КИБЕРИМПЕРИЯ ШИФРОВАЛЬЩИКОВ

Часть 2

ROOT LEVEL RESOURCES

Анализ текущих трендов

В 2021 количество новых публичных партнерских программ[1] резко снизилось, однако это никак не сказалось на появлении новых DLS[2], а это значит, что многие программы-вымогатели продолжают работать без партнерских программ. Количество данных новых компаний-жертв на DLS-сайтах операторов программ-вымогателей растет.

Самыми активными группами в 2021 были Conti, Lockbit и Avvadon. Они опубликовали больше всего компаний на DLS, при этом общий процент от количества жертв упал, так как количество мелких групп операторов программ-вымогателей увеличилось (в 2020 лидирующие позиции данного списка занимали: Maze, Egregor и Conti).

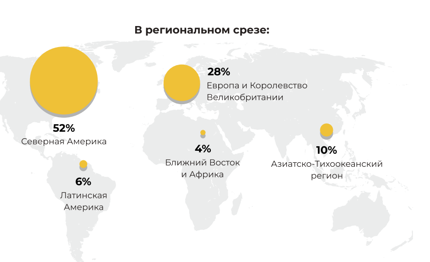
В 2022 В ТОП-3 активных групп вошли:

LockBit **Conti** **Pysa**

Что касается **географии распределения жертв**, то она выглядит следующим образом:

США	968	49,4%
Канада	110	5,6%
Франция	103	5,2%
Великобритания	92	4,7%
Италия	76	3,9%
Германия	72	3,6%
Испания	42	2,1%
Австралия	41	2,1%
Бразилия	39	2,0%
Индия	24	1,2%
Нидерланды	22	1,1%
Другие	295	6%

В региональном срезе:



Основными **атакуемыми отраслями** в 2022 стали **производство, недвижимость** и **транспорт**. Они же были в ТОП-3 в 2021, что указывает на то, что злоумышленники обычно ищут одни и те же типы компаний, которые им кажутся наиболее прибыльными.

Компании, которые им кажутся наиболее прибыльными

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

1 Публичной партнерской программой (RaaS) называют появление предложения присоединиться к группе, оперирующей программами-шифровальщиками, с целью заниматься распространением ВПО за процент от выкупа.

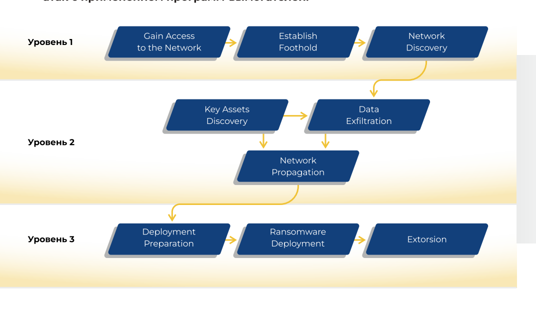
2 DLS используются операторами программ-вымогателей в качестве техники double extortion – то есть, с их помощью оказывается дополнительное давление на жертв для того, чтобы заставить их заплатить. После уплаты выкупа, операторы шифровальщиков обещают удалить скомпрометированные данные с DLS или не размещать их в публичном доступе.

Обзор тактик, техник и процедур в атаках

ROOT LEVEL RESOURCES

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.

Так, специалистами разработана **унифицированная структура атак с применением программ-вымогателей:**



Набор характерных для атак с использованием программ-вымогателей техник и инструментов остается стабильным, так как этот арсенал хорошо зарекомендовал себя и позволяет достигать своей цели, а также создавать обучающие материалы даже для неопытных игроков.

Развитие рынка брокеров первоначального доступа, что позволило многим атакующим без труда получить доступ к сетям своих жертв, в значительной мере повлияло на успех и количество атак с использованием программ-вымогателей.

Наиболее часто используемыми **техниками получения первоначального доступа** стали: компрометация служб удаленного доступа (21%), фишинг (26%), эксплуатация публично доступных приложений (47%).

