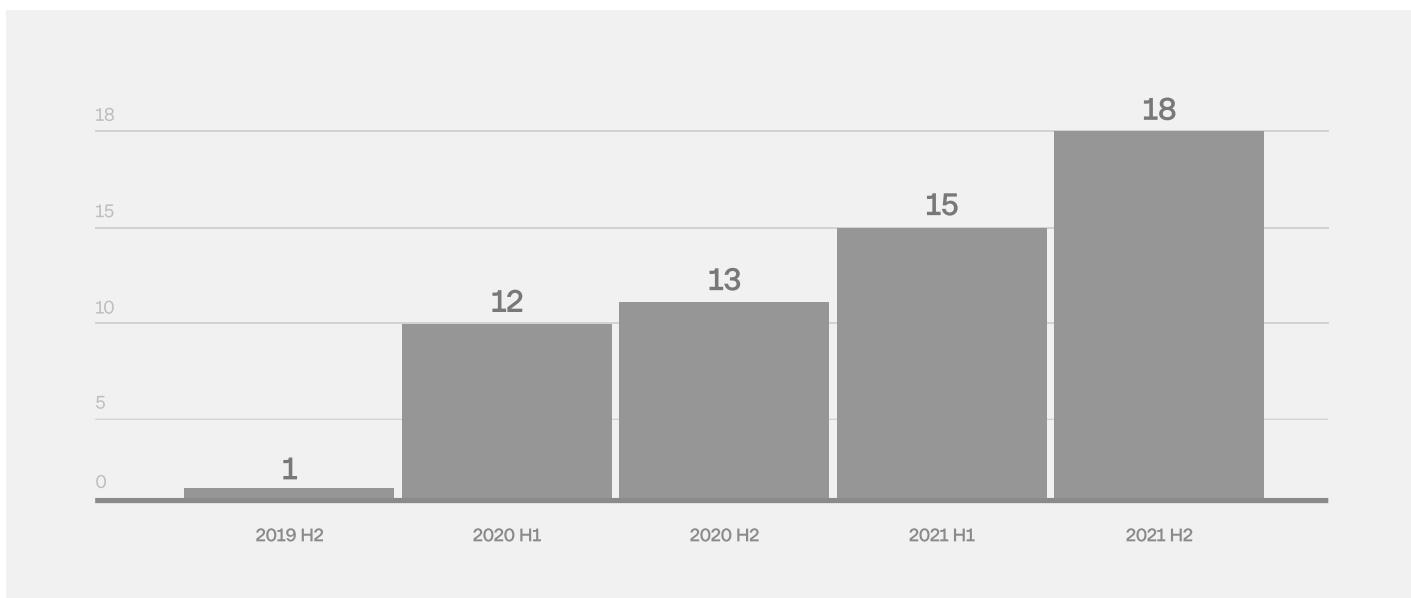
³ Данные в главе представлены для периода Q1 2020 – Q3 2021

Группы операторов программ-вымогателей, использующих DLS, 2019-2021



Как было отмечено в предыдущей главе, количество новых партнерских программ в 2021 году снизилось. Однако это никак не сказывается на появлении новых DLS, а это значит, что многие программы-вымогатели продолжают работать без публичных партнерских программ.

Рис. 56. Появление новых Data Leaks Sites, 2019-2021

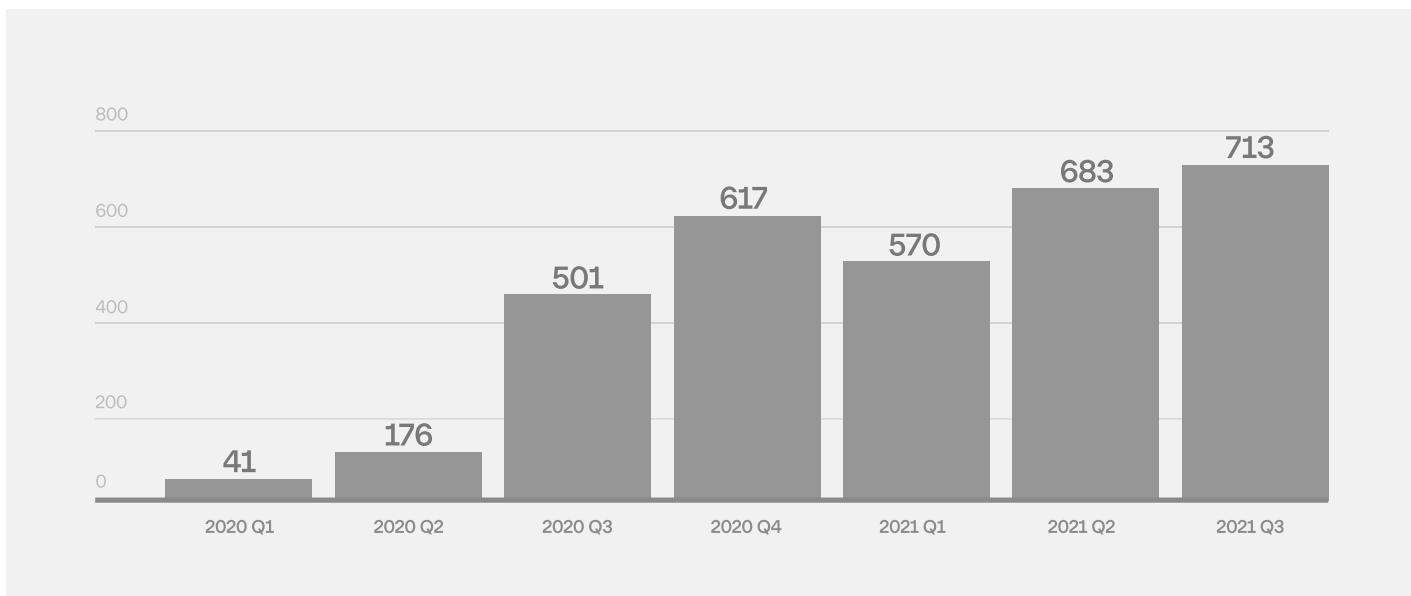


Как видно из графика, количество новых сервисов Data Leaks Sites для публикации выгруженных данных из зашифрованных сетей жертв выросло на 115% (с 13 до 28) за период H2 2020 — H1 2021 по сравнению с H2 2019 - H1 2020.

Это приводит к тому, что количество данных новых компаний-жертв на DLS-сайтах операторов программ-вымогателей, напротив, растет. За анализируемый период (H2 2020 — H1 2021) на DLS были выставлены данные **2 371 компании**, более того, если сравнить это с периодом (H2 2019 — H1 2020), за который было опубликовано только **229 компаний**, то рост составляет **935%**.

Таким образом, за весь 2020 год — данные **1 335 компаний-жертв шифровальщиков** были опубликованы на DLS, а уже за первые три квартала 2021 года — **1 966**, то есть на **47%** больше, чем за весь прошлый год.

Рис. 57. Рост публикаций данных скомпрометированных компаний на DLS, 2020-2021



Подчеркнем, что данная статистика также частично отражает увеличение количества жертв операторов программ-вымогателей, но она не отражает их реального количества. Например, анализ административной панели группы **Hive** и количество опубликованных на DLS данных показывает нам, что только 13% всех жертв преступной группы были выставлены в публичном доступе. Таким образом, реальное количество жертв может быть в 10 раз больше.

В 2020 году самыми активными группами стали **Maze, Egregor, Conti** и **Revil**. Они опубликовали больше всего компаний на DLS:



Рис. 58. Распределение количества жертв по группам операторов, опубликованных на DLS, 2020

В 2021 ситуация меняется — общий процент от количества жертв падает, так как количество мелких групп операторов программ-вымогателей увеличилось. Несмотря на это, Conti остается крупнейшим по количеству жертв, за ним идет Lockbit:



Рис. 59. Распределение количества жертв по группам операторов, 2021

Самой атакуемой страной в 2020 году является США, на втором и третьем месте с большим отставанием идут Канада и Великобритания. Также в топ-5 входят Франция и Германия:



Ситуация практически не меняется в 2021 году и по странам, где сконцентрировано наибольшее количество жертв шифровальщиков. Однако в топ-3 появляется Франция, а Германия смещается на 6-е место.



В региональном срезе в 2020-м и 2021-м годах лидировали Северная Америка, Европа и Азиатско-Тихоокеанский регион:



Рис. 60. Распределение жертв по странам, 2020

Рис. 61. Распределение жертв по странам, 2021

Рис. 62. Распределение жертв по регионам, 2020-2021

Основными атакуемыми отраслями в 2020 году являются производство, недвижимость и транспорт:

Рис. 63. Распределение жертв по отраслям, 2020

Индустрия	Количество
❖ Производство	142
❖ Недвижимость	132
❖ Транспорт	113
❖ Торговля и магазины	82
❖ Профессиональные услуги	81
❖ Здравоохранение	71
❖ ИТ	66
❖ Образование	57
❖ Финансовые услуги	57
❖ Другая промышленность	53
❖ Правительство и вооруженные силы	53
❖ Продукты питания и напитки	50
❖ Наука и инженерное дело	46
❖ Потребительские товары	42
❖ Энергетика	35
❖ Административные услуги	34
❖ Передача сообщений и телекоммуникации	25
❖ Конфиденциальность и безопасность	21
❖ Потребительская электроника	20
❖ Медиа и развлечения	20
❖ Путешествия и туризм	19
❖ Программное обеспечение	16
❖ Одежда и аксессуары	15
❖ Природные ресурсы	14
❖ Оборудование	12
❖ Сельское хозяйство и фермерство	10
Другие	49

Ситуация в 2021 году практически не меняется. Это говорит о том, что злоумышленники обычно ищут одни и те же типы компаний, которые им кажутся наиболее прибыльными.

Рис. 64. Распределение жертв по отраслям, 2021

Индустрия	Количество
❖ Производство	210
❖ Недвижимость	207
❖ Транспорт	178
❖ Профессиональные услуги	169
❖ Финансовые услуги	140
❖ Торговля и шопинг	128
❖ Здравоохранение	125
❖ Другое	104
❖ ИТ	97
❖ Правительство и вооруженные силы	82
❖ Продукты питания и напитки	79
❖ Наука и инженерное дело	75
❖ Образование	70
❖ Энергетика	50
❖ Административные услуги	45
❖ Продукты потребления	43
❖ Оборудования	40
❖ Связи и медиакоммуникации	31
❖ Медиа и развлечения	30
❖ Безопасность	29
❖ Путешествия и туризм	27
❖ Программное обеспечение	27
❖ Одежда и аксессуары	24
❖ Техника	23
❖ Природные ресурсы	23
❖ Продажи и маркетинг	21
❖ Данные и аналитика	18
❖ Агрокультура и фермерство	16
Другие	56

Обзор тактик, техник и процедур в атаках с использованием программ-вымогателей

Активное развитие рынка RaaS, а также смещение фокуса многих финансово-мотивированных групп на организацию атак с использованием программ-вымогателей, значительно повлияло на количество расследуемых инцидентов такого типа.

Более 60% всех расследованных специалистами Group-IB инцидентов пришлось на атаки шифровальщиков за период Q1-Q3 2021. Несмотря на значительный рост подобной активности и вовлеченность различных киберпреступных групп, заметны значительные пересечения с точки зрения тактик, техник и процедур атакующих. При этом набор характерных для атак с использованием программ-вымогателей техник и инструментов остается стабильным. Данный факт может быть обусловлен тем, что неизменный арсенал злоумышленников хорошо зарекомендовал себя и позволяет атакующим достигать своей цели, а также создавать обучающие материалы, которые позволяют вовлекать в подобную деятельность даже неопытных игроков.

Хорошим примером в этом контексте является руководство для партнеров **Conti**, которое в августе 2021 попало в открытый доступ благодаря одному из бывших участников под псевдонимом **m1Geelka**.

60%

всех расследованных специалистами Group-IB инцидентов пришлось на атаки шифровальщиков за период Q1-Q3 2021

Рис. 65. Опубликованное в открытом доступе руководство партнерской программы Conti, 2021

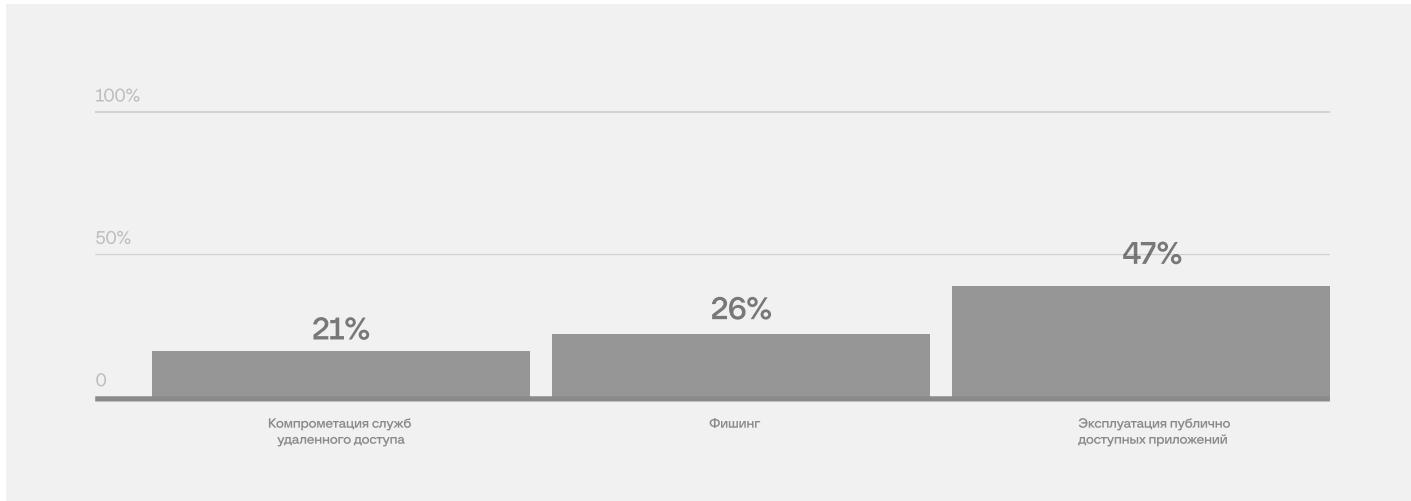
The screenshot shows a forum post from a user named m1Geelka. The post is dated Aug 5, 2021. It contains a warning message: "Please note, if you want to make a deal with this user, that it is blocked." Below this, there is a text block describing a scam where scammers hire penetration testers, collect Active Directory information, and then demand 1500\$ for the data. It also mentions a Tokyo-based scammer named cicada3301@strong.pm. The post includes several attachments showing screenshots of Cobalt Strike interface, specifically the connect dialog, with IP addresses like 185.141.63.120 and 162.244.60.235, port numbers 47734 and 58879, and user names Hookah. There are also other attachments labeled 222.PNG and 7777.PNG. The post has received 10 likes and 10 replies. The user m1Geelka is marked as banned.

Еще одним фактором, в значительной мере повлиявшим на количество и успех атак с использованием программ-вымогателей, послужило развитие рынка брокеров первоначального доступа, что позволило многим атакующим без труда получить доступ к сетям своих жертв.

В целом, как и в прошлом отчетном периоде, наиболее часто используемыми техниками получения первоначального доступа стали:

- компрометация служб удаленного доступа;
- фишинг;
- эксплуатация публично доступных приложений.

Рис. 66. Распределение способов получения первоначального доступа, 2020-2021



Использование RDP и VPN

Наиболее распространенным методом компрометации служб удаленного доступа остаются атаки на публично доступные терминальные серверы с доступными подключениями по протоколу удаленного рабочего стола (RDP). При этом чаще всего атакующим удается получить к ним доступ через перебор паролей, например с использованием NLBrute.

В некоторых случаях атакующие прибегали к эксплуатации, используя эксплойт для уязвимости BlueKeep (CVE-2019-0708). Несмотря на нестабильность, в ряде случаев его использование оказывалось довольно эффективным.

Отсутствие мультифакторной аутентификации позволяло злоумышленникам активно компрометировать учетные записи для подключения через VPN. Более того, ряд уязвимостей, в том числе и довольно старых, например в продуктах Pulse Secure и Fortinet, позволило активно использовать VPN для доступа к корпоративным сетям.

Популярность RDP и VPN прослеживается и на теневых форумах:

RDP

протокол подключения пользователя к удаленному рабочему столу через сервер терминалов

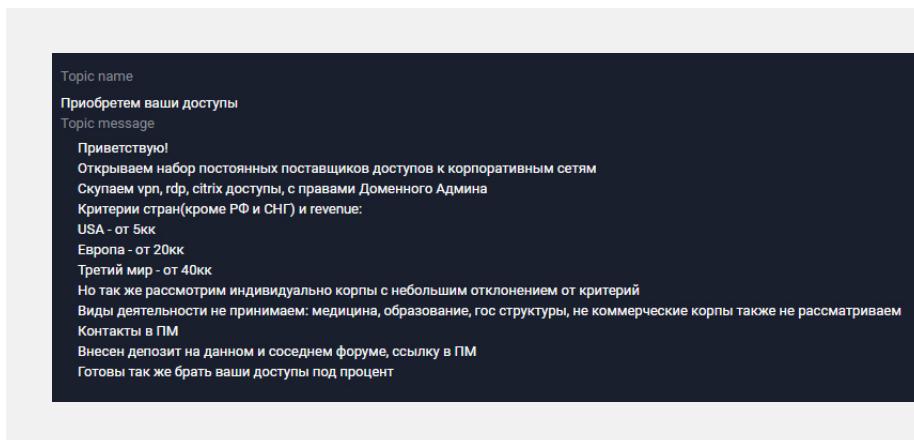


Рис. 67. Объявление о желании приобрести доступ к корпоративным сетям на одном из теневых форумов, 2021

Свежие уязвимости, позволяющие получить первоначальный доступ к сетям, были использованы в атаках с применением программ-вымогателей практически сразу после публикации.

Так партнеры **Conti** и **AvosLocker** активно использовали ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), что позволило им наравне с финансируемыми государствами группами атаковать уязвимые сервера Microsoft Exchange.

Еще один пример — партнеры **HelloKitty**, программы-вымогателя, ставшей хорошо известной после атаки на **CD Projekt RED** — эксплуатировали уязвимые устройства SonicWall, причем сначала используя старую уязвимость (CVE-2019-7481), а впоследствии и свежую (CVE-2021-20016).

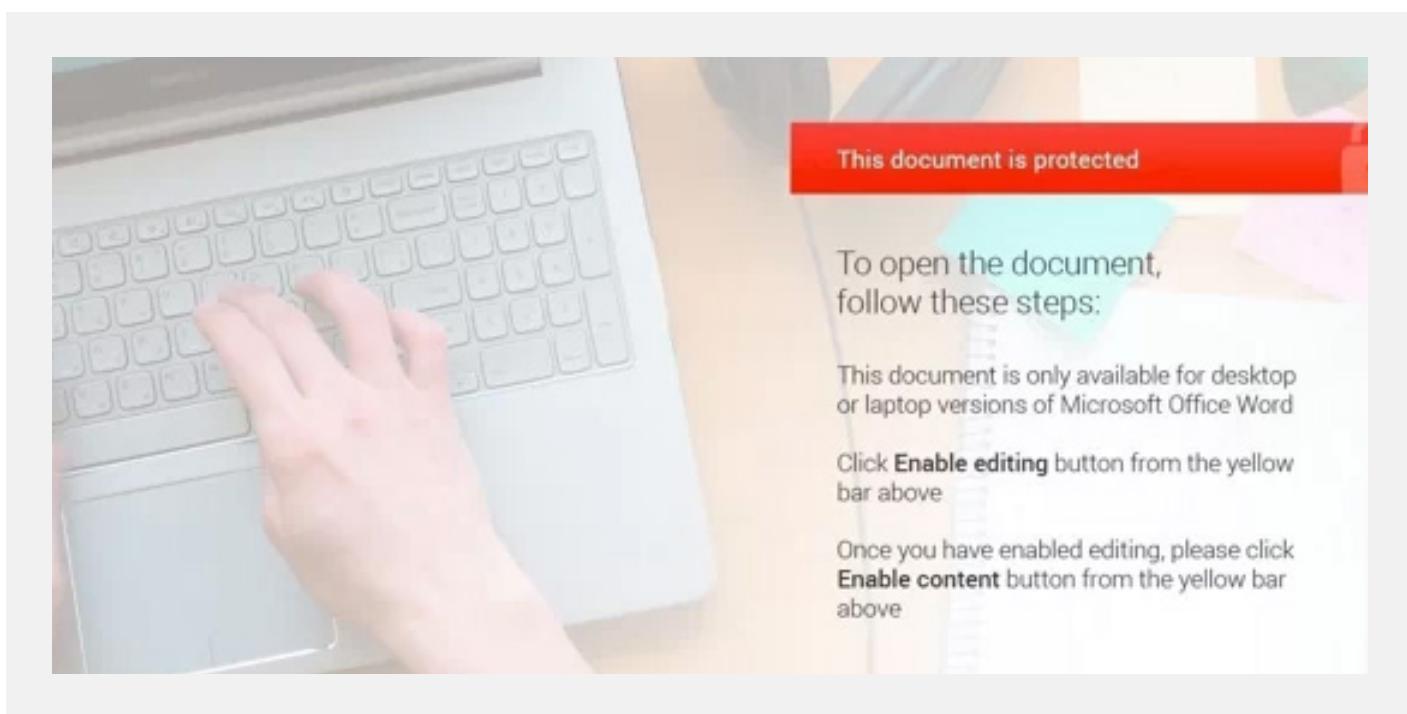
В некоторых случаях злоумышленникам удавалось получить доступ к так называемым уязвимостям нулевого дня. Показательным примером является атака партнеров **REvil** на компанию **Kaseya** с использованием уязвимостей нулевого дня, которые впоследствии получили следующие идентификаторы: CVE-2021-30116, CVE-2021-30119 и CVE-2021-30120.