Атаки на публично доступные терминальные серверы с доступными подключениями по протоколу удаленного рабочего стола (RDP) остаются популярным методом компрометации служб удаленного доступа. 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**.

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.

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**, 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**.

В некоторых случаях злоумышленникам удавалось получить доступ к так называемым **уязвимостям нулевого дня**. Показательным примером является атака партнеров **REvil** на компанию **Kaseya**.

Для получения первоначального доступа операторами программ-вымогателей продолжают активно использоваться 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.

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**, для заражения распространяемых по электронной почте документов.

Помимо традиционного фишинга операторы BazarLoader использовали и **вишинг**. Они рассылали 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.

Популярные техники атакующих:

100%	Command and scripting interpreter
100%	Remote Services
95%	Remote System Discovery
93%	Impair Defenses
91%	OS Credential Dumping
89%	Encrypted data for impact
89%	Inhibit system recovery
72%	Exfiltration over Web service
69%	Segned binary proxy execution
66%	System services

Традиционно атакующими широко применяются различные **интерпретаторы команд и сценариев**. Популярными являются следующие интерпретаторы: **командная строка Windows**; **PowerShell**; **Visual Basic**; **JavaScript**.

Первые два используются на различных стадиях жизненного цикла атаки. Visual Basic активно эксплуатируется вредоносными макросами, а JavaScript встречается реже, что повышает вероятность успешной компрометации.

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

Первый этап атаки, в большинстве случаев, это лишь доступ к корпоративной сети. Злоумышленники используют все средства, чтобы начать продвижение по сети и повысить привилегии. Это подтверждает тот факт, что в 100% случаев используются **службы удаленного доступа**.

Самым распространенных методов остается протокол удаленного рабочего стола (RDP). Некоторые группы даже имеют сценарии для включения возможности подобного доступа.

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

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**.

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

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.

Шифрование данных с целью получения выкупа осуществлялось атакующими лишь в 89% инцидентов.

Это связано с тем, что злоумышленники ограничились лишь выгрузкой данных, либо пользователи обнаруживали 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 епосредственно в программы-вымогатели, так и мог реализовываться посредством сценариев.

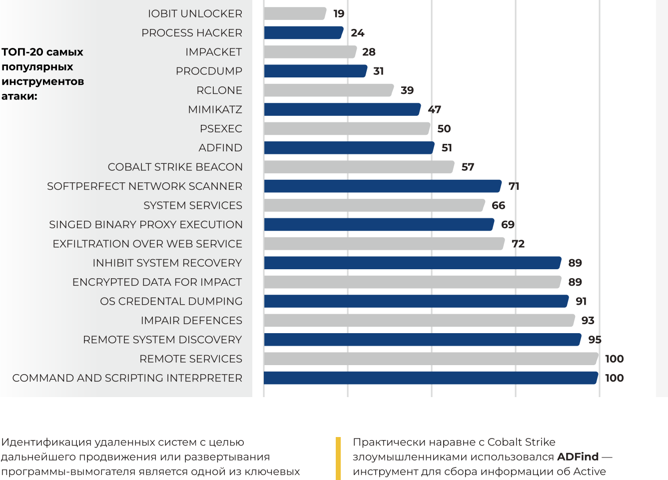
Многие группы все еще активно выгружают данные из скомпрометированных сетей.

Часто для этого ***используются веб-сервисы***. Особенно популярны различные облачные хранилищ, такие как **MEGA**, **DropMeFiles**, **SendSpace**.

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**.

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

ТОП-20 самых популярных инструментов атаки:



Идентификация удаленных систем с целью дальнейшего продвижения или развертывания программы-вымогателя является одной из ключевых задач злоумышленников. Инструментом для ее реализации стал популярный коммерческий сетевой сканер - **SoftPerfect Network Scanner**.