Использование бот-сетей

Для получения первоначального доступа операторами программ-вымогателей продолжают активно использовать популярные бот-сети, в частности **IcedID**, **Qakbot**, **Hancitor**, **Trickbot** и другие.

Зачастую содержимое рассылаемых писем довольно тривиально, а вредоносный документ содержит инструкции по запуску макроса, который и загрузит бот на скомпрометированный компьютер.

Рис. 68. Содержимое вредоносного документа, используемое операторами Hancitor, 2021



В некоторых случаях атакующие также использовали уязвимости для загрузки и запуска вредоносного кода. Например, операторы **BazarLoader**, активно участвующие в распространении программы-вымогателя **Ryuk**, использовали уязвимость в MSHTML (CVE-2021-40444), чтобы заразить распространяемые по электронной почте документы.

Помимо традиционного фишинга операторы BazarLoader использовали и **виишинг**. Они рассыпали электронные письма с информацией о платной подписке и номером телефона для ее отмены. Звонящую по номеру жертву убеждали перейти на сайт и загрузить форму для отказа от подписки, которая, разумеется, была вредоносным документом.

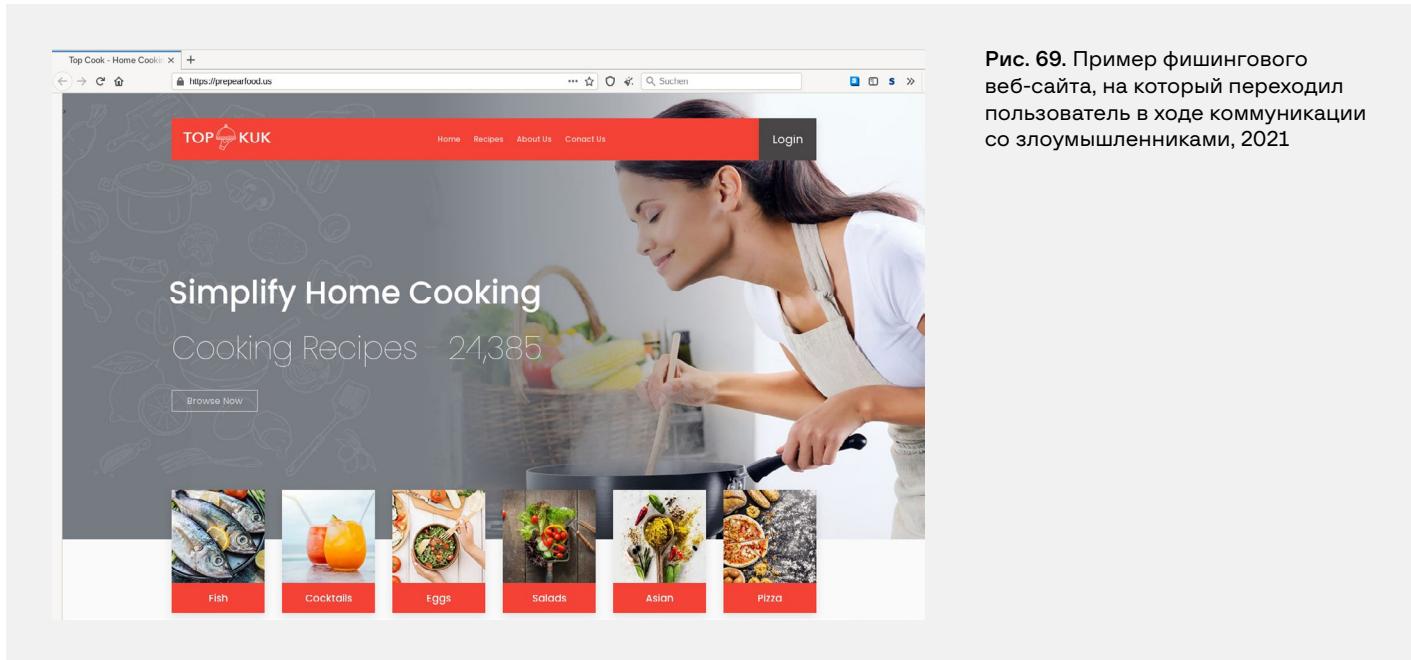
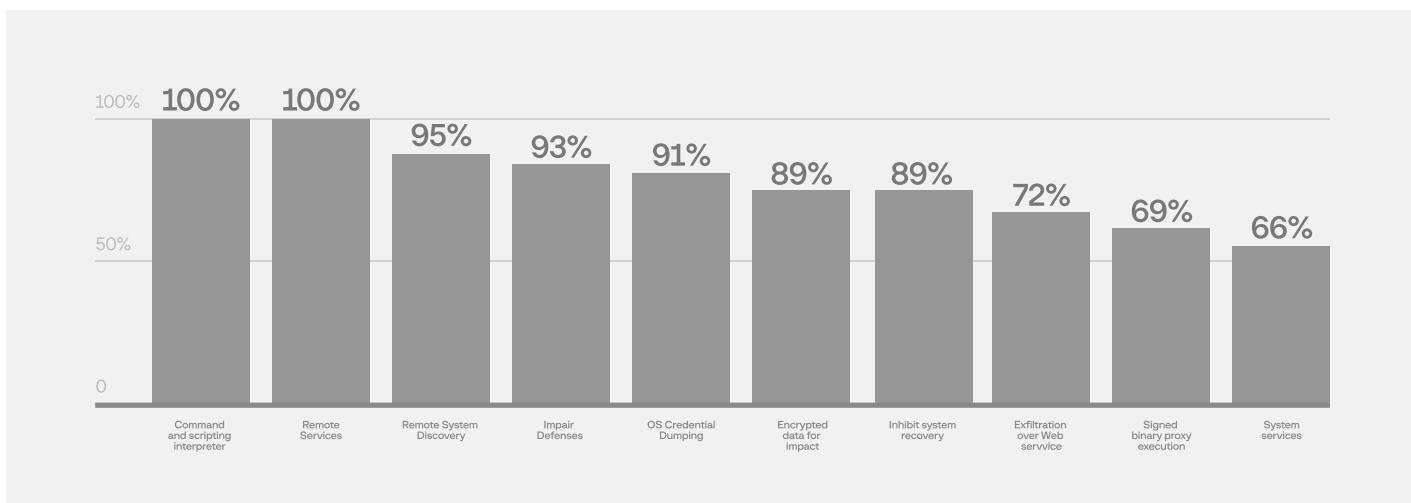


Рис. 69. Пример фишингового веб-сайта, на который переходил пользователь в ходе коммуникации со злоумышленниками, 2021

Техники постэксплуатации

Что касается постэксплуатации, эксперты Group-IB выделили наиболее часто используемые атакующими техники в зависимости от того, насколько часто они встречались в инцидентах.

Рис. 70. Популярные техники атакующих, 2020-2021



Использование интерпретаторов команд и сценариев

Традиционно атакующими широко применяются различные интерпретаторы команд и сценариев. Они использовались злоумышленниками в 100% инцидентов, в расследовании которых участвовали специалисты Group-IB.

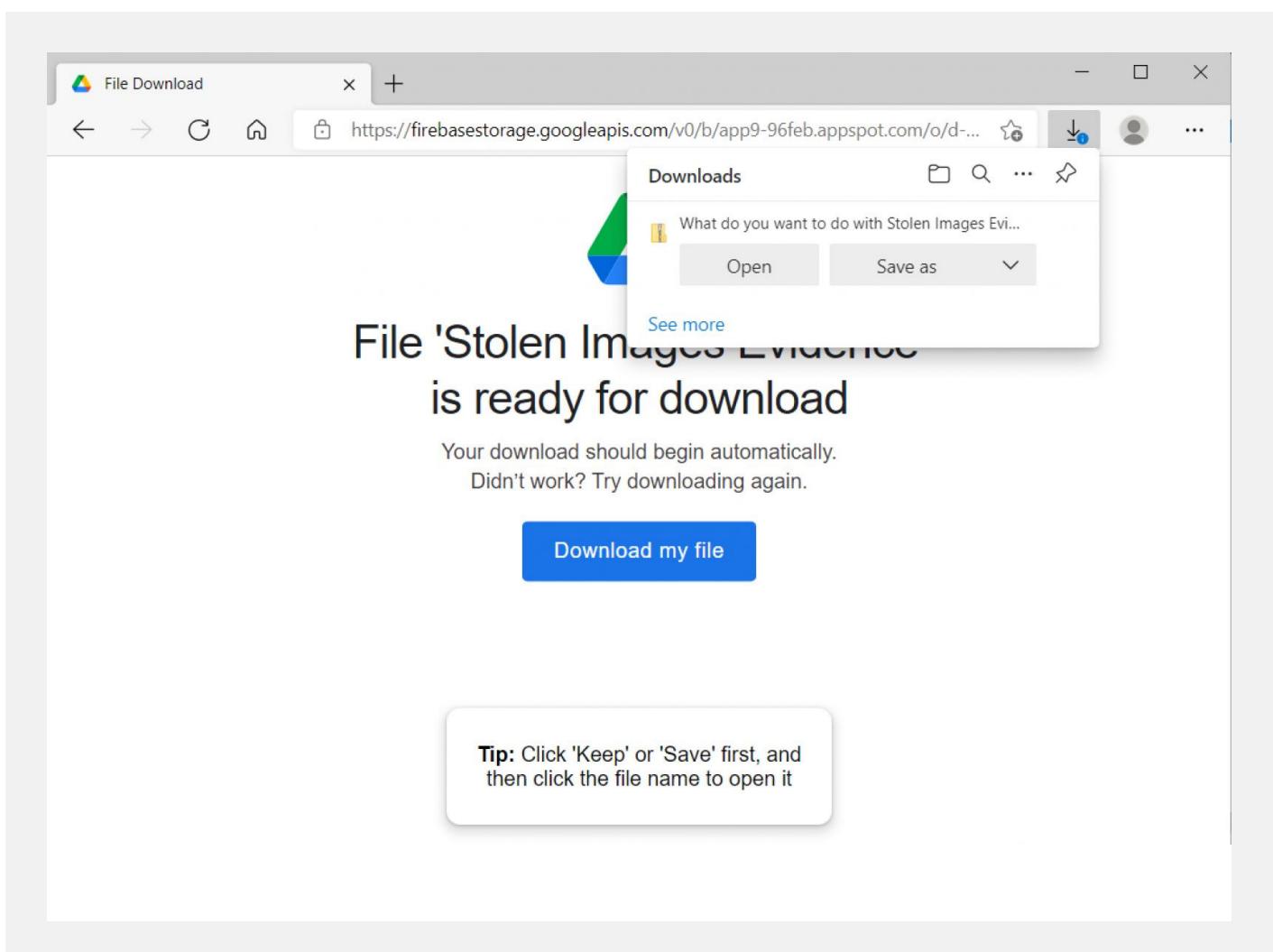
Особенно следует выделить следующие интерпретаторы:

- командная строка Windows;
- PowerShell;
- Visual Basic;
- JavaScript.

Если первые два традиционно используются злоумышленниками на различных стадиях жизненного цикла атаки, то Visual Basic активно эксплуатируется вредоносными макросами. JavaScript встречается реже, что негативно влияет на детектируемость и повышает вероятность успешной компрометации.

Операторы IcedID, успевшие поработать с представителями самых разных партнерских программ, использовали файлы JavaScript, упакованные в ZIP-архивы для доставки полезной нагрузки. При этом ссылки на такие архивы размещались на Google-сайтах, что снижало бдительность жертв. Более того, жертве предлагалось войти в свой Google-аккаунт, после чего загрузка архива происходила автоматически.

Рис. 71. Архив с вредоносным файлом JavaScript, 2021



Отдельного внимания заслуживает группа **OldGremlin**, атаковавшая компании на территории России и активно использующая интерпретатор NodeJS.

В большинстве случаев доступ к корпоративной сети – лишь первый этап жизненного цикла атаки. Злоумышленники используют любые доступные средства, чтобы повысить имеющиеся привилегии и начать продвижение по сети. Это подтверждает тот факт, что в **100%** случаев мы видели использование **служб удаленного доступа**.

Одним из наиболее распространенных методов остается протокол удаленного рабочего стола (RDP). Некоторые группы даже имеют в своем арсенале сценарии для включения возможности подобного доступа.

Например, такой сценарий использовали партнеры **REvil**:

```
(Get-WmiObject Win32_TerminalServiceSetting -Namespace root\cimv2\TerminalServices).SetAllowTsConnections(1,1)
(Get-WmiObject -Class «Win32_TSGeneralSetting» -Namespace root\cimv2\TerminalServices -Filter «TerminalName='RDP-tcp'»).SetUserAuthenticationRequired(0)
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -name «UserAuthentication» -Value 1
Enable-NetFirewallRule -DisplayGroup «Remote Desktop»
```

Разумеется, не меньшей популярностью пользуется и протокол Server Message Block (SMB), причем как для продвижения по сети, так и для развертывания программ-вымогателей.

Методы сбора информации об удаленных системах

Говоря о продвижении по сети, нельзя не упомянуть методы **сбора информации об удаленных системах**. Атакующие активно используют различные сетевые сканеры, а также средства сбора информации об Active Directory. Впрочем, в некоторых случаях использовались и встроенные административные средства Windows, например, PowerShell:

```
Get-ADComputer -Filter {enabled -eq $true} -properties * | select Name, DNSHostName, OperatingSystem, LastLogonDate | Export-Csv C:\temp\AllWindows.csv -NoTypeInformation -Encoding UTF8
```

Сценарии нейтрализации средств защиты

Успешное развертывание программы-вымогателя едва ли возможно без **нейтрализации средств защиты**. Зачастую для этого используются заранее подготовленные сценарии, которые выполняются на целевых хостах через модификацию групповой политики или PsExec. Кроме того, многие экземпляры программ вымогателей также содержат списки процессов и служб, относящихся к средствам защиты, которые будут остановлены в ходе выполнения вредоносной программы. Например, среди строк, которые использовались экземпляром программы-вымогателя **BlackMatter** для идентификации процессов и служб для последующей остановки, была строка sophos, указывающая на популярное средство антивирусной защиты.

Дампинг учетных данных

Своей популярности не теряет **дампинг учетных данных**. Помимо популярных инструментов, например, Mimikatz, которые легко детектируются средствами защиты, атакующие начали использовать и менее привлекающие внимание методы, в том числе и основанные на эксплуатации встроенных в Windows средств. Например, comsvcs.dll — библиотеку, которая позволяет осуществить дамп памяти определенного процесса, в том числе lsass.exe:

```
rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 900  
C:\Users\Public\lsass.dmp full
```

Непосредственно **шифрование данных с целью получения выкупа** осуществлялось атакующими лишь в **89% инцидентов**, на которые реагировали специалисты Group-IB. Это связано с тем, что в части инцидентов злоумышленники ограничились лишь выгрузкой данных, либо наши клиенты обнаружили подозрительную активность до развертывания программы-вымогателя.

В таком же проценте инцидентов атакующие **нарушали средства восстановления системы**, а именно теневые копии Windows. Такой функционал был включен как непосредственно в программы-вымогатели, так и мог реализовываться посредством сценариев. Обычно для этого эксплуатировался либо vssadmin, либо Windows Management Instrumentation, например:

```
wmic shadowcopy delete /nointeractive
```

Использование веб-сервисов

Многие группы, вовлеченные в атаки с использованием программ-вымогателей, все еще активно выгружают данные из скомпрометированных сетей. Часто для этого используются **веб-сервисы**. Особенно популярны различные облачные хранилища. MEGA, DropMeFiles, SendSpace – вот лишь некоторые примеры таких хранилищ.

Выполнение кода через подписанное приложение

Говоря о популярных техниках постэксплуатации, нельзя оставить без внимания **выполнение кода через подписанное приложение**. Яркими примерами реализации этой техники является эксплуатация rundll32.exe и regsvr32.exe. Например, операторы IcedID использовали rundll32.exe для запуска загруженной полезной нагрузки:

```
C:\Windows\System32\rundll32.exe  
«C:\users\public\leftSwapStorage.jpg,PluginInit
```

Использование системных служб

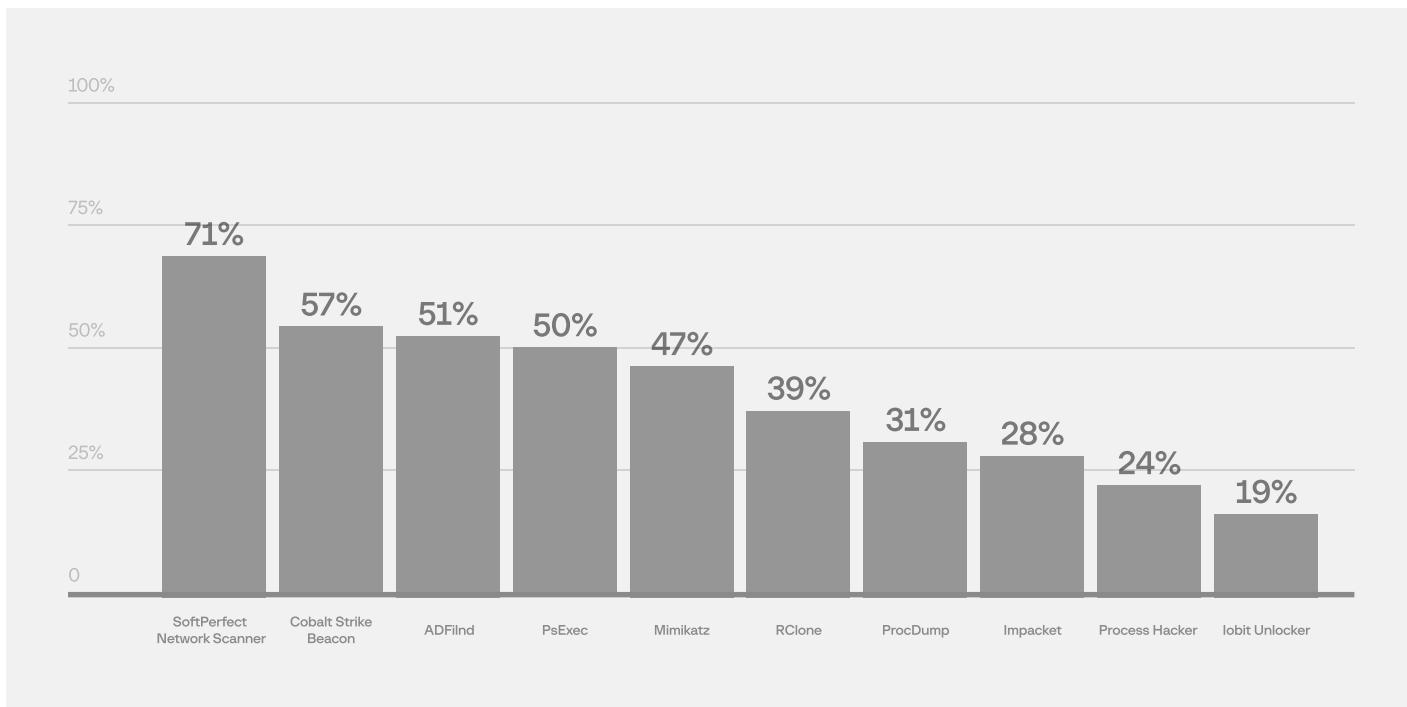
Последней техникой, которая вошла в список десяти самых популярных, является использование системных служб. Это по большей части связано с тем, что злоумышленники активно используют **PsExec** и его реализации, в том числе те, которые являются частью постэксплуатационных фреймворков, например Cobalt Strike.

Шифрование данных с целью получения выкупа осуществлялось атакующими лишь в 89% инцидентов, на которые реагировали специалисты Group-IB

ТОП-10 самых популярных инструментов, используемых в атаках программ-вымогателей

Ниже – список из десяти самых популярных инструментов, которые эксперты Group-IB встречали в ходе реагирований на атаки, связанные с использованием программ-вымогателей.

Рис. 72. Самые популярные инструменты операторов программ-вымогателей по версии Group-IB, 2021



Как уже отмечалось, одной из ключевых задач злоумышленников является идентификация удаленных систем с целью дальнейшего продвижения или развертывания программы-вымогателя. Наиболее популярным инструментом для ее реализации стал **SoftPerfect Network Scanner** – популярный коммерческий сетевой сканер, который был частью арсенала атакующих в 71% атак, которые довелось расследовать.

Еще одним очень популярным инструментом стал **Cobalt Strike**. Специалисты Group-IB обнаруживали следы его использования в 57% случаев. В некоторых случаях атакующие использовали **Beacon**, основную полезную нагрузку Cobalt Strike, вместо ботов в рамках фишинговых рассылок. Так, например, атакующие рассыпали фишинговые письма с вредоносными документами для доставки загрузчика Squirrelwaffle, который в свою очередь использовался для загрузки Cobalt Strike Beacon.

Практически наравне с Cobalt Strike злоумышленниками использовался **ADFind** – инструмент для сбора информации об Active Directory. Часто атакующие загружали его на ранних стадиях, чтобы изучить скомпрометированную инфраструктуру. Обычно для его запуска использовались сценарии, например:

```
adfind.exe -f «(objectcategory=person)»
adfind.exe -f «(objectcategory=organizationalUnit)»
adfind.exe -f «(objectcategory=computer)»
adfind.exe -gcb -sc trustdmp
adfind.exe -f «(objectcategory=group)»
adfind.exe -subnets -f (objectCategory=subnet)
adfind.exe -sc trustdmp
```

Как уже отмечалось, одной из задач злоумышленников является продвижение по сети, в том числе выполнение команд и вредоносного кода на удаленных хостах. В связи с этим в половине инцидентов были следы использования **PsExec**, причем как для запуска команд, так и непосредственно для распространения программы-вымогателя.

Mimikatz, инструмент для извлечения учетных данных и памяти, не теряет своей актуальности. Более того, злоумышленники используют и его варианты, например, PowerShell-версию Invoke-Mimikatz и Python-версию Pupykatz.

Некоторые операторы программ-вымогателей решили облегчить жизнь своим партнерам, обогатив их арсенал инструментами для автоматического сбора и выгрузки данных. Хорошим примером является StealBit от операторов вымогателя LockBit. Тем не менее, многие партнеры все еще выгружают данные своими средствами. Наиболее популярным инструментом для решения этой задачи стал **RClone**. Его специалисты Group-IB видели в 39% инцидентов.

Так как популярные инструменты для извлечения учетных данных из памяти довольно легко детектируются, ряд злоумышленников использует легитимные инструменты для дампинга lsass.exe. В 31% инцидентов фиксировали использование **ProcDump**.

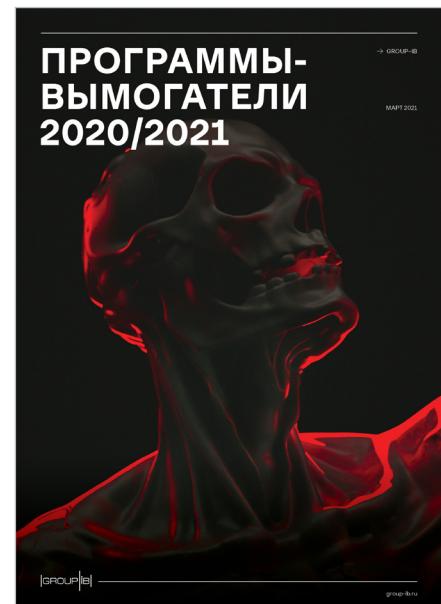
Помимо PsExec, для выполнения команд на удаленных хостах злоумышленниками активно использовался сценарий SMBExec из пакета **Impacket**. Его использование фиксировало в 28% инцидентов.

Популярный инструмент для мониторинга системных ресурсов, **Process Hacker**, также активно использовался для сбора информации об имеющихся средствах защиты и их последующей нейтрализации.

Еще одним инструментом, который использовался злоумышленниками для решения схожих задач – **l0bit Unlocker**. Его применение обнаружено в 19% атак, и использовался он в том числе для завершения процессов, взаимодействующих, например, с базами данных и препятствующих их шифрованию.

Представленные техники и инструменты не являются исчерпывающими, подробный анализ тактик, техник и процедур характерных для атак с использованием программ-вымогателей будет доступен в отчете **«Программы-вымогатели 2021-2022»**.

Программы-вымогатели 2020/2021



ЗАКУЛИСЬЕ МИРА КИБЕРВЫМОГАТЕЛЕЙ

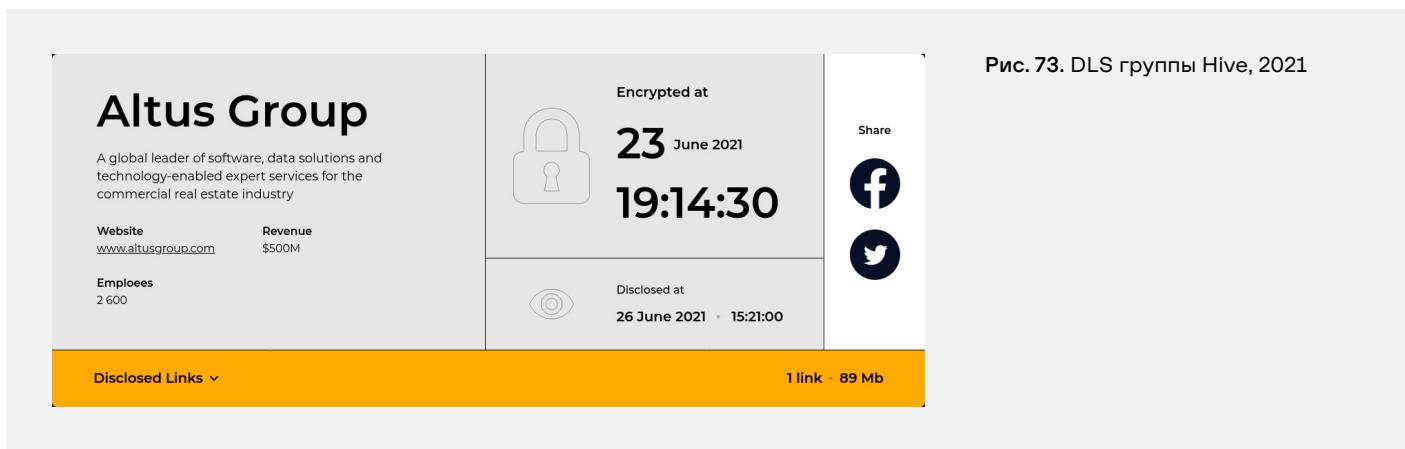
Партнерские программы изнутри, активность групп на форумах и статистика атак Hive. Как выглядит интерфейс партнерской программы

HI-TECH CRIME TRENDS 2021/2022

GROUP-IB.RU

История Hive и разбор DLS

Впервые активность преступной группы **Hive** была обнаружена в июне 2021 года. А 25 июля 2021 у преступной группы появляется DLS уже с одной жертвой.



Altus Group

A global leader of software, data solutions and technology-enabled expert services for the commercial real estate industry

Website: www.altusgroup.com Revenue: \$500M

Employees: 2 600

Encrypted at: 23 June 2021 19:14:30

Disclosed at: 26 June 2021 15:21:00

Share: [Facebook](#) [Twitter](#)

Disclosed Links: 1 link · 89 Mb

Рис. 73. DLS группы Hive, 2021

Hive использует комбинацию AES и RSA для шифрования данных жертвы. После того как данные зашифрованы, программа загружает их на удаленный сервер. Зашифрованные файлы можно узнать по расширению .hive.

У группы Hive не было публичных партнерских программ, поэтому изначально не было понятно, работает ли Hive по принципу RaaS или же это закрытая группа, вход в которую невозможен.

DLS отличался тем, что работал при помощи API. Кроме Hive есть только 2 группы, которые использовали API – **Grief** и **DoppelPaymer**.

```

▼ GET
  Scheme: http
  Host: hiveapi4nyabjdfz2hxdsr7otrcv6zq6m4rk5i2w7j64lrtny4b7vjad.onion
  Filename: /v1/companies/disclosed

▼ JSON
  ▼ 0: Object { id: "A8H1S4VA3jL_com", title: "Palacios & Asociados", description: "Logistics Operator that provides comprehensive solutions in customs agency, cargo, transportation, storage and advice in different jurisdictions throughout the Peruvian territory.", ... }
    id: "A8H1S4VA3jL_com"
    title: "Palacios & Asociados"
    description: "Logistics Operator that provides comprehensive solutions in customs agency, cargo, transportation, storage and advice in different jurisdictions throughout the Peruvian territory."
    country: null
    tax_number: null
    website: "https://www.pasoc.pe"
    revenue: null
    employees: null
    disclose_at: null
    encrypted_at: "2021-07-01T04:40:00Z"
    disclosed_at: "2021-07-30T17:02:30Z"
  ▼ 1: Object { id: "AcFdjHAqmXg_com", title: "Erik Buell Racing", website: "https://www.ebr.com", ... }
    id: "AcFdjHAqmXg_com"
    title: "Erik Buell Racing"
    description: null
  
```

Рис. 74. Ответ с сервера злоумышленников, 2021

Украденные файлы группировка Hive выкладывала на файлообменники: **sendspace**, **anonfiles**, **send.exploit** и другие. Интересно, что размер выложенных файлов часто находился в пределах 500 MB, и только одна утечка весила более 200 GB.

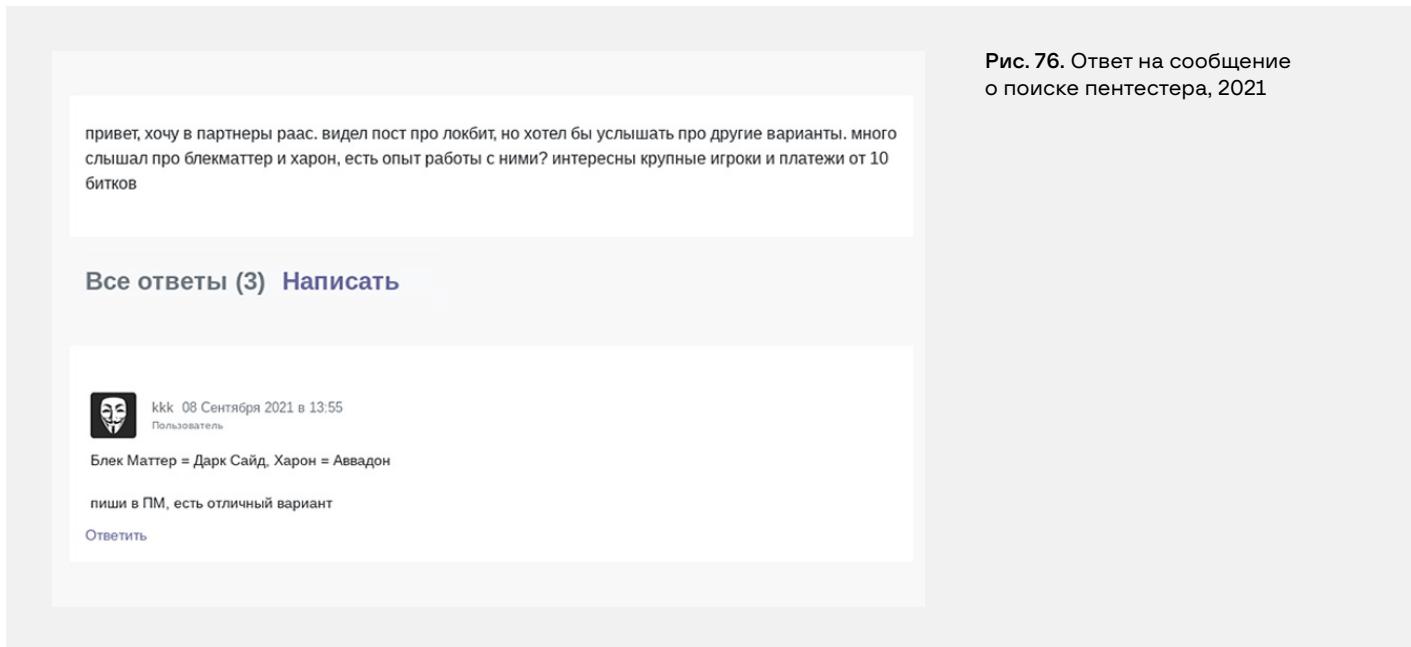
Hive и RAMP

7 сентября 2021 года на закрытом форуме RAMP было опубликовано сообщение от пользователя kkk, который рекламировал партнёрскую программу.



Рис. 75. Сообщение о поиске пентестера, 2021

В партнёрскую программу требуются пентестеры со своими таргетами
Поддерживаемые ОС: Windows x86/x64, Linux x86/x64, Freebsd (Freenas), ESXi начиная с 6.7.0, в
процессе написания версия под все ESXi.
Админка в Tor с чатом, блог. Бекэнд API не боится RCE, SQLi
Полное описание по запросу в ПМ. Выплаты на ваш кошелёк.
Рейт: 80/20



В ходе общения с указанным злоумышленником была получена детальная информация о данном вредоносном ПО:

Note 3rFNnyte

Note deleted, be sure to copy the data before closing the page

- пропускает файлы по регулярному выражению
 - Каждый файл шифруется отдельным уникальным ключом, пятнами по 4096 байт, начало, конец и далее в зависимости от размера файла
 - Быстрый и многопоточный (очень высокая скорость за счет неизменного конечного размера файла)
 - Отсутствуют зависимости от внешних библиотек
 - Запускается в скрытом режиме, если был запуск через консоль, выводит лог в нее (Windows)
 - Очищает все дисковое пространство (можно отключить, сетевые диски пропускает)

Размер сжатого файла: ~825Kb для Windows, ~786Kb для Linux

Админка в тор с чатом, есть блог. Бекэнд API не боится RCE, SQLi

Скорость 4.5 гига в минуту. До этого была скорость 0.9гб в минуту. Кодогенерация на каждый билд

Copy data

Когда эксперты Group-IB увидели характеристики программы-вымогателя, то предположили, что это Hive. Последующие общение с kkk это подтвердило.

Рис. 76. Ответ на сообщение о поиске пентестера, 2021

Партнерская программа Hive изнутри

В ходе общения со злоумышленником был получен доступ к закрытой партнерской программе. Злоумышленник предоставил адрес административной панели и аутентификационные данные для входа в неё.

[hxxp://hiveaffi5ci2xxaz2fjfrfi5mwpqvuw4wtomc3fflzcopxt2654ryqd\[.\]onion/auth](http://hiveaffi5ci2xxaz2fjfrfi5mwpqvuw4wtomc3fflzcopxt2654ryqd[.]onion/auth) при переходе по адресу административной панели специалисты Group-IB подтвердили гипотезу, что это партнерская программа Hive.

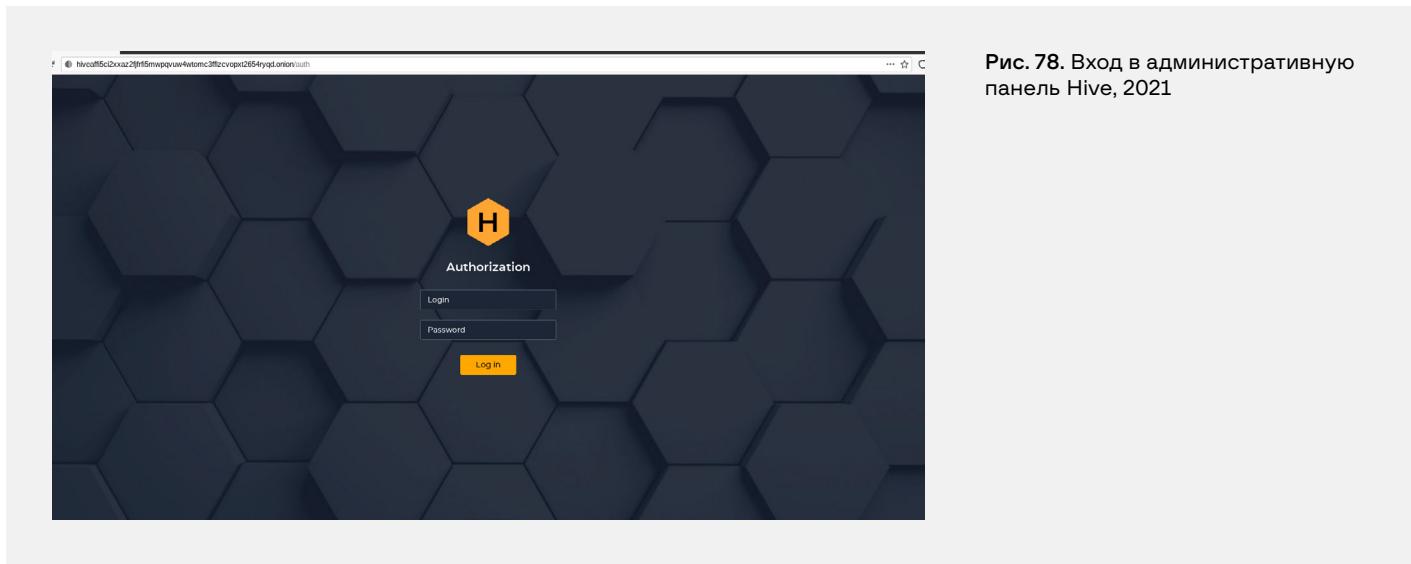


Рис. 78. Вход в административную панель Hive, 2021

После ввода логина и пароля, выданных злоумышленником, открывается главная страница партнерской программы.

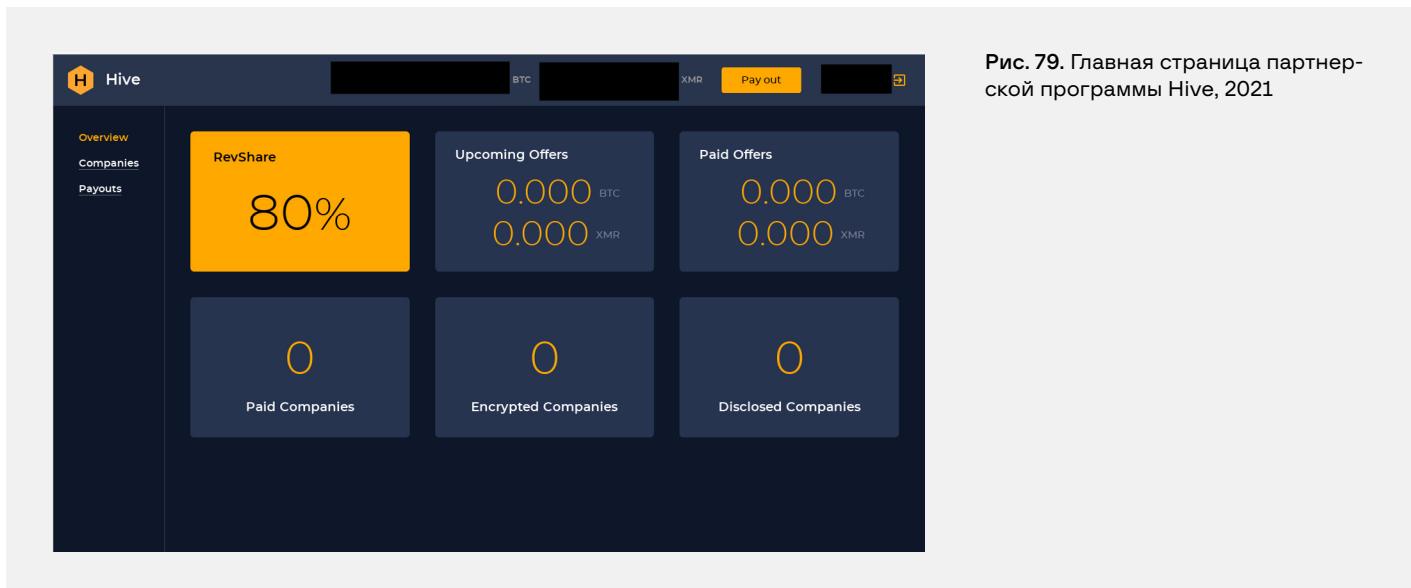


Рис. 79. Главная страница партнерской программы Hive, 2021

Здесь приводится краткая статистика: какой процент от выкупа получает злоумышленник, сколько должен получить в будущем, сколько уже получил, количество заплативших, зашифрованных и раскрытых компаний, а также общий баланс и логин. Вкладка Payouts отвечает за вывод средств с партнерской программы на личный кошелек злоумышленника.

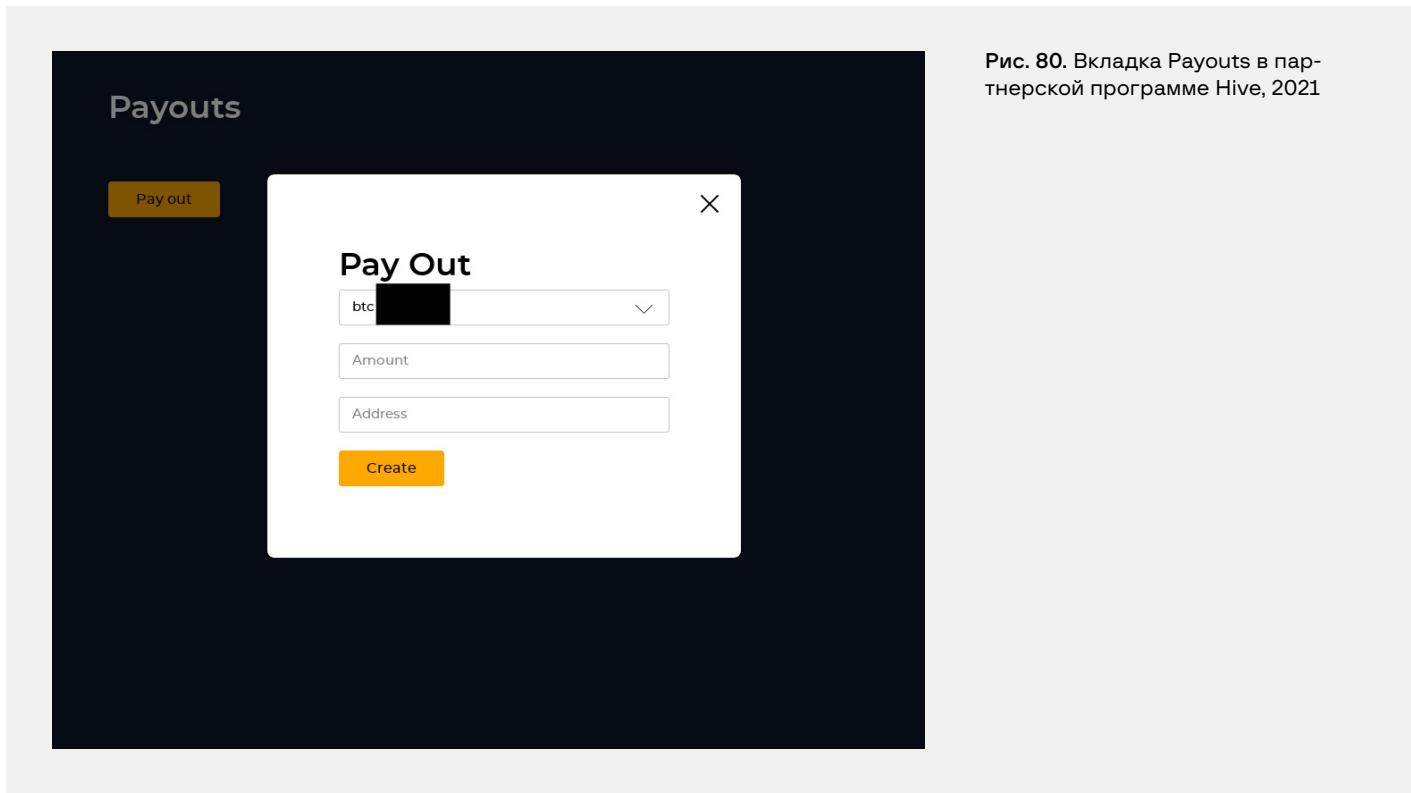


Рис. 80. Вкладка Payouts в партнерской программе Hive, 2021

Наиболее интересные данные находятся в разделе Companies. Здесь злоумышленник указывает название компании жертвы, её сайт, дает краткое описание, а также может указать её выручку и количество сотрудников.