Cobalt Strike - еще один популярный инструмент. В некоторых случаях, вместо ботов в рамках фишинговых рассылок, атакующие использовали **Beacon**. Так, например, рассылались фишинговые письма с вредоносными документами для доставки загрузчика Squirrelwaffle, который в свою очередь загружал Cobalt Strike Beacon.

Практически наравне с Cobalt Strike злоумышленниками использовался **ADFind** — инструмент для сбора информации об Active Directory. Атакующие загружали его на ранних стадиях для изучения скомпрометированной инфраструктуры.

Кроме того, одной из задач злоумышленников является 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.

Не теряет своей актуальности инструмент для извлечения учетных данных и памяти - **Mimikatz**. Более того, злоумышленники используют и его варианты, такие как PowerShell-версию Invoke-Mimikatz и Python-версию Pypykatz.

Некоторые операторы программ-вымогателей решили облегчить жизнь своим партнерам обогатив арсенал инструментами для автоматического сбора и выгрузки данных. Хорошим примером является StealBit от LockBit. Тем не менее, многие все еще выгружают данные своими средствами. Наиболее популярным инструментом для решения этой задачи стал **Rclone**.

Так как популярные инструменты для извлечения учетных данных из памяти легко обнаружить, ряд злоумышленников использует легитимные инструменты для дампинга lsass.exe (использование **ProcDump**).

Помимо PsExec, для выполнения команд на удаленных хостах, активно использовался сценарий SMBExec из пакета **Impacket**.

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

Инструмент, который использовался злоумышленниками для решения схожих задач – **Iobit Unlocker**, в том числе применялся для завершения процессов, взаимодействующих с базами данных и препятствующих их шифрованию.

Однако, стоит отметить, что представленные техники и инструменты не являются исчерпывающими.

Закулисье мира кибервымогателей

ROOT LEVEL RESOURCES

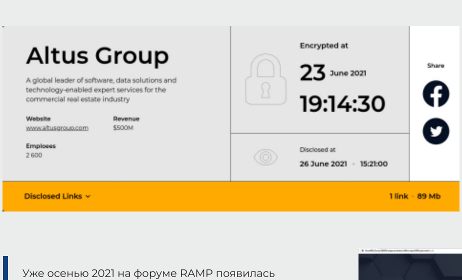
1 HIVE

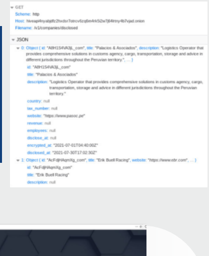
Летом 2021 была обнаружена активность группы **Hive** с помощью DLS.

Они используют комбинацию AES и RSA для шифрования данных, после чего, программа загружает их на удаленный сервер. Зашифрованные файлы можно узнать по расширению .hive.

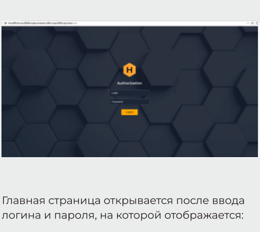
Отличительная черта DLS в том, что он работал при помощи API. Кроме Hive есть только 2 группы, которые также использовали API - **Grief** и **DoppelPaymer**.

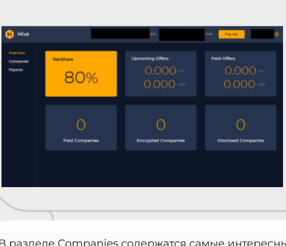
Украденные файлы Hive выкладывала на файлообменники (sendspace, anonfiles, send.exploit и другие).





Уже осенью 2021 на форуме RAMP появилась реклама партнерской программы. В ходе общения с злоумышленником был получен доступ к закрытой партнерской программе (был предоставлен адрес административной панели и аутентификационные данные для входа), что позволило установить, что это Hive.