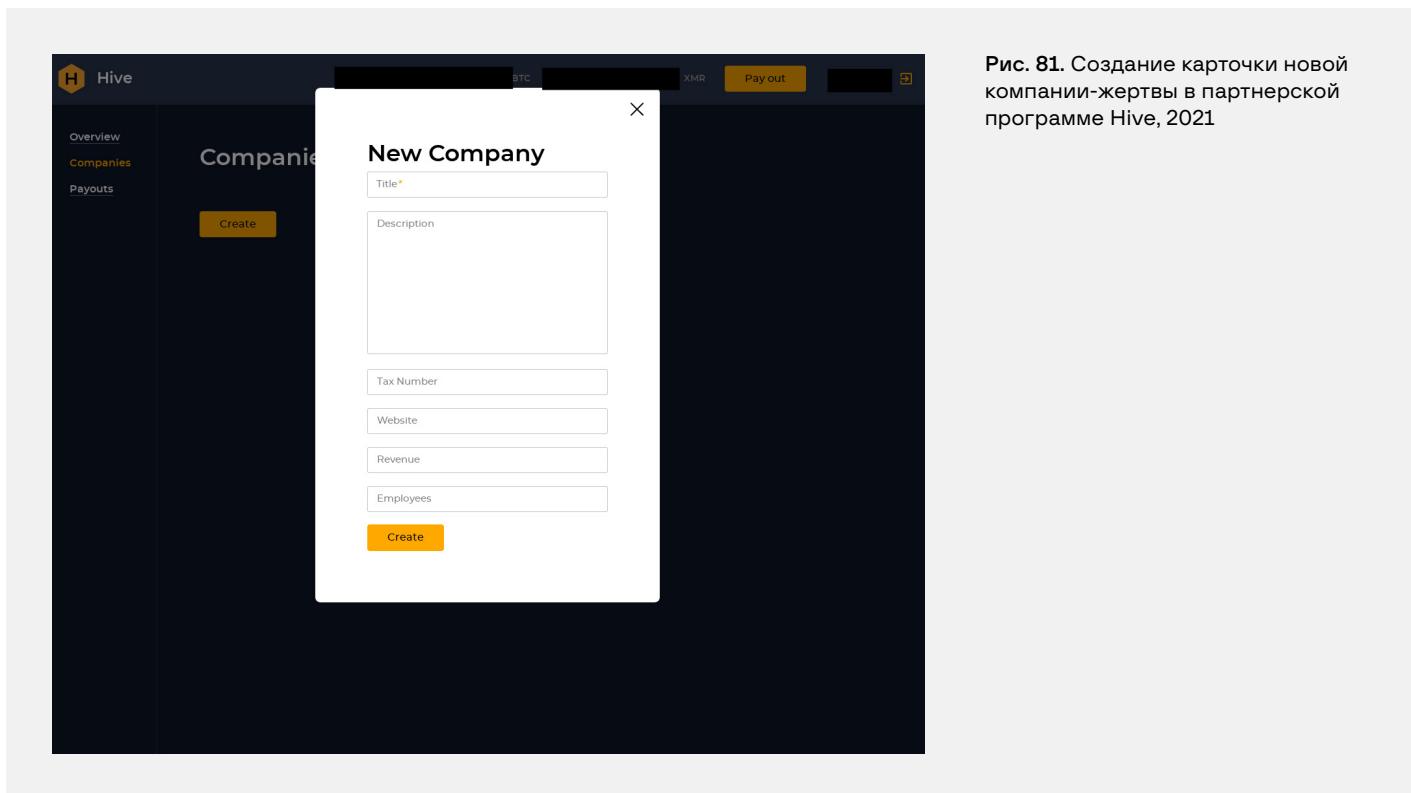


Рис. 81. Создание карточки новой компании-жертвы в партнерской программе Hive, 2021

После заполнения информации о жертве злоумышленник увидит следующую картину:

The screenshot shows a dark-themed web interface for the Hive partner program. At the top, there are currency options: BTC, XMR, and Pay out. Below the header, a sidebar on the left lists 'Overview', 'Companies' (which is selected and highlighted in blue), and 'Payouts'. The main content area is titled 'Companies' and displays a single row for a company named 'Test'. The row includes columns for 'Title' (Test), 'Activity' (80%), 'RevShare' (—), 'Offer' (—), 'Expires at' (—), and 'Status' (created). A yellow 'Create' button is located below the row. The background of the main content area is dark, and the overall design is modern and minimalist.

Если перейти на эту карточку компании, то слева на странице будет отображена краткая информация, появится возможность оставить комментарий для администратора, а также обновить информацию о жертве. В правой части злоумышленник может скачать программу-вымогатель для будущей компании-жертвы, а также отметить, удалось ли зашифровать данные компании.

The screenshot shows a detailed view of a company profile ('Test') within the Hive partner program. The left sidebar contains basic company information: Title (Test), Status (created), Website (tesr.com), Tax Number (00000), Revenue (\$1M), and Employees (1000). It also includes a 'Comments for admin' input field and an 'Update' button. The right side of the screen is dominated by a large yellow callout box. Inside the box, there's a large stylized letter 'T' and the text 'Encryption software' with a subtext 'Should be run on every machine in company's network'. Below this is a 'Download' button. To the right, a section titled 'Confirm encryption process ends' with the subtext 'Your may cancel the company when you are unable to encrypt it.' contains 'Confirm' and 'Cancel' buttons. At the bottom of the yellow box, there's a 'Disclosure links' section with the subtext 'This links will be publicly disclosed when the company refuses to pay.' and an 'Add link' button. The overall design is clean and professional, with a strong emphasis on the yellow color scheme.

Рис. 82. Вкладка со списком компаний-жертв в партнерской программе Hive, 2021

Генерация программы-вымогателя может занимать до 15 минут. Если компания откажется платить выкуп, можно добавить ссылку, которая будет опубликована в блоге Hive.

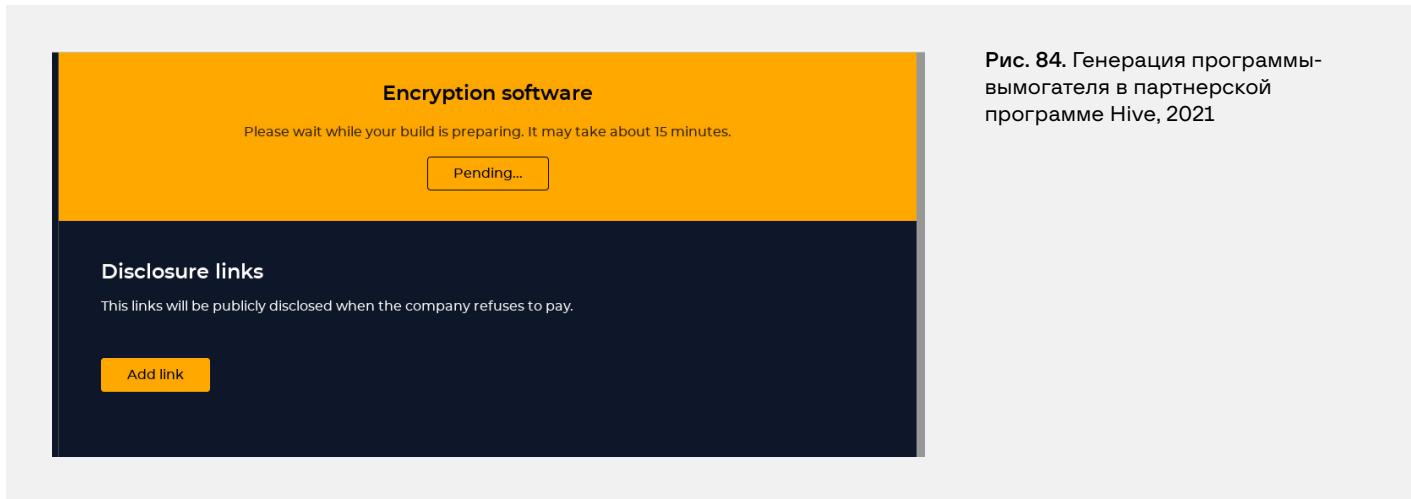


Рис. 84. Генерация программы-вымогателя в партнерской программе Hive, 2021

После создания программы-вымогателя будет сгенерирован архив .rar со следующими файлами:

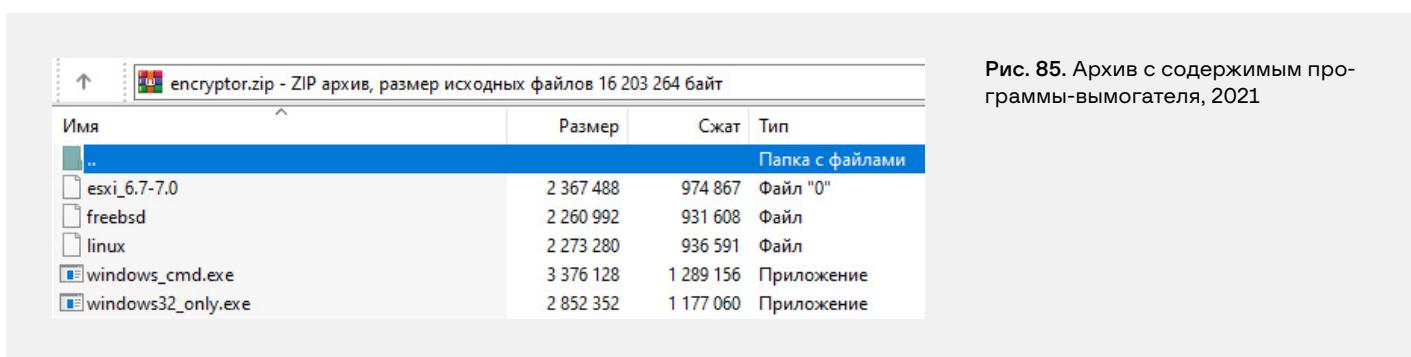


Рис. 85. Архив с содержимым программы-вымогателя, 2021

После заражения жертвы будет автоматически создана записка с запросом выкупа, в которой будет ссылка на сайт, а также логин и пароль для доступа:

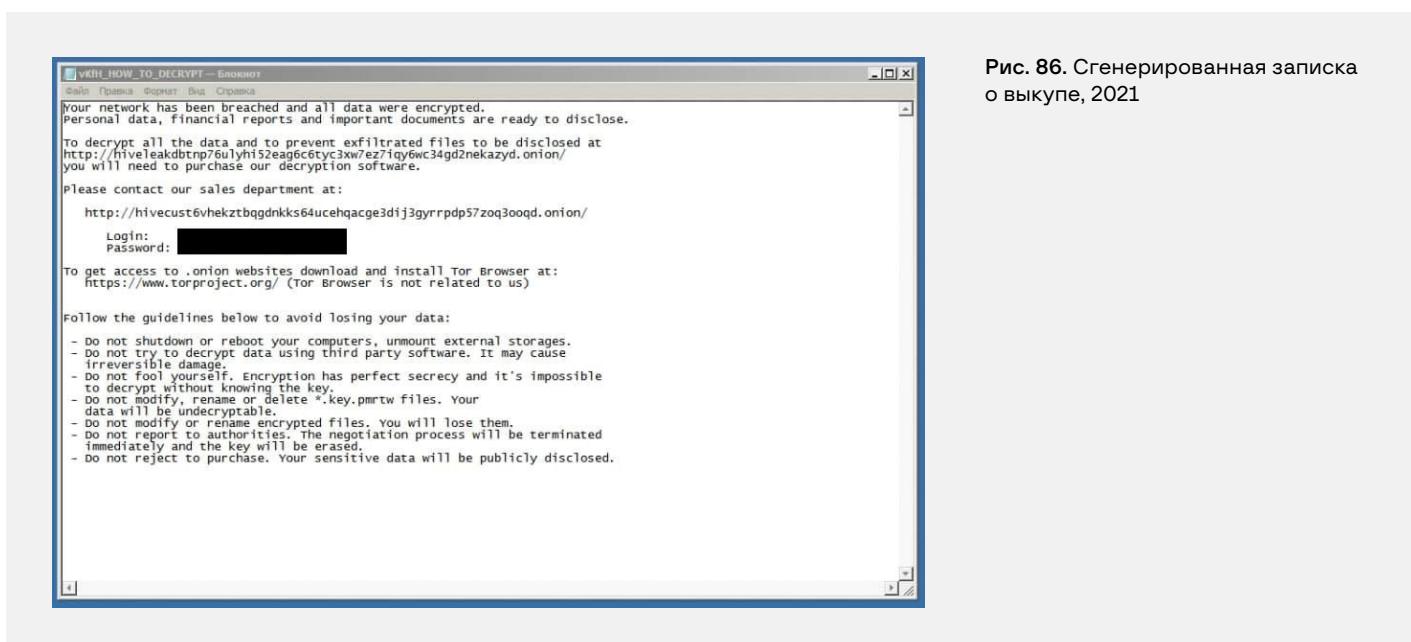


Рис. 86. Сгенерированная записка о выкупе, 2021

Если злоумышленник подтверждает, что компания была зашифрована, будет открыт чат с жертвой. Но сейчас общение с жертвой происходит следующим образом:

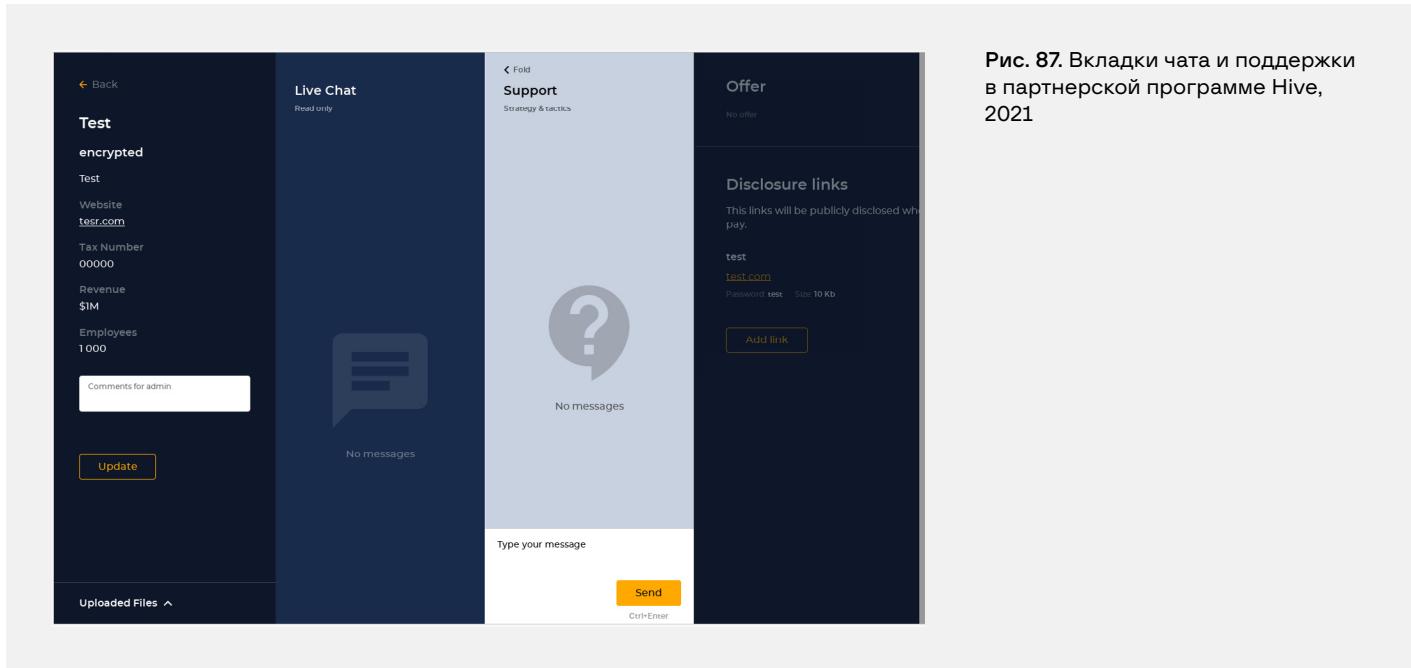


Рис. 87. Вкладки чата и поддержки в партнерской программе Hive, 2021

1. Жертва оставляет сообщение в чат с администратором (слева), этот чат виден и злоумышленнику.
2. Злоумышленник пишет администратору (справа).
3. Администратор пересыпает сообщение в чат с жертвой.

В этой схеме жертва и злоумышленник не общаются напрямую, и все общение идет через администратора.

После того как жертва заплатит выкуп, она сможет получить декриптор с инструкцией его использования.

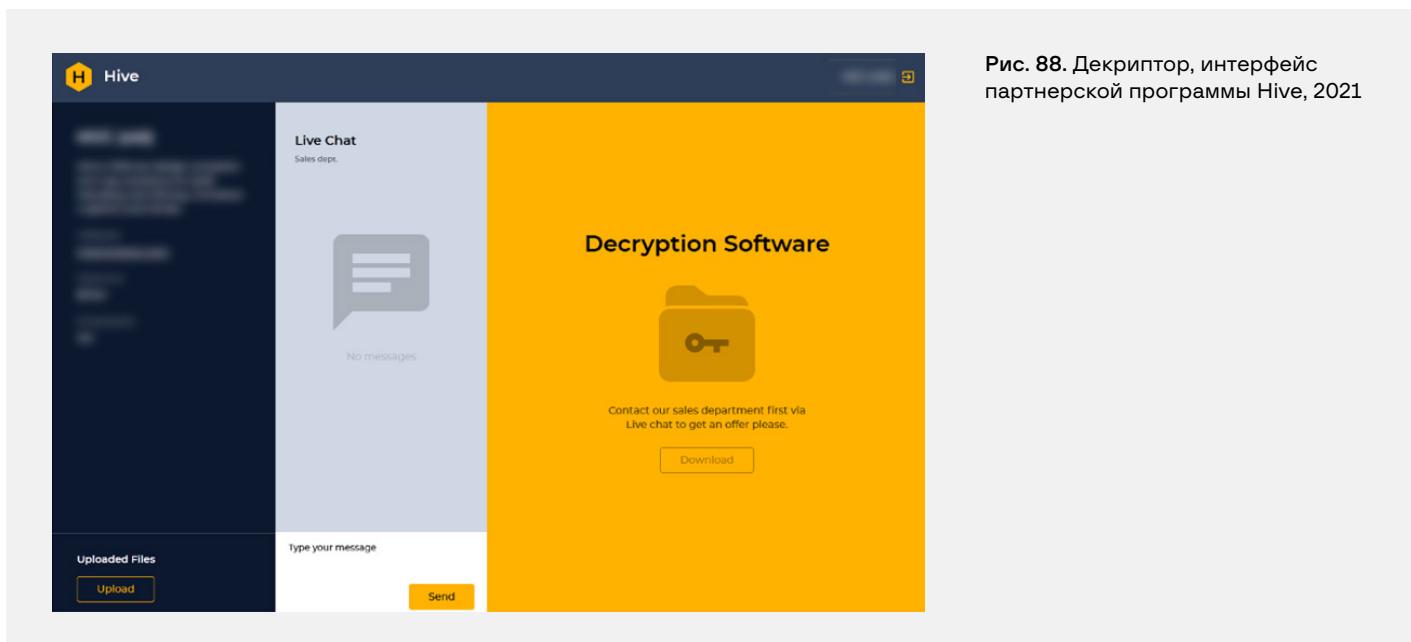


Рис. 88. Декриптор, интерфейс партнерской программы Hive, 2021

Реальное количество жертв Hive и технические особенности сайта группы

В начале сентября 2021 года в партнерской программе Hive была создана **181 компания**, а в конце октября их было уже **312**. Административная панель Hive и DLS работают с использованием API. Каждой компании присваивается уникальный ID, который также можно найти на DLS.

«Компании, которые вели переписку с операторами Hive, и их данные не были опубликованы» — жертва имеет сообщения в чате со злоумышленником, но при этом данные жертвы не публиковались на DLS; «Компании, которые не вступали в переписку с операторами и данные которых не были выложены на DLS» — жертва имеет 0 сообщений в чате со злоумышленником, но при этом данные жертвы не публикуются на DLS

```

    ▼ JSON
      ▶ 0: Object { id: "AEW2L9eTjEV_Ink", company_id: "ADNkkKVrAsec_com", title: "Roche Residence 1
      West 67th St.", ... }
        id: "AEW2L9eTjEV_Ink"
        company_id: "ADNkkKVrAsec_com"
        title: [REDACTED]
  
```

Рис. 89. Уникальный ID компаний-жертвы

Интересно то, что любому участнику партнерской программы доступны все ID компаний, которые есть в базе. Также указывается количество сообщений, которые были написаны жертвой и злоумышленником.

```

    ▼ JSON
      ▶ 0: Object { company_id: "DC3XA6ZZXZD_com", activity: 0 }
      ▶ 1: Object { company_id: "DDSErMemKGc_com", activity: 0 }
      ▶ 2: Object { company_id: "CZJj6wYnwSf_com", activity: 1 }
      ▶ 3: Object { company_id: "CwQ7im69U4m_com", activity: 57 }
        company_id: "CwQ7im69U4m_com"
        activity: 57
      ▶ 4: Object { company_id: "D1JPovnEyhg_com", activity: 0 }
      ▶ 5: Object { company_id: "AQ5yWM5go9k_com", activity: 7 }
      ▶ 6: Object { company_id: "A8YEJDURdJw_com", activity: 1 }
      ▶ 7: Object { company_id: "BCU88H21ksa_com", activity: 1 }
  
```

Рис. 90. Данные о компаниях: ID и количество сообщений, 2021

Тем самым можно составить статистику о количестве жертв, а также предположить, сколько компаний заплатили злоумышленникам за сокрытие информации.

Рис. 91. Диаграмма с распределением компаний-жертв Hive за сентябрь 2021



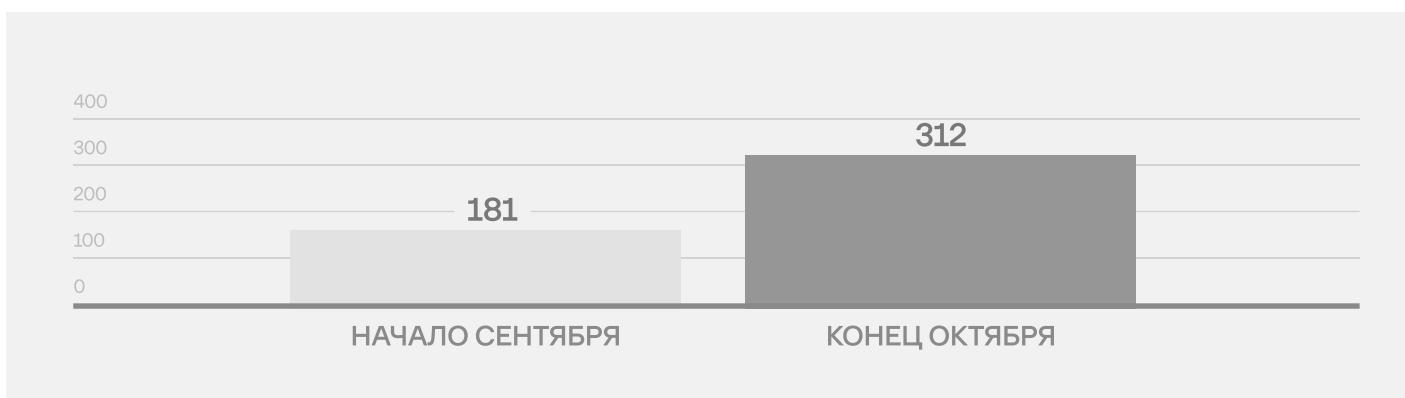
Специалисты Group-IB зафиксировали расхождения между данными с API злоумышленников и их DLS-сайта. API не возвращал одну компанию, которая уже была выложена на DLS, позже она пропала и из API, и из DLS. Можно предположить, что после публикации данных компания согласилась выплатить деньги злоумышленникам.

Если проанализировать компании, которые были опубликованы на DLS, то мы можем заметить, что большинство компаний не вели переписку со злоумышленниками.

Рис. 92. Распределение между компаниями, чьи данные были выложены на DLS, и теми, чьи данные не были опубликованы, сентябрь 2021



Исходя из анализа компаний, полученных через API, за месяц количество жертв увеличилось практически вдвое:



Более того, 43 компании из сентябрьского списка пропали из октябряского списка жертв. Предположительно, **около 24% компаний выплатили деньги злоумышленникам**.

В октябре статистика несколько изменилась:

Рис. 93. Диаграмма со статистикой жертв Hive за сентябрь-октябрь 2021

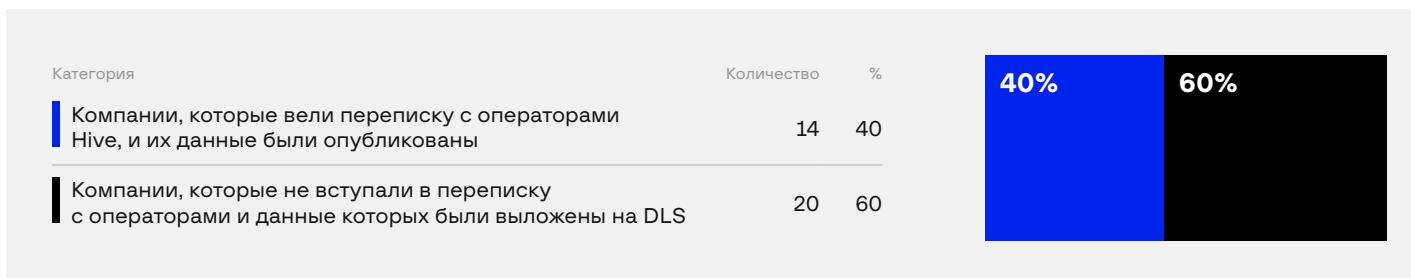
Рис. 94. Диаграмма с распределением компаний-жертв за октябрь 2021



Стоить иметь ввиду, что количество компаний, которое приводится в таблице, расходится с более ранними данными, потому что 14 компаний после публикации были удалены из DLS и API. Данные компании точно были взломаны и их данные точно были украдены. Можно предположить, что компании в итоге согласились на выкуп, из-за чего информация о них была полностью удалена.

Что касается переписки со злоумышленниками, можно заметить, что большинство жертв, информация которых была опубликована, не вели переписку с злоумышленниками.

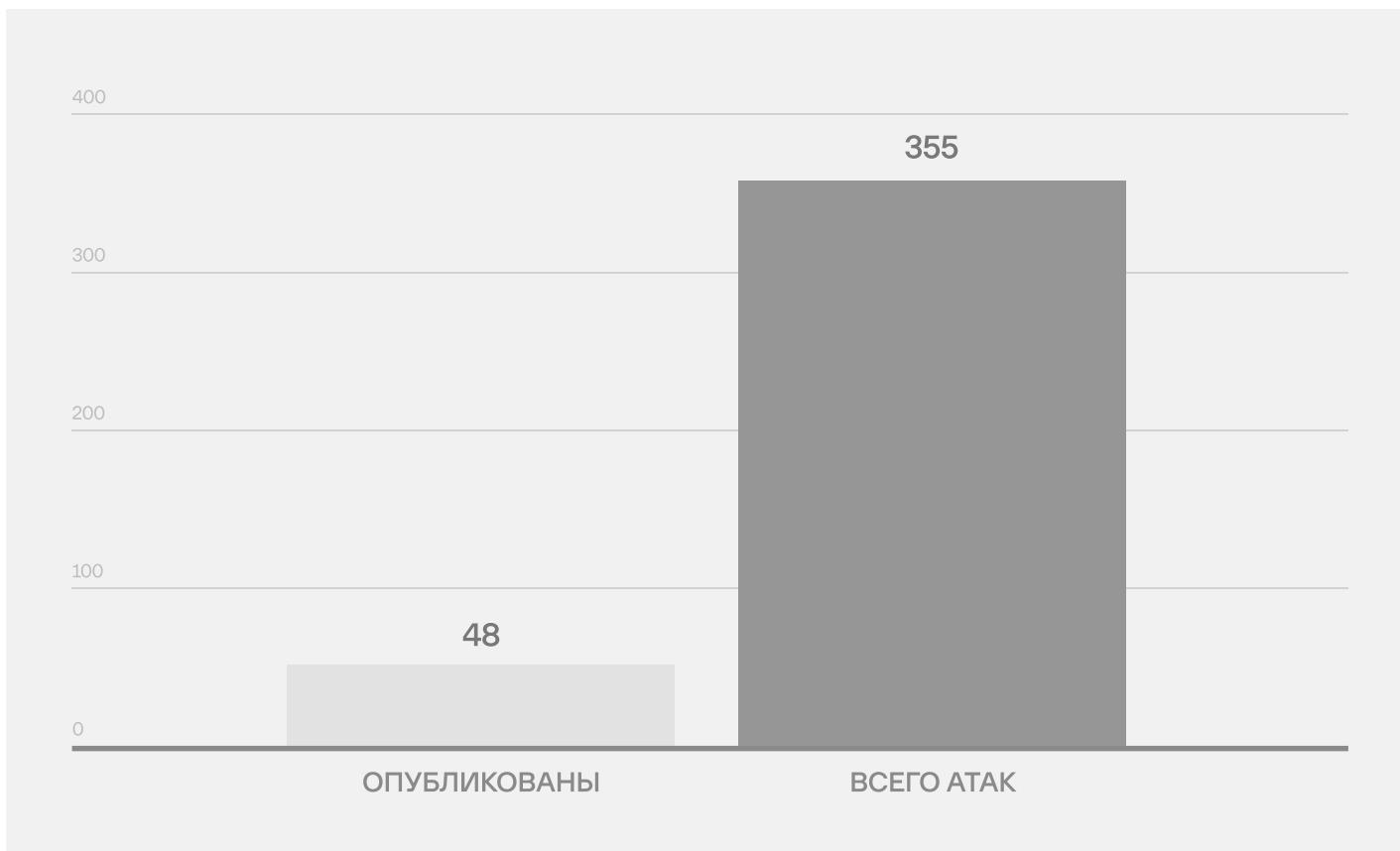
Рис. 95. Распределение между компаниями, чьи данные были выложены на DLS, и теми, чьи данные не были опубликованы, октябрь 2021



На данный момент в блог Hive попало лишь 48 компаний, включая и те, которые были позже удалены и из DLS, и из API. Но благодаря ошибке в работе API, Group-IB может определить количество атак начиная с сентября 2021 года по конец октября.

Если сложить количество уникальных id-компаний (312) за октябрь, а также id-компаний, которые пропали из API в период с сентября по октябрь (43), то можно определить, что суммарное количество атак составило 355.

Рис. 96. Диаграмма со статистикой жертв, 2021



Из этого можно сделать вывод, что лишь 13,5% компаний попадают в блог. Все остальные атаки либо неудачны, либо жертвы заплатили за молчание. Большую часть жертв данной группы вымогателей составляют компании из США.

Распределение компаний-жертв Hive по странам и индустриям, 2021



Suncrypt

DLS

Еще один интересный пример, который мы рассмотрим в данном отчете, это группа Suncrypt. Первая активность группы Suncrypt была обнаружена еще в октябре 2019 года. На тот момент записка о выкупе выглядела следующим образом и была переведена на английский, французский, немецкий и испанский языки.

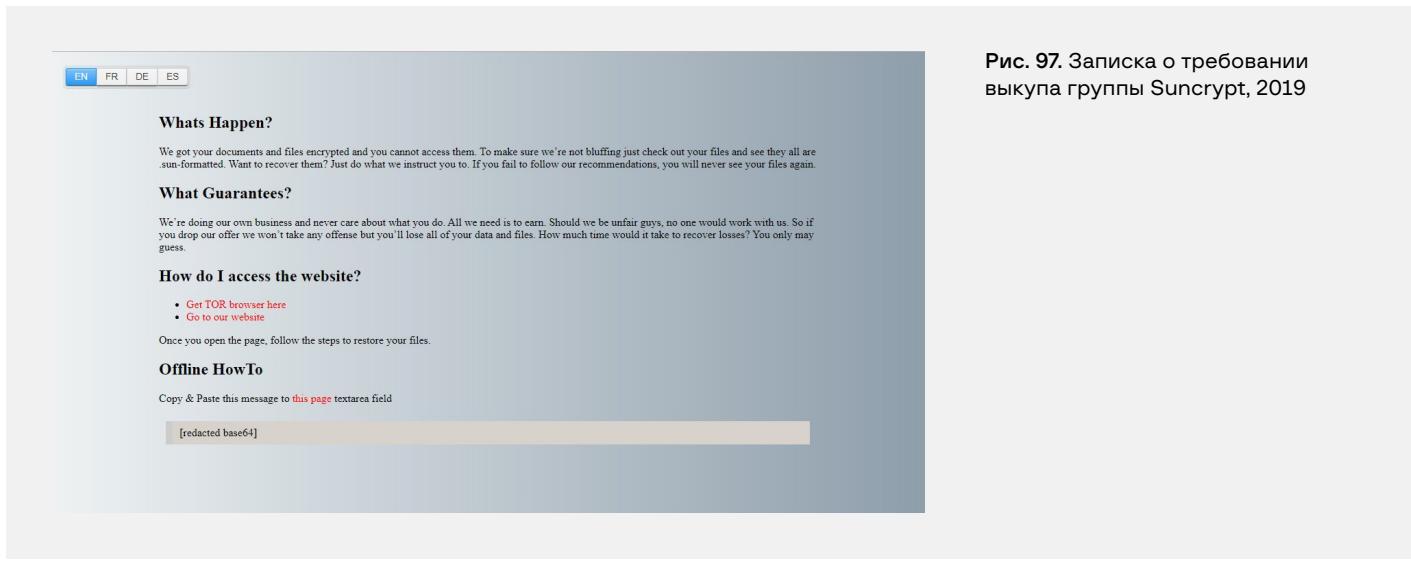


Рис. 97. Записка о требовании выкупа группы Suncrypt, 2019

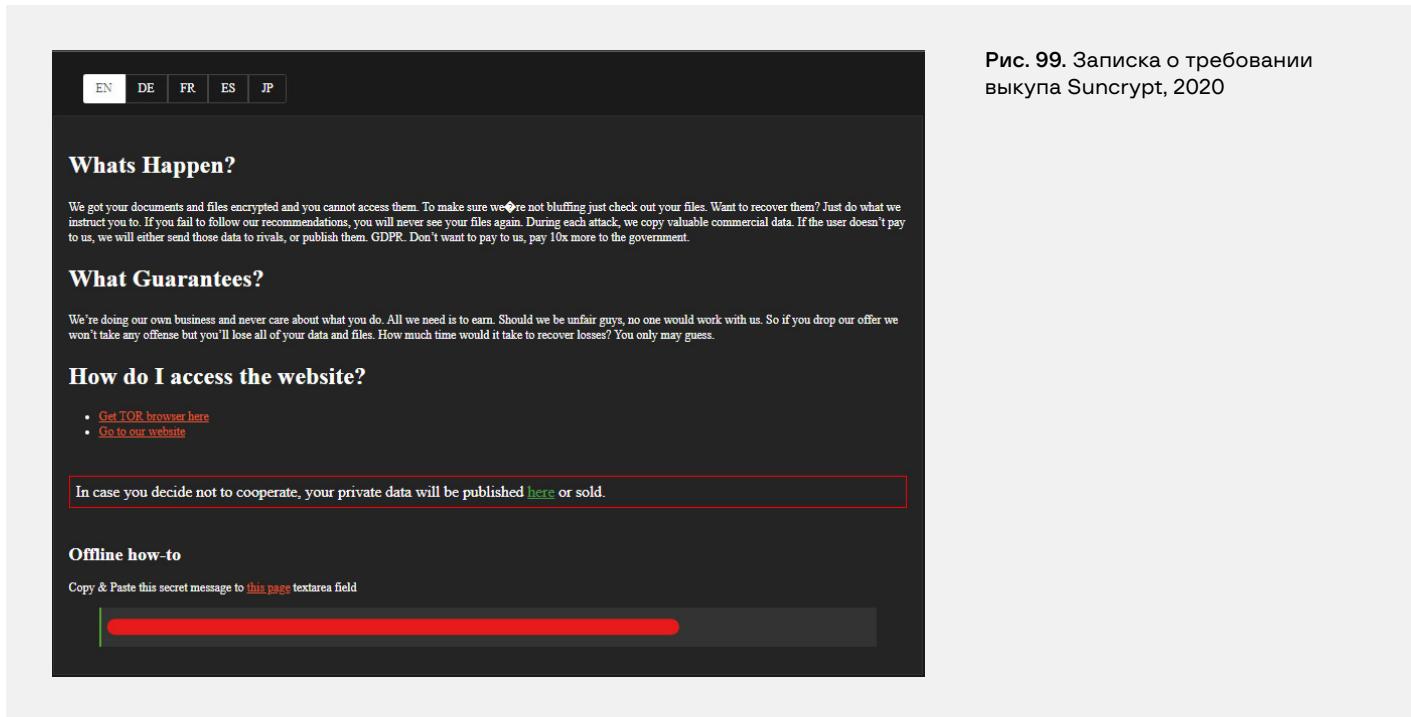
В записке было стандартное сообщение о том что файлы компании были зашифрованы, а также уникальный base64 код для жертвы и ссылка на ресурс злоумышленников [hxxp://sunlocksmdmv65mf.onion/](http://sunlocksmdmv65mf.onion/). Он представлял собой веб-форму, на которой необходимо было ввести полученный код для связи с преступной группой.

The screenshot shows a contact form page with the following content:

- EN FR DE ES** (Language buttons)
- Whats Happen?**
- We got your documents and files encrypted and you cannot access them. To make sure we're not bluffing just check out your files and see they all are sun-formatted. Want to recover them? Just do what we instruct you to. If you fail to follow our recommendations, you will never see your files again.
- What Guarantees?**
- We're doing our own business and never care about what you do. All we need is to earn. Should we be unfair guys, no one would work with us. So if you drop our offer we won't take any offense but you'll lose all of your data and files. How much time would it take to recover losses? You only may guess.
- Input Secret Message Here** (Text area)
- Send** (Button)
- Reset** (Button)

Рис. 98. Форма для обратной связи со злоумышленниками Suncrypt, 2019

Первые сэмплы данной программы-вымогателя, в которых был указан их текущий DLS-сайт, были обнаружены в записках о выкупе в конце августа 2020 года.



Записка выглядит почти точно так же, за исключением того, что в ней появляется японский язык и новые ссылки. Первая ведет на DLS группы [hxxp://nbzzb6sa6xiura2z.onion](http://nbzzb6sa6xiura2z.onion).

Вторая ссылка ведет на персональный чат [hxxp://ebwxexiymsib4rmw.onion/chat.html](http://ebwxexiymsib4rmw.onion/chat.html) с жертвой. Для каждой жертвы генерируется персональный идентификатор, который выглядит следующим образом⁵ и передается в качестве параметра:

1abc137b7d-2e7d3314f2-f8e60fc37a-b06f444368-f012d06402-d4bda6390a-daea3c5b58-b68cf150d5

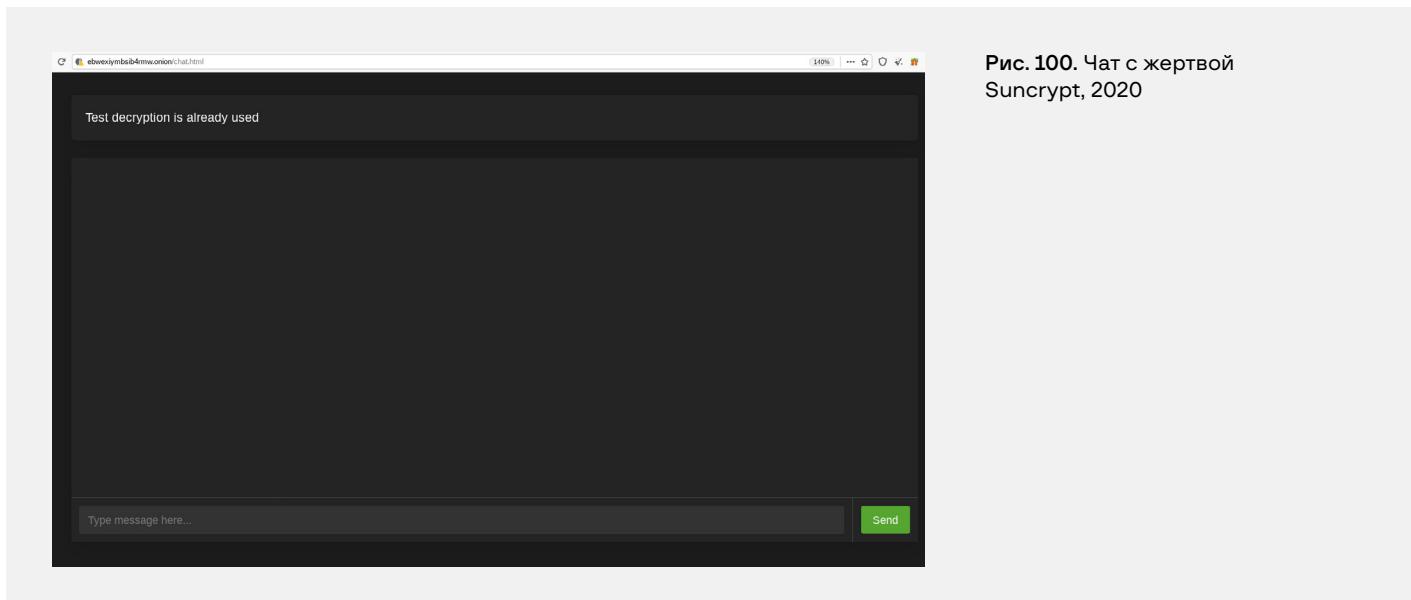


Рис. 99. Записка о требовании выкупа Suncrypt, 2020

⁵ Здесь некоторые числа были изменены для сохранения конфиденциальности

Когда DLS впервые появился в открытом доступе, он уже содержал скомпрометированные данные по пяти жертвам. Три из них находились в США, остальные две в Канаде и Норвегии.