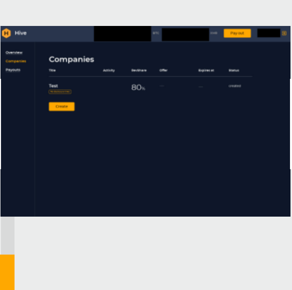
Главная страница открывается после ввода логина и пароля, на которой отображается:

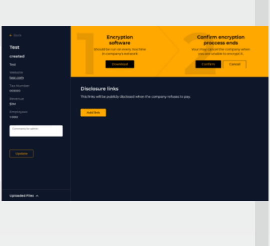
- Какой процент от выкупа получает злоумышленник
- Сколько должен получить в будущем, сколько уже получил, количество заплативших
- Зашифрованных и раскрытых компаний
- Также общий баланс и логин

В разделе Companies содержатся самые интересные данные. Здесь указываются название компании жертвы, её сайт, краткое описание, а также её выручку и количество сотрудников.

Вкладка Payouts отвечает за вывод средств с партнерской программы на личный кошелек злоумышленника.

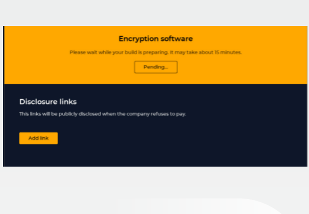
После заполнения этой информации открывается следующее окно:



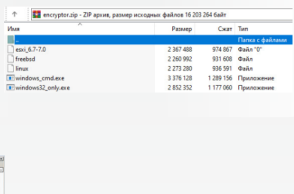


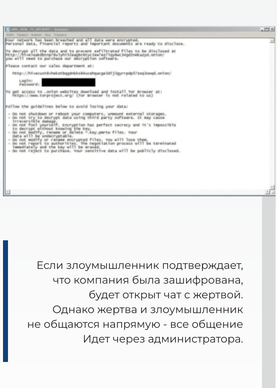
Открыв карточку компании появится возможность скачать программу-вымогатель для компании-жертвы и отметить, удалось ли зашифровать ее данные.

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



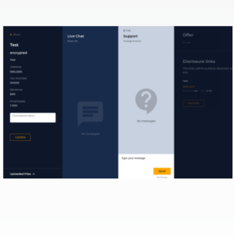
После создания программы-вымогателя будет сгенерирован архив .rar со следующими файлами:

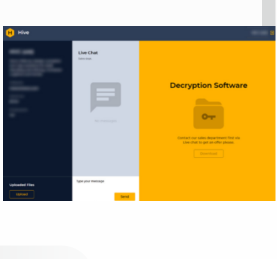




После заражения будет автоматически создана записка с запросом выкупа, в которой будет ссылка на сайт, а также логин и пароль для доступа:

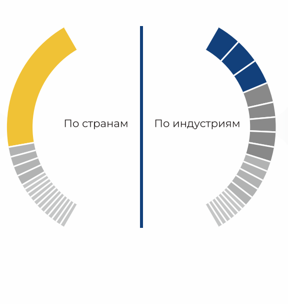
Если злоумышленник подтверждает, что компания была зашифрована, будет открыт чат с жертвой. Однако жертва и злоумышленник не общаются напрямую - все общение идет через администратора.





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

Распределение компаний-жертв Hive

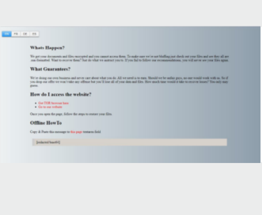


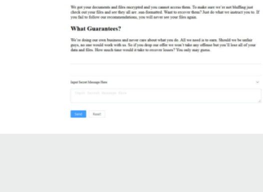
США	28
Великобритания	2
Австралия	2
Нидерланды	2
Китай	2
Канада	1
Перу	1
Швейцария	1
Португалия	1
Таиланд	1
Индия	1
Норвегия	1
Испания	1
Германия	1
Тайвань	1
Франция	1
Италия	1

5	Недвижимость
5	ИТ
5	Производство
4	Другое
3	Коммерция и шоппинг
3	Транспорт
3	Медиа и развлечения
3	Финансовые услуги
2	Профессиональные услуги
2	Административные услуги
2	Продукты питания и напитки
2	Оборудование
2	Здравоохранение
1	Кредитование и инвестиции
1	Предметы одежды и аксессуары
1	Образование
1	Приватность и безопасность
1	Товары потребления
1	Игры
1	Программное обеспечение