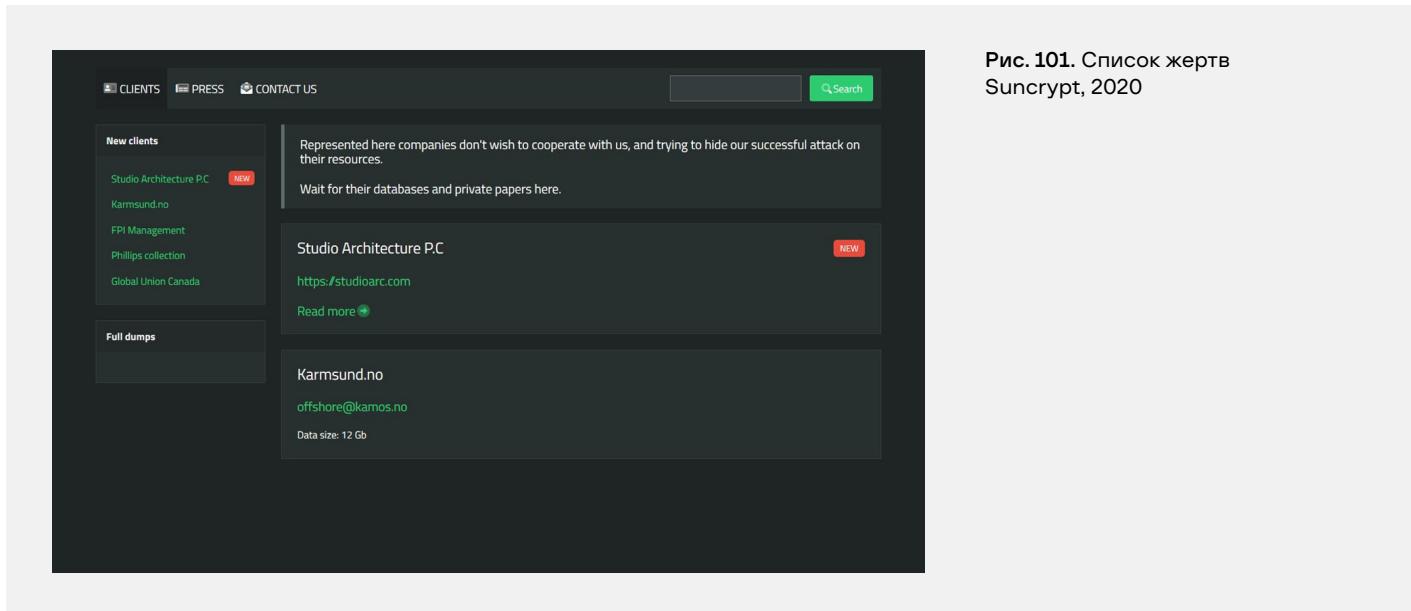


Рис. 101. Список жертв Suncrypt, 2020

Отрасль	Страна	Дата публикации	ID
Правительство и вооруженные силы	США	2020-08-01 0:00:00	5
Программное обеспечение	Канада	2020-08-08 0:00:00	3
Приватность и безопасность	США	2020-08-14 0:00:00	6
Производство	Норвегия	2020-08-14 0:00:00	7
Недвижимость: строительство	США	2020-08-21 0:00:00	8

В ходе дальнейшего исследования было выявлено, что у каждой скомпрометированной компании на DLS есть свой уникальный ID в базе злоумышленников в виде:

```
/client?id=ID
```

Особенностью данного DLS является то, что некоторые записи в ответ на запрос возвращают сообщение **Forbidden**. На момент появления DLS в сети, ID 1, 2, 4 были уже недоступны.

В августе 2021 года на ресурсе были доступны данные по **21 компании**, размещенных на разных ID. Последний ID 30 принадлежал компании-разработчику решений для автоматизации электронной коммерции. Девять разных ID отвечали **Forbidden**. В ходе исследования специалисты Group-IB выявили, что некоторые из текущих **Forbidden** ID соответствовали ранее атакованным компаниям, однако сейчас их данные были изъяты с DLS, предположительно в результате того, что компании заплатили выкуп.

Таким образом, можно предположить, что **30% компаний, которые были атакованы Suncrypt**, в результате заплатили выкуп, и их данные были удалены с ресурса злоумышленников.

Рис. 102. Соотношение компаний, размещенных на DLS и заплативших выкуп, 2020



Однако стоит отметить одну из особенностей в работе данной киберпреступной группы. На своем ресурсе они открыто заявляют, что готовы продать полные данные о компании любому заинтересованному лицу. Следовательно, данные также могли быть проданы другим лицам.

На самом ресурсе есть два основных подраздела – New clients и Full dumps. Как указывают злоумышленники, изначально они публикуют 10% данных скомпрометированной компании, только потом выставляют их на продажу. В случае, если данные не были выкуплены в течение недели, вымогатели публикуют полный дамп компании.

В первый год работы DLS (2020-й год), для размещения скомпрометированных данных группа использовала публичный файлообменник mega.nz. Начиная с 2021 года, они перешли на использование собственного сервера: <http://l4sd5qtsofedx7ss.onion/>.

Активность SunCrypt на андеграундных площадках

Пользователь с псевдонимом **SunCrypt** создал первый аккаунт на закрытом андеграундном форуме Maza в июле 2020 года с депозитом \$5000. Публичная партнерская программа появилась на том же форуме 3 августа 2020 года.

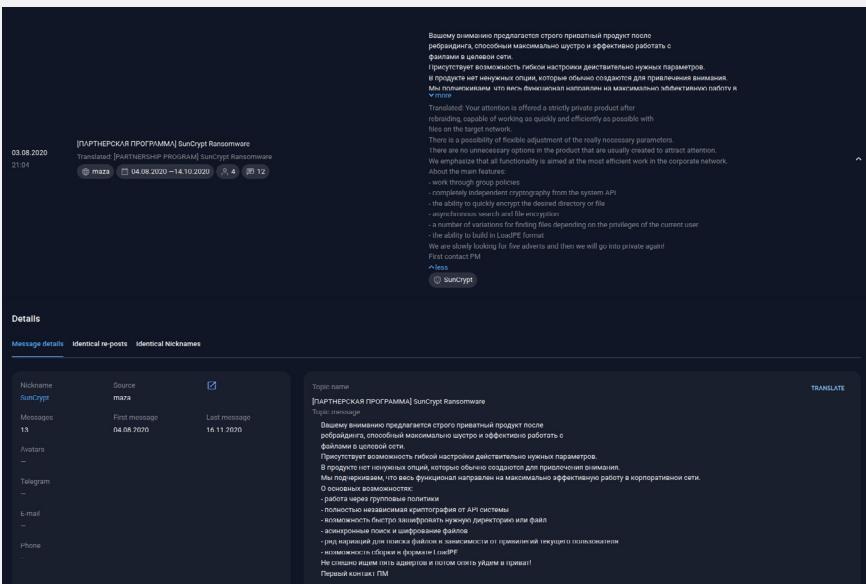


Рис. 103. Сообщение о партнерской программе SunCrypt, 2020

Скриншот сообщения на форуме Maza, датированного 03.08.2020, 21:44. Сообщение о партнерской программе SunCrypt Ransomware. Текст сообщения на русском языке:

Вашему вниманию предлагается строго приватный продукт после реорганизации, способный максимально быстро и эффективно работать с файлами в целях сети.

При этом имеется возможность гибких настроек действительно нужных параметров.

И продукт нет ненужных опций, которые обычно создаются для привлечения внимания.

Мы подтверждаем, что все функциональное направление на максимально эффективную работу и ребрэндинг, capable of working as quickly and efficiently as possible with files on the target network.

There is a possibility of flexible adjustment of the really necessary parameters.

Имеется множество различных опций в продукте, которые обычно созданы для привлечения внимания.

We emphasize that all functionality is aimed at the most efficient work in the corporate network.

About the main features:

- work through group policies
- full support of system cryptography from the system API
- the ability to quickly encrypt the desired directory or file
- asynchronous search and file encryption
- a number of variations for finding files depending on the privilege of the current user
- a number of variations for file decryption
- a number of variations for file recovery

We are slowly looking for five agents and then we will go into private again!

First contact PM

Details

Message details | Identical re-posts | Identical Nicknames

Nickname	Source	Last message
SunCrypt	maza	04.08.2020

Messages 13 First message 04.08.2020 Last message 16.11.2020

Topics 13 Topic name [ПАРТНЕРСКАЯ ПРОГРАММА] SunCrypt Ransomware Topic message

Давшему вниманию предлагается строго приватный продукт после реорганизации, способный максимально быстро и эффективно работать с файлами в целях сети.

Приступает возможность гибкой настройки действительно нужных параметров.

В продукте нет ненужных опций, которые обычно создаются для привлечения внимания.

Мы подтверждаем, что все функциональное направление на максимально эффективную работу в корпоративной сети.

работа через групповые политики

- полностью изолированная криптография от API системы

- возможность быстрого зашифрования папку/директорию или файла

- асинхронный поиск и шифрование файлов

- различные варианты поиска файлов и зависимость от привилегий текущего пользователя

- возможность сборки в формате .exe

Не спешите искать адверты и потом спешить удалить в браузере!

Первый контакт PM

По словам SunCrypt, они временно вышли из привата для поиска пяти новых партнеров. Кроме описания вредоносного ПО, в постах группа отмечает, что у них есть своя команда, которая отвечает за эксfiltrацию данных из сетей жертв, и от потенциальных партнеров им нужна только добыча сессий с доступом к Domain administrator. Они также сообщают, что если жертва отказывается платить выкуп, то они связываются с клиентами жертвы и журналистами, чтобы склонить компанию к выплате.

Стоит упомянуть, что один из модераторов форума Maza с псевдонимом **«Модератор 7»** (mod6@mfclub.ws) отметил, что они знают данную преступную группу и давно с ними сотрудничают.

12 августа 2020 SunCrypt разместили рекламу своей партнерской программы на другом закрытом форуме exploit.in.

На форуме exploit.in SunCrypt зарегистрировался еще в октябре 2019 году (<https://exploitivzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/profile/96576-suncrypt/>), что совпадает со временем начала активности первой вредоносной кампании Suncrypt. Можно предположить, что злоумышленник изначально искал себе партнеров приватно через личные сообщения на форуме exploit.in. Депозит на данном форуме составляет 0,5 BTC.

В качестве аватарки аккаунта SunCrypt использовал изображение художницы из Украины **DASHA PLISKA**. Это не самый популярный художник, что говорит либо об увлечении злоумышленника нишевым искусством, либо о его национальной принадлежности.



Рис. 104. Аватарка SunCrypt, 2020

16 августа 2020 SunCrypt написали, что у них осталось два свободных места из пяти. Уже к 20 августа у них оставалось одно свободное место, а 29 августа набор в партнерскую программу был завершен.

3 сентября SunCrypt отметили, что добавили возможность запуска своей полезной нагрузки в безфайловом режиме.

16 сентября злоумышленники упомянули, что у них снова появилось свободное место.

23 сентября они сделали публикацию о том, что добавили автокрипт exe и dll, и все еще продолжают искать партнеров.

1 октября они написали, что ищут последнего партнера. Но затем последовало странное сообщение, 8 октября они сделали пост о том, что решили закрыть партнерскую программу:

[ПАРТНЕРСКАЯ ПРОГРАММА] SunCrypt Ransomware
Translated: [PARTNERSHIP PROGRAM] SunCrypt Ransomware

08.10.2020 21:39
@ exploit.in 12.08.2020 – 09.10.2020 11 29

Details

Reliability: 51% Dredibility: 100% Admiralty code: D1 TLP: ● ●

Message details Identical re-posts Identical Nicknames

Nickname: SunCrypt Source: exploit.in Topic name: [PARTNERSHIP PROGRAM] SunCrypt Ransomware

Messages: 15 First message: 12.08.2020 Last message: 09.10.2020 Topic message: I'm sorry if it's late to respond.
Partnership program is being closed.
All ads will be removed from this account.
All advertisers for work will be paid.
All the best in business!
0.5 bits goes to the fund of the forum, pls.

Avatars

Telegram: @wazawaka @Deklighs Pictures

Email: — Phone: —

Рис. 105. Сообщение SunCrypt о закрытии партнерской программы, 2020

Конфликты с подельниками

18 октября 2020 года злоумышленник под псевдонимом **TrueFighter** опубликовал на форуме exploit.in денежную претензию к пользователям SunCrypt и avx. Он описал, что работал с данной командой, однако после закрытия партнерской программы ему не выплатили обещанные денежные средства.

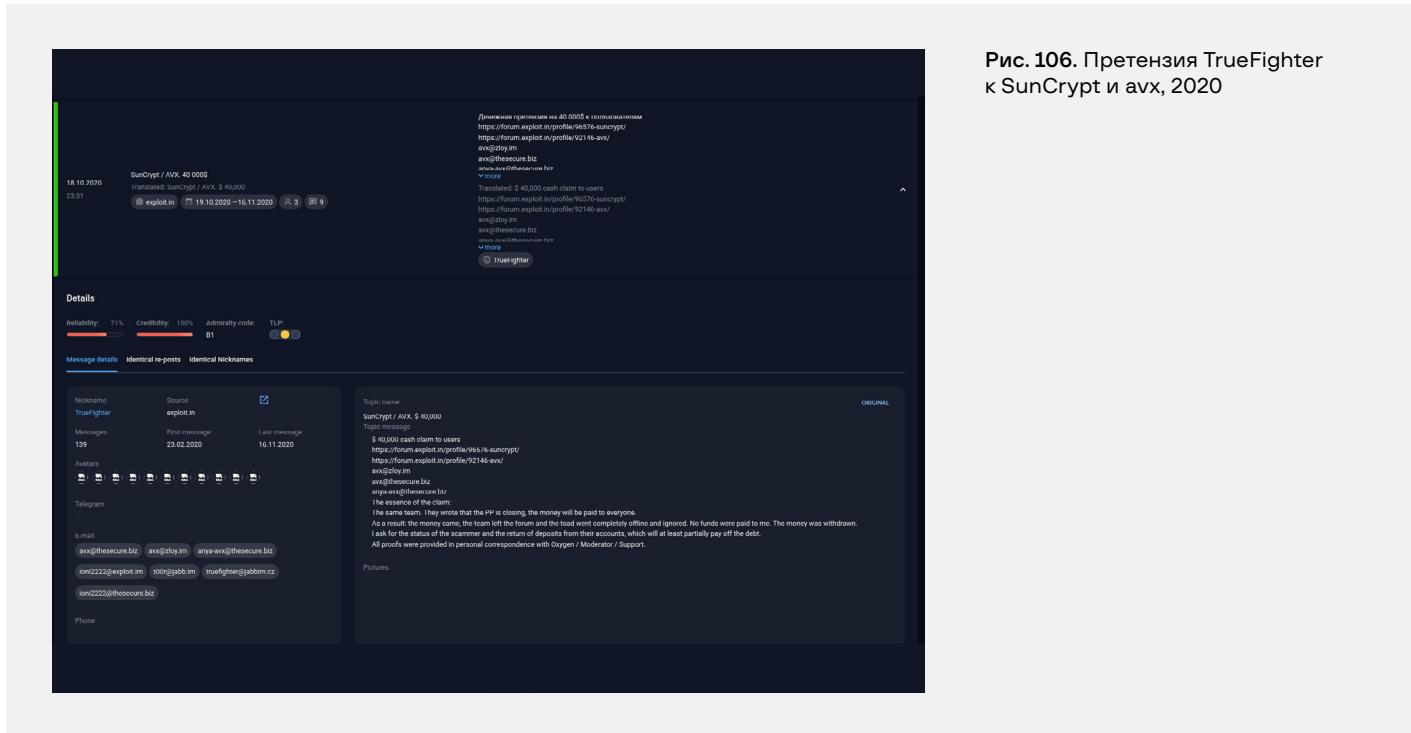


Рис. 106. Претензия TrueFighter к SunCrypt и avx, 2020

В ходе дальнейших разбирательств уже на другом форуме — Maza — SunCrypt дал пояснения, что они напрямую работали с avx и выплатили ему все, но не знают пользователя TrueFighter. Скорее всего, avx не выплатил деньги своему наемному работнику. SunCrypt также отметил, что avx родом из США.

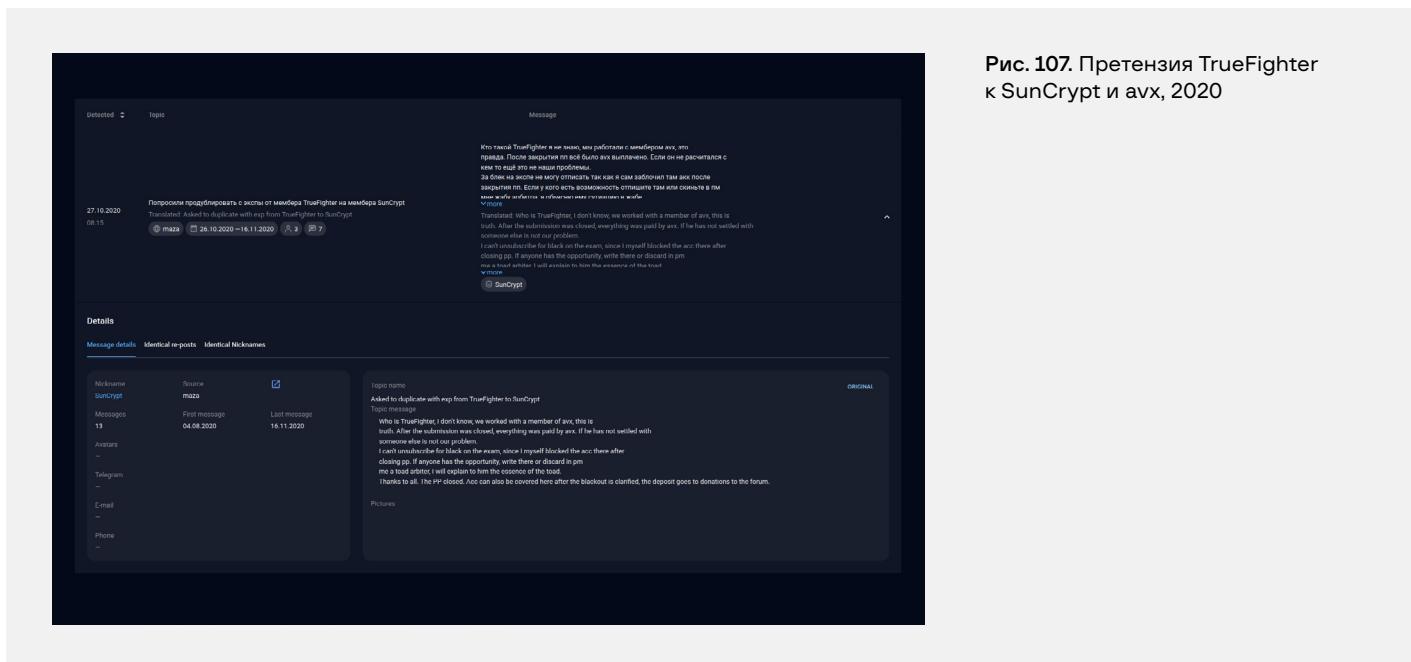


Рис. 107. Претензия TrueFighter к SunCrypt и avx, 2020

Предположительно, одним из партнеров SunCrypt являлся пользователь с псевдонимом D4rkL1ght (<https://forum.exploit.in/profile/104635-d4rkL1ght/>). В одном из своих постов он опубликовал гайд, полученный из панели управления ПП Suncrypt:

```

1 What the processing order is?
2
3 Stop services (In agressive mode only, check -agr argument below)
4 Remove shadow copies
5 Mount local volumes (connected to the computer but isn't mounted)
6 Encrypt shares
7 Encrypt local volumes
8 Report
9 Exit
10
11 Does it encrypt all the files?
12
13 In agressive mode (-agr argument):
14 Yes, except: exe, dll, sys, lnk, ico
15
16 In normal mode:
17 No, it does encrypt only certain extension.
18 You can check extension list HERE.
19
20 In addition it completely skips following folders:
21
22 Windows
23 Program Files
24 Program Files (x86)
25 $Recycle.bin
26 System Volume Information
27
28 When it create the note?
29
30 After all supported files are encrypted in the folder.
31 Folder proceesing order is:
32
33 Enter the folder
34 Encrypt files
35 Create note
36 Go to the next folder
37
38 Which arguments can be passed to the EXE?
39
40 -noreport
41 Don't report to the server after encryption is done
42
43 -noshares
44 Don't encrypt network shares and network disks, work only with local disks
45
46 -nomutex
47 Ignore mutex, start new instance even if another instance of cryptor is already running
48
49 -log
50 Create console window and write log
51
52 -path <folder/disk>
53 Work only with specified path
54
55 -skip
56 (BETA only)
57 Don't encrypt folder or file with specified name
58
59 -agr
60 (BETA only)
61 Stop non-standard services (except Citrix), encrypt all extensions except: exe, dll, sys,
62 lnk, ico
63 Is there a difference in the logic or processing order between PS1, EXE and DLL?
64
65 No, they are the same.
66 How to run PS1?
67
68 powershell -ep bypass -file cryptor.ps1
69 [ ! ] PS1 doesn't support arguments (e.g. -log, -path, etc.)
70 How to run DLL?
71
72 rundll32 cryptor.dll,DllRegisterServer
73 [ ! ] rundll32 does support arguments
74 regsvr32 cryptor.dll
75 [ ! ] regsvr32 doesn't support arguments
76
77 What is the difference between EXE and EXE-beta?
78
79 EXE has been tested a lot and considered to be stable
80 EXE-beta contains latest fixes, updates and so on, but less tested

```

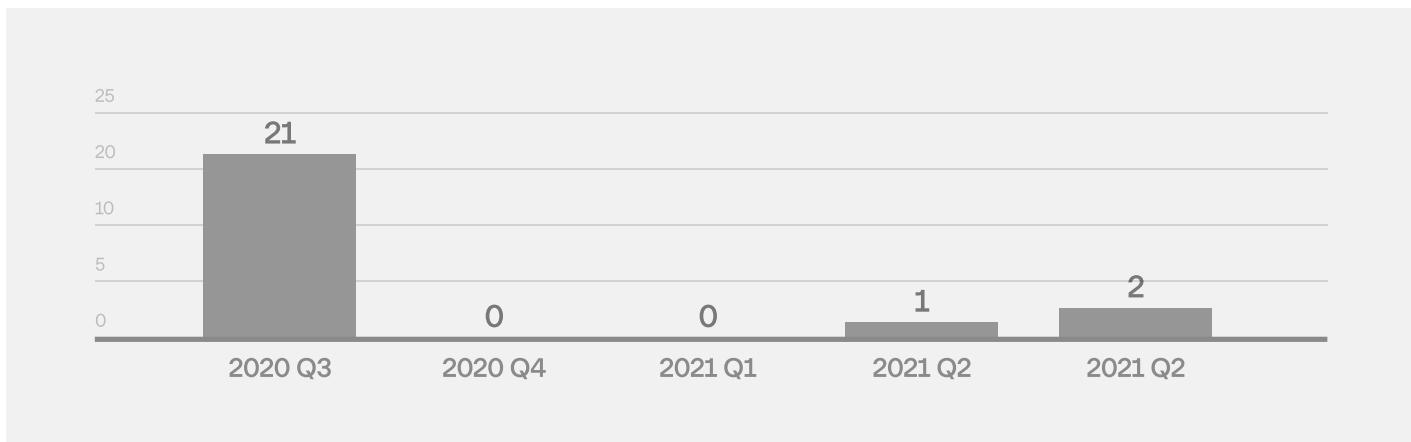
Рис. 108. Гайд, полученный из панели управления партнерской программы Suncrypt, 2020

У злоумышленника SunCrypt был конфликт на форуме с данным пользователем в связи с тем, что среди их жертв были больницы. SunCrypt отметил, что это была случайность, так как партнер не был проинформирован о запрете атак на такие цели.

Статистика по атакам

Как уже было отмечено выше, данная группа операторов программ-вымогателей опубликовала на своем блоге всего **30 компаний**. Из них на данный момент известны 24. Основная активность группы пришлась на третий квартал 2020 года, а в 2021 у этой партнерской программы было всего три известных жертвы.

Рис. 109. Статистика атак SunCrypt, 2020-2021



В основном данная группа специализировалась в своих атаках на производственную и энергетическую отрасли. Основные цели находились в США.

Распределение компаний-жертв SunCrypt по странам и индустриям, 2021



RTM: как зарождаются новые партнерские программы, или тихие локеры

За последние два года программы-вымогатели стали основной угрозой для бизнеса. Из-за успехов таких группировок, как **Revil** и **Lockbit**, все больше киберпреступников меняют свой род деятельности на программы-вымогатели, в силу их понятной монетизации и значительных финансовых возможностей. Некоторые стараются повторить успех Lockbit и организовывают свою Ransomware-as-a-Service. Особенно четко эта тенденция видна на примере человека под ником **RTM Team** (aka **BlackBet**). Процесс трансформации RTM в этом смысле показателен.

Впервые BlackBet появился на форуме 17 февраля 2017, где он рекламировал свой собственный маркет по продаже различных данных.

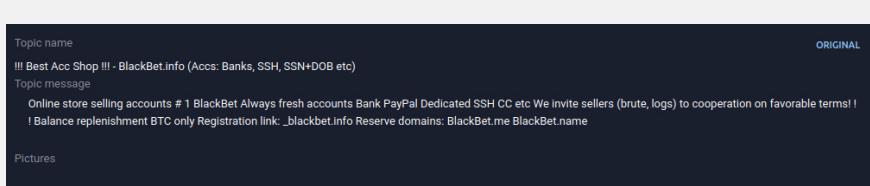
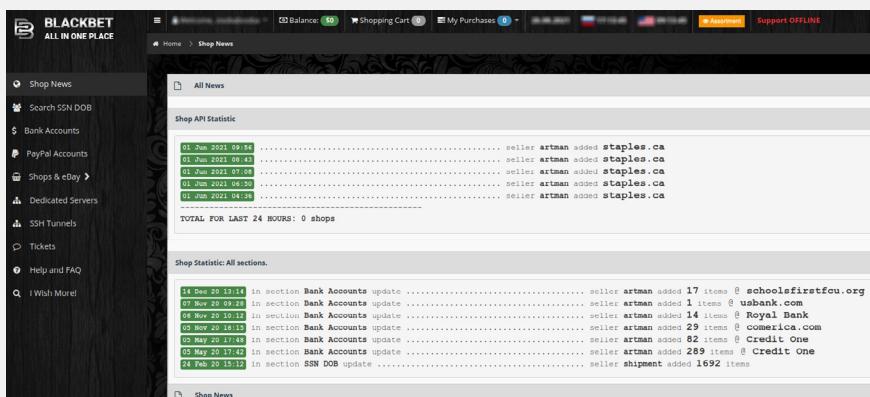
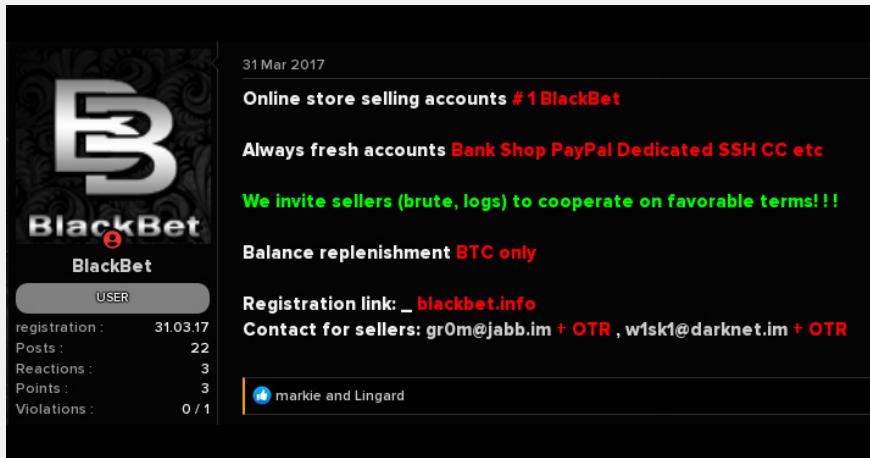


Рис. 110. Рекламы маркета BlackBet, 2017



Чуть позже он открыл свою партнерскую программу для своего маркета.

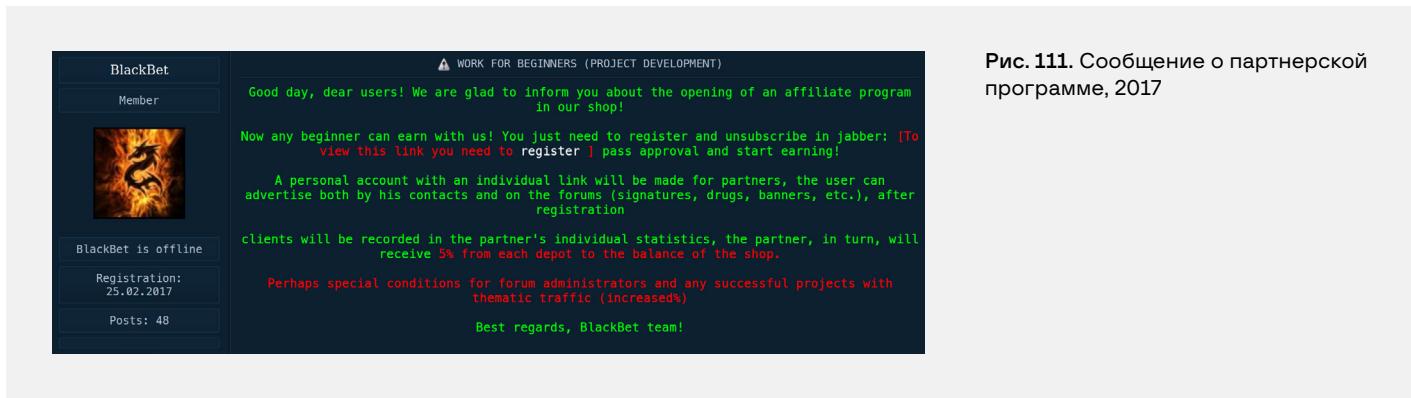


Рис. 111. Сообщение о партнерской программе, 2017

Помимо этого он скапывал логи по США, занимался майнингом, продавал и покупал вредоносные программы, продавал доступы к сетям и занимался другими вредоносными активностями. Главной его особенностью было то, что он всегда старался уследить за наиболее прибыльными трендами.

Когда злоумышленник понял, что программы-вымогатели как раз такой тренд, то решил попробовать его.

1 декабря 2021 он начал искать программиста для написания программы-вымогателя и пентестера для «работы в команде».

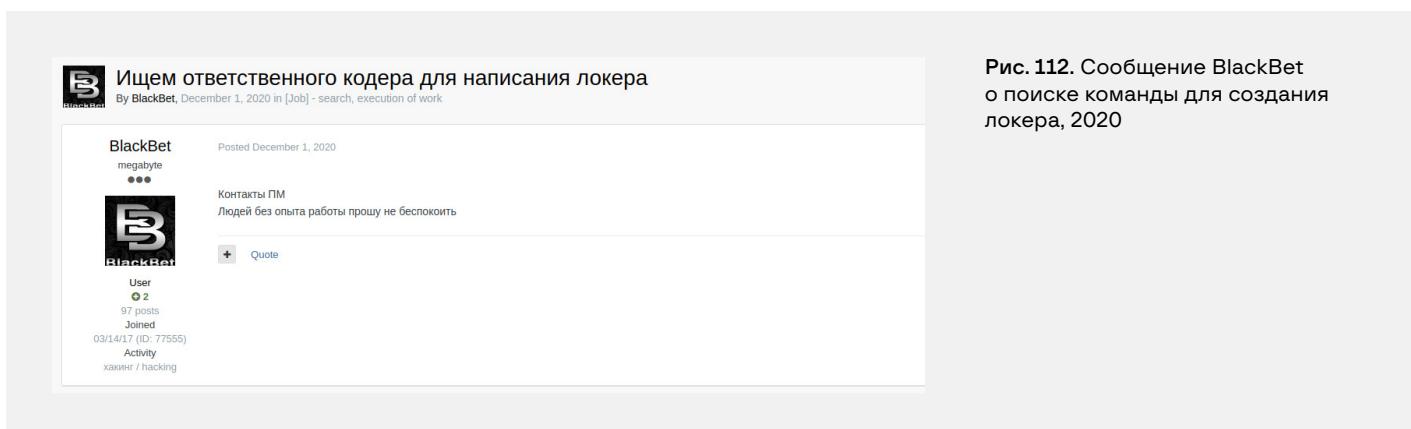


Рис. 112. Сообщение BlackBet о поиске команды для создания локера, 2020

Скрытая партнерская программа

19 августа 2021 администратор форума RAMP **Orange** интересовался партнерскими программами для вымогателей. Человек под ником **RTMTeam (aka BlackBet)** ответил, что скоро программа будет готова, а также звал других людей в свою партнерскую программу.

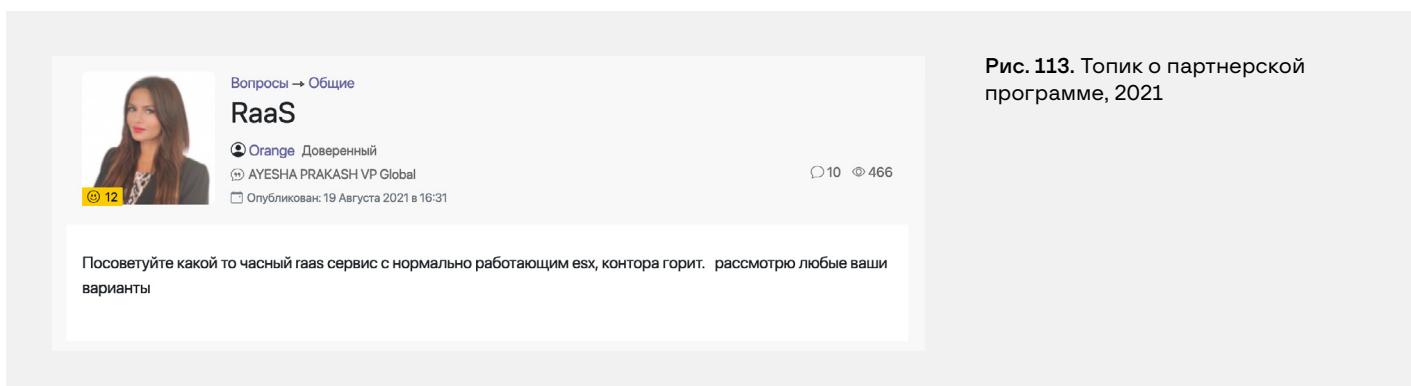
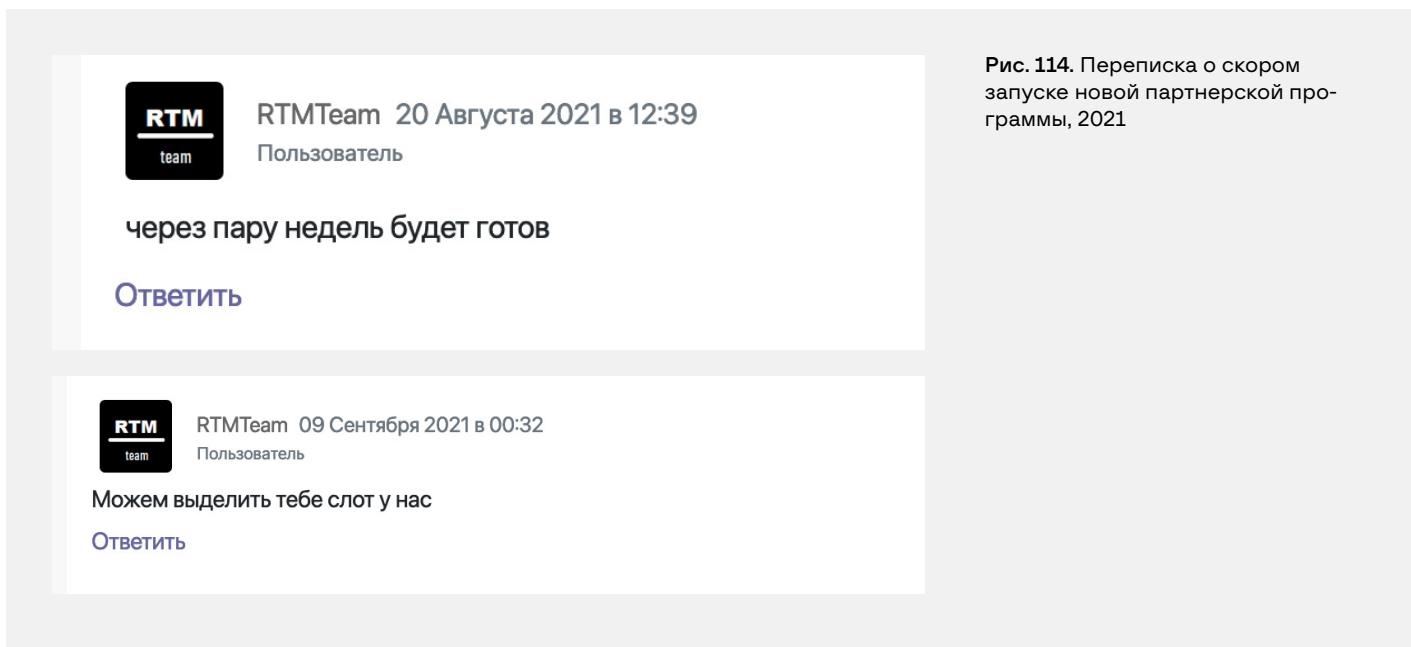
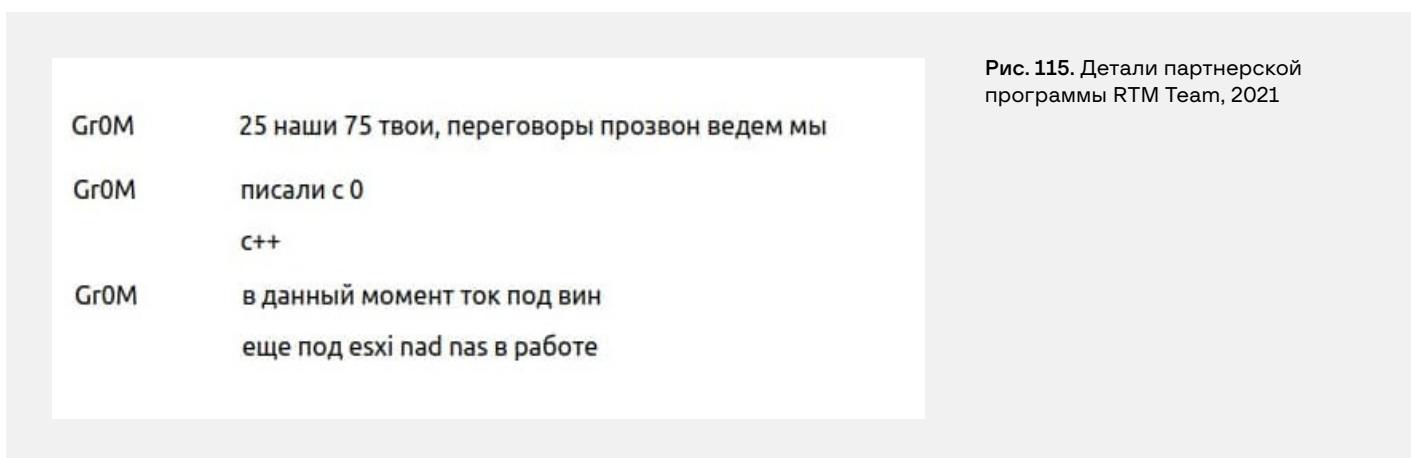


Рис. 113. Топик о партнерской программе, 2021



В ходе дальнейшего общения были выявлены основные детали партнерской программы, а также удалось получить сэмпл вредоносного ПО.



В ходе анализа сэмпла было выявлено, что представленные образцы являются вредоносным ПО, выполняющим выборочное шифрование файлов с использованием алгоритмов асимметричного шифрования Chacha20 и Curve25519, а также AES через расширения x86.

В процессе заражения ВПО перечисляет строки встроенных дисков и проверяет наличие действующего корневого диска и смонтированных дисков. Оно пропускает пути ОС и некоторые папки приложений и приступает к шифрованию всех пользовательских файлов, частично делая их бесполезными для восстановления без резервной копии или ключа дешифрования. Также ВПО проверяет наличие процессов и служб, строки которых встраиваются в последнюю секцию двоичного файла для соответствующего завершения процесса и службы.

Кроме того, им выполняется очистка корзины на всех обнаруженных дисках и очистка журналов событий системы, приложений и безопасности зараженной системы, после чего проверяется наличие теневых копий томов, где содержится код для доступа и запроса теневых копий с использованием WMI в качестве интерфейса.

Рис. 114. Переписка о скором запуске новой партнерской программы, 2021

После завершения процесса шифрования файлов обои сменяются на jpg-файл с требованием выкупа, а текстовый файл с запросом выкупа помещается в каждый каталог, где файлы были успешно зашифрованы. После заражения вредоносная программа удаляет себя из пути запуска.

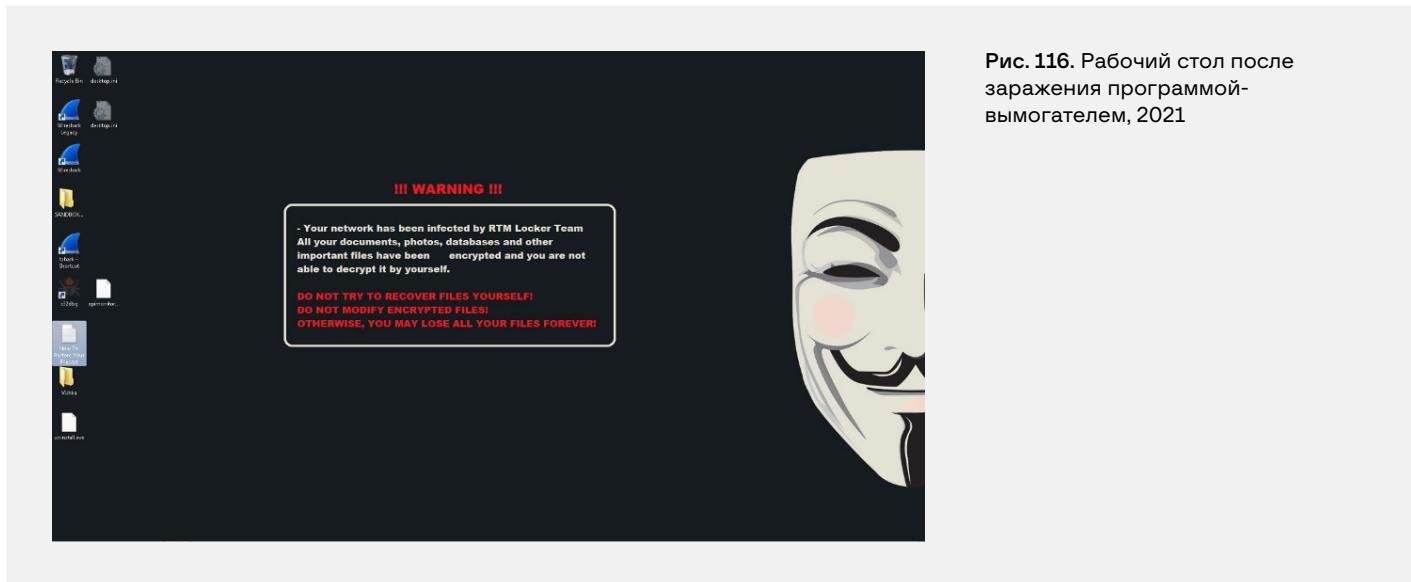


Рис. 116. Рабочий стол после заражения программой-вымогателем, 2021

Образцы, представленные в архиве, и образец, полученный через PS-дроппер, эквивалентны по функциональности и внешне отличаются друг от друга статическими атрибутами, включая ключи шифрования и ID-номера. Это указывает на то, что это могут быть сгенерированные образцы с разными ID для каждой зараженной системы.

История Groove и первой Fake DLS

История появления

Первое упоминание о **Groove** датируется 23 августа 2021, когда главному администратору форума RAMP — Orange — требовалась помочь в создании сайта для Groove.

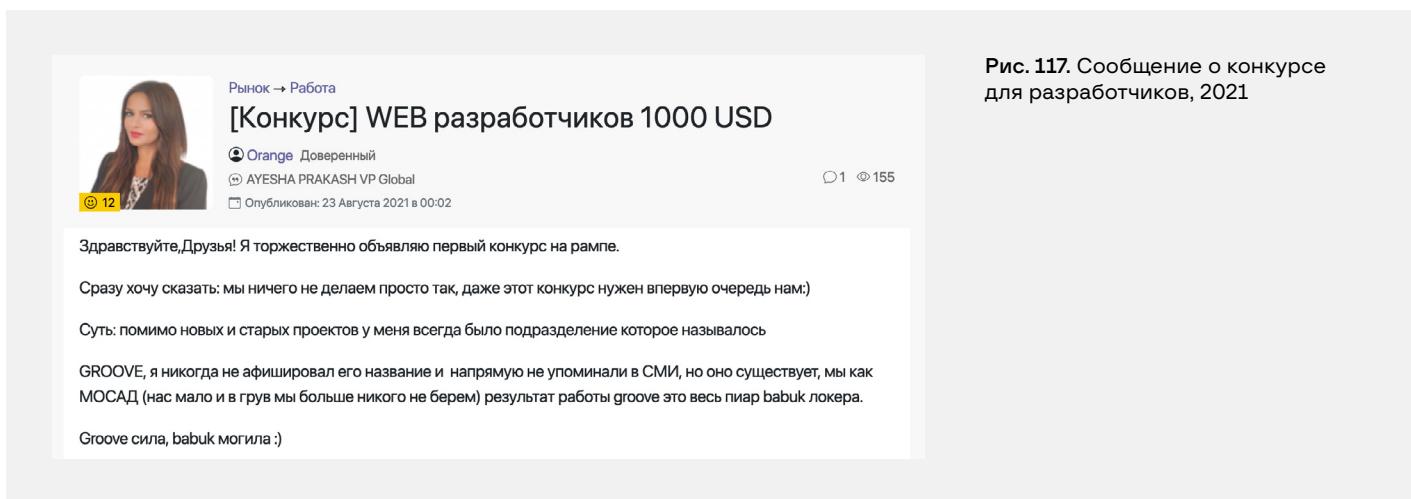


Рис. 117. Сообщение о конкурсе для разработчиков, 2021

Долгое время сайт Groove был пуст, затем там появились несколько утечек. Сайт выглядел как обычная DLS, до момента публикации 10 000 доступов к VPN сервису компании Fortinet.

10 000 доступов к Fortinet

31 августа 2021 года модератор форума RAMP разместил тему, в которой он отдавал архив, содержащий 10 тысяч записей о VPN-доступах Fortinet.



Инфо и ПО → Базы данных

запатченные валидные 10k fortinet

999 Модератор
in the middle of the nowhere
Опубликован: 31 Августа 2021 в 06:19 / Обновлен: 31 Августа 2021 в 06:20

БЕСПЛАТНО
в этом архиве небольшой кусок пробитых летом прошлого года фортинет ВПН, на сегодняшний день они уже запатчены но они валидные
пишите в этой теме кто хочет получить обосновав причину. в архиве будет 10к фортиков и чекер

Рис. 118. Сообщение об архиве с 10 000 доступов Fortinet, 2021

Модератор пишет, что отбор пользователей будет очень серьезным, и если доступы попадут в открытый доступ, он забанит всех, кому они были предоставлены.



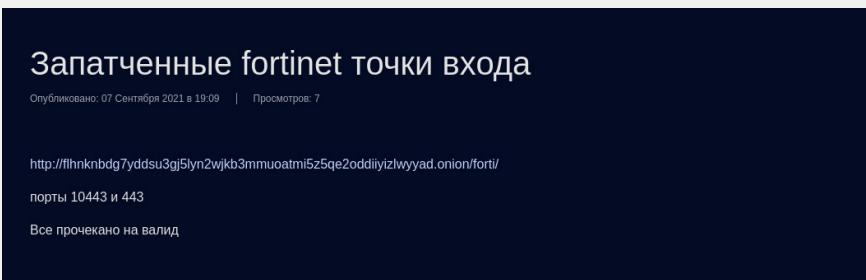
999 31 Августа 2021 в 06:22
Модератор

отбор будет суровый потому что их реально очень много и там наверняка что то еще есть очень хорошее, если архив уйдет в гору забаним всех кто получил его

Ответить

Рис. 119. «Отбор будет суровый», 2021

Однако 7 сентября 2021 года этот архив выложили на Groove, который возглавлял администратор RAMP'a. Он отметил, что все учетные данные были проверены на достоверность.



Запатченные fortinet точки входа

Опубликовано: 07 Сентября 2021 в 19:09 | Просмотров: 7

<http://flhnknbdg7yddsu3gj5lyn2wjk3mmuoatm5z5qe2oddiyyizlwyyad.onion/forti/>
порты 10443 и 443
Все прочекано на валид

Рис. 120. Выложенный архив доступов, 2021

Последствия и странные посты на DLS

После публикации 10 000 точек доступа к Fortinet, Groove привлек много внимания как со стороны пользователей RAMP, так и со стороны СМИ. Однако затем на ресурсе стали появляться странные записи с мыслями злоумышленника:

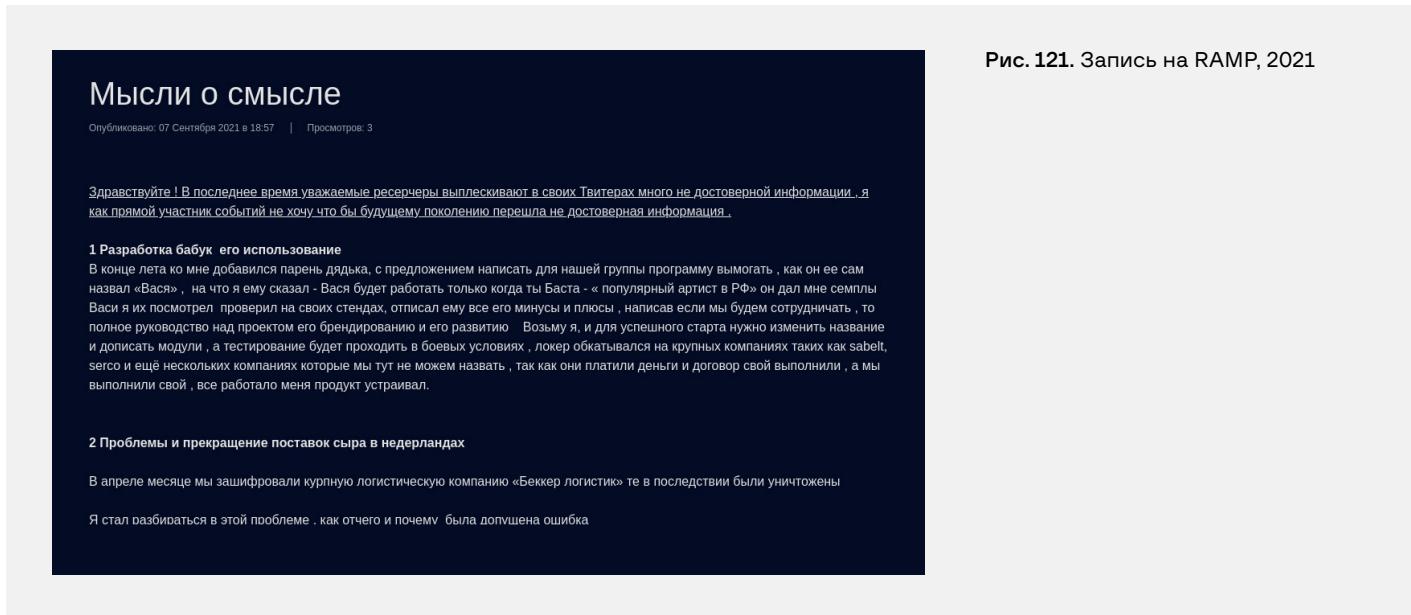


Рис. 121. Запись на RAMP, 2021

Однако в октябре 2021 владелец Groove (**boriselcin**) на форуме [xss.is](#) опубликовал пост, что вся это DLS была фейковая и была создана исключительно для манипуляции СМИ, так как программы-вымогатели сейчас приковывают много внимания.

Таким образом, из-за возросшей популярности вымогателей и партнерских программ можно предположить, что в будущем будут появляться Fake DLS и Fake-Ransomware-as-a-Service. Для входа в такие «партнерки» соучастнику придется заплатить, после чего администратор пропадает и не выходит на связь.

Что же касается данных на Fake DLS, то они могут быть взяты у менее популярных вымогателей, добыты при помощи OSINT или вообще сгенерированы. В случае с Groove, Fake DLS была сделана ради эксперимента и манипуляции СМИ, что не исключает вероятности того, что киберпреступники могут воспользоваться данной тактикой. Более того, подобная схема была уже успешно реализована ранее кардераами, мы подробно её описывали в нашем блоге [Кардеры-каннибалы](#).

РЕКОМЕНДАЦИИ ПО ПРОАКТИВНОМУ ПОИСКУ УГРОЗ

HI-TECH CRIME TRENDS 2021/2022

GROUP-IB.RU

1. Отслеживайте события, связанные с созданием подозрительных папок или файлов или запуском таких процессов как rundll32.exe или regsvr32.exe с помощью winword.exe/excel.exe
2. Выявляйте подозрительные запуски cscript.exe / wscript.exe, особенно те, которые связаны с сетевой активностью.
3. Выявляйте процессы powershell.exe с подозрительными или обfuscированными командными строками.
4. Анализируйте исполняемые файлы и скрипты, помещенные в папку автозагрузки, добавленные в ключи Run или запускаемые с помощью планировщика задач.
5. Отслеживайте выполнение sdbinst.exe на предмет подозрительных аргументов командной строки.
6. Проверяйте создание новых ключей в разделе HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.
7. Убедитесь, что ваши системы защиты умеют выявлять командные строки, характерные для средств дампинга учетных данных, таких как Mimikatz.
8. Ищите артефакты, характерные для инструментов сетевой разведки, такие как аргументы командной строки AdFind.
9. Выявляйте артефакты, связанные с выполнением файлов из необычных мест, таких как C:\ProgramData, %TEMP% or %AppData%.
10. Выявляйте модификации реестра и брандмауэра Windows, связанные с подключениями по RDP.¹
11. Отслеживайте и анализируйте соединения по RDP, чтобы выявлять попытки продвижения по сети.
12. Выявляйте запуски wmic.exe с использованием подозрительных командных строк.
13. Отслеживайте аномальное поведение bitsadmin.exe, особенно связанное с загрузкой потенциально вредоносных файлов.
14. Убедитесь, что ваши системы умеют выявлять полезные нагрузки Cobalt Strike Beacon и подобных им инструментов, характерных для постэксплуатационных фреймворков (как минимум те, которые запускаются с типичными аргументами командной строки и из типичных мест).

15. Отслеживайте сетевые соединения из распространенных системных процессов. Используйте известные списки серверов Cobalt Strike, которые вы можете получить у вашего поставщика Cyber Threat Intelligence.
16. Отслеживайте события создания новых служб, связанных с PsExec, SMBExec и другими средствами двойного назначения или инструментами пентестинга.
17. Отслеживайте исполняемые файлы, замаскированные под общие системные файлы (такие как svchost.exe), но имеющие аномальные родительские файлы или местоположение.
18. Отслеживайте признаки несанкционированного использования инструментов удаленного доступа в вашей сети.
19. Отслеживайте события установки клиентов облачных хранилищ и события доступа к облачному хранилищам, и проверяйте, являются ли они легитимными.
20. Отслеживайте распространенные FTP-программы на конечных хостах для выявления событий установки файлов с вредоносными конфигурациями.

- [1] Aids Info Disk или PC Cyborg Trojan — троян, заменяющий файл AUTOEXEC.BAT, который затем будет использоваться AIDS для подсчета количества загрузок компьютера. Как только число загрузок достигает 90, AIDS скрывает каталоги и шифрует имена всех файлов на диске C:, делая систему непригодной для использования, после чего пользователя просят «продлить лицензию» и связаться с PC Cyborg Corporation для оплаты (которая потребует отправки 189 долларов США на почтовый ящик в Панаме). Существует несколько версий AIDS, и, по крайней мере, одна версия не ждет, чтобы повредить диск C:, а скрывает каталоги и шифрует имена файлов при первой загрузке после установки AIDS. [стр. 13](#)
- [2] PGPCoder или GPCode — это троян, появившийся в 2004 году, который шифрует файлы на зараженном компьютере, а затем запрашивает выкуп для расшифровки файлов. Как сообщали пострадавшие, в начале каждого зашифрованного файла имеется строка PGPCoder 88.77.94. Зашифровываются файлы txt, zip, doc и xls. Указывается, что «Антивирус этот вирус не обнаруживает». [стр. 13](#)
- [3] Cryzip — семейство троянов, появившееся в 2006 году, которое шифрует данные и требует выкуп. Оказавшись на компьютере жертвы, ищет файлы 44 различных типов, шифрует их и затем оставляет послание пользователю с требованием заплатить 300 долларов за пароль для восстановления файлов. Cryzip помещает файлы в защищенный паролем ZIP-файл с помощью коммерческой библиотеки сжатия. Пароль ко всем зашифрованным файлам один и тот же: C:Program FilesMicrosoft Visual StudioVC98. Эта строка хранится в троянце в незашифрованном виде. Такая строка часто встречается в проектах, скомпилированных Visual C++ 6. Видимо, автор вредоносной программы рассчитывал на то, что тот, кто будет искать пароль в трояне, не станет обращать внимание на эту строку. [стр. 14](#)
- [4] Krotten — семейство троянов, появилось в 2005 году. Распространение происходит под видом фейкового генератора кодов для нелегального пополнения счета мобильных телефонов. Попытка пользователя пополнить свой лицевой счет с помощью Krotten оборачивается заражением компьютера, в результате которого невозможно использовать ресурсы операционной системы в полном объеме. Чтобы ее восстановить, ему предлагается пополнить баланс злоумышленника, который за вознаграждение (на скриншоте указана сумма в 25 украинских гривен) восстановит работоспособность системы. [стр. 15](#)

- [5] Winlock (Винлокер) — семейство вредоносных программ, блокирующих или затрудняющих работу с операционной системой, и требующих перечисления денег злоумышленникам за восстановление работоспособности компьютера, частный случай Ransomware. Первые версии вредоносной программы Winlock были обнаружены в 2007 году, однако свою популярность данный вид троянов получил только в 2009 году. [стр. 15](#)
- [6] Trojan.Encoder — троянская программа, шифрующая пользовательские файлы. Вредоносное ПО использовало XOR и TEA для шифрования файлов, написано на MASM. [стр. 19](#)
- [7] ULocker — это семейство троянов, появившееся в 2012 году. ULocker использовал поддельные сообщения некой полицейской ассоциации (International Police Association). Сообщение гласило, что компьютер жертвы был заблокирован, поскольку с него якобы просматривался неправомерный контент. Для разблокировки компьютеров запуганных пользователей предлагалось выплатить довольно значительные суммы: до €100. ULocker легко отличить от других локеров, поскольку они используют характерную картинку с большим изображением замка. [стр. 22](#)
- [8] Citadel — троян, созданный для кражи банковских данных. Был запущен в 2011 году, является модифицированной версией трояна Zeus. Citadel нанес ущерб в размере 500 млн долларов и заразил около 5 миллионов компьютеров. Помимо кражи данных, он может значительно замедлять работу компьютера и скачивать другое вредоносное программное обеспечение. [стр. 23](#)
- [9] CryptoLocker – это семейство программ-вымогателей, заражающее компьютеры под управлением операционной системы Microsoft Windows. Данная программа была впервые размещена в Интернете 5 сентября 2013 года. Троян распространялся через вложения электронной почты или при посещении пользователем зараженных сайтов. Вредоносная программа шифрует определенные типы файлов, хранящиеся на локальных и подключенных сетевых дисках, используя криптосистему с открытым ключом RSA, причём закрытый ключ хранится только на серверах управления вредоносной программой. Затем вредоносное ПО отображает сообщение, которое предлагает расшифровать данные. Если платеж (чаще всего в криптовалюте) не производится в указанный срок, вредоносное ПО предлагает расшифровать данные через онлайн-сервис, предоставляемый операторами вредоносного ПО, за значительно более высокую цену в биткоинах. [стр. 25](#)
- [10] TorrentLocker – троянская программа-вымогатель, нацеленная на Microsoft Windows. Вредоносная программа шифрует файлы жертвы аналогично CryptoLocker, используя симметричный блочный шифр AES, а ключ шифруется асимметричным шифром. [стр. 28](#)
- [11] VaultCrypt – программа-вымогатель, которая шифровала данные с помощью RSA-1024, после чего требовала посетить сайт в Tor, чтобы заплатить выкуп и вернуть файлы. Этот вымогатель сам не выводил сообщение с требованием выкупа. Вместо этого он регистрировал новое расширение .vault, в результате чего у всех зашифрованных файлов появлялась новая иконка с изображением замка. Если жертва пыталась открыть такой файл двойным нажатием кнопки мыши, на экране появлялось сообщение: "Stored in Vault" («Убрано в сейф»). [стр. 28](#)

- [12]** Chimera – программа-вымогатель, шифрует все файлы, которые находит на подключенных дисках, а затем требует 0,939 биткоинов, чтобы вернуть файлы. После шифровки файлов Chimera отображает записку с требованием выкупа, в которой даёт инструкцию, как произвести оплату и получить ссылку на дескриптор. Chimera не только шифрует файлы, но и публикует их в Интернете, если выкуп не выплачивается. [стр. 30](#)
- [13]** CryptoWall – семейство программ-вымогателей, впервые появившееся в начале 2014 года. Оно отличалось использованием невзламываемого шифрования AES, уникальным механизмом заражения СНМ и С2-активностью через анонимную сеть Tor. Злоумышленники, управляющие операцией CryptoWall, также предоставляли бесплатную одноразовую услугу дешифрования, чтобы доказать, что у них есть ключи, необходимые для восстановления захваченных файлов. Сумма выкупа составляла 700 USD, подлежала оплате в валюте биткойн, и в пересчете на криптоденьги была равна 1,8 BTC. [стр. 30](#)
- [14]** KeRanger – программа-вымогатель, нацеленная на компьютеры под управлением macOS. Обнаруженная 4 марта 2016 года компанией Palo Alto Networks, она затронула более 7 000 пользователей Mac. [стр. 32](#)

Group-IB

— один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

Миссия Group-IB: Fight Against Cybercrime

Interpol и Europol

Group-IB — партнер и участник совместных расследований

Топ-10 в APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Реагирование и исследование киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB



Москва



Амстердам



Дубай



Сингапур

- Европа
- Россия
- Ближний Восток
- Азиатско-Тихоокеанский регион

Решения Group-IB

Решения Group-IB признаны мировыми агентствами

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединяющую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества.



F R O S T
S U L L I V A N



Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры



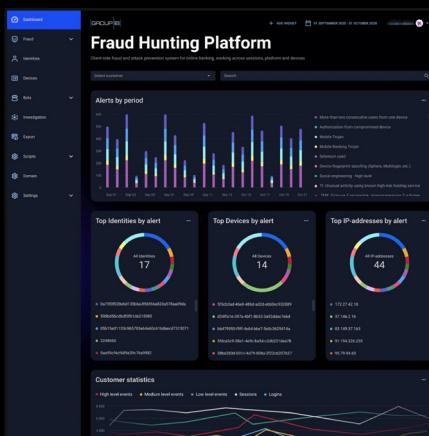
Threat Hunting Framework

Система защиты от сложных целевых атак и проактивной охоты за угрозами внутри и за пределами периметра



Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта



Fraud Hunting Platform

Цифровая защита и противодействие мошенничеству в реальном времени



Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз



AssetZero

Мониторинг внешнего períметра с помощью данных киберразведки

Экспертиза Group-IB

600+

экспертов междуна-
родного класса

70 000+

часов реагирования на инциденты
информационной безопасности

1 300+

успешных расследований
по всему миру

18 лет

практического опыта

Intelligence- driven services

В основе технологического лидерства компании, возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

Предотвращение

- Аудит безопасности
- Оценка безопасности
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Обучение

Реагирование

- Managed Incident response
- Managed detection and threat hunting

Расследование

- Компьютерная криминалистика
- Расследования
- Финансовые расследования
- eDiscovery



GROUP-IB

FIGHT AGAINST CYBERCRIME

**ПРЕДОТВРАЩАЕМ
И ИССЛЕДУЕМ
КИБЕРПРЕСТУПЛЕНИЯ
С 2003 ГОДА**