2 Suncrypt

Suncrypt была обнаружена осенью 2019. Тогда записка о выкупе была переведена на английский, французский, немецкий и испанский языки и выглядела следующим образом:

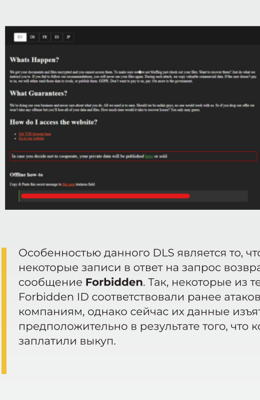




Она содержала сообщение, что файлы компании зашифрованы, а также уникальный код для жертвы и ссылка на ресурс злоумышленников, на котором необходимо было ввести полученный код для связи.

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

Записка выглядит почти точно так же, за исключением того, что в ней появляется японский язык и новые ссылки. Первая ведет на DLS группы, а вторая - на персональный чат.



Когда DLS впервые появился в открытом доступе, он уже содержал скомпрометированные данные по пяти жертвам. Три из них находились в США (индустрии: правительство и вооруженные силы, приватность и безопасность, недвижимость: строительство), остальные две в Канаде (программное обеспечение) и Норвегии (производство). При этом у каждой скомпрометированной компании на DLS, в базе злоумышленников, есть свой уникальный ID.

Особенностью данного DLS является то, что некоторые записи в ответ на запрос возвращают сообщение **Forbidden**. Так, некоторые из текущих Forbidden ID соответствовали ранее атакованным компаниям, однако сейчас их данные изъяты с DLS, предположительно в результате того, что компании заплатили выкуп.

Suncrypt открыто заявляют, что готовы продать полные данные о компании любому заинтересованному лицу.

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

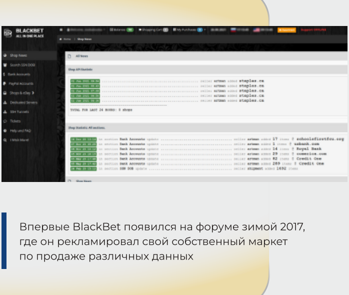
Распределение компаний-жертв SunCrypt

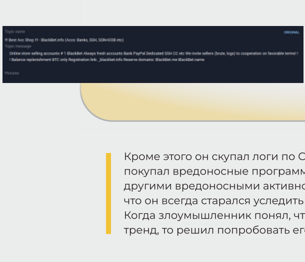
США	12
Норвегия	3
Канада	2
Бельгия	2
Германия	2
Италия	1
Великобритания	1
Австралия	1

5	Производство
4	Энергетика
3	Торговля и шопинг
2	Недвижимость
2	Профессиональные услуги
1	Правительство и вооруженные силы
1	Образование
1	ИТ
1	Транспорт
1	Безопасность
1	Здравоохранение
1	Финансовые услуги
1	Наука и инженерное дело

3 RTM: как зарождаются новые партнерские программы, или тихие локеры

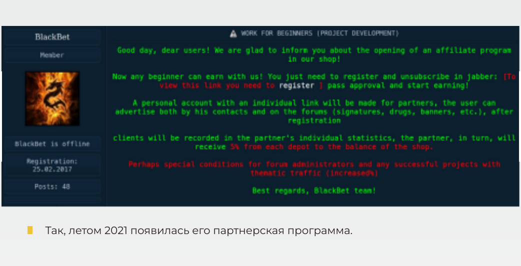
За последние два года программы-вымогатели стали основной угрозой для бизнеса. Все больше киберпреступников меняют свой род деятельности на программы-вымогатели, в силу их понятной монетизации и значительных финансовых возможностей. Некоторые стараются повторить успех Lockbit и организовывают свою Ransomware-as-aService. 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 зимой 2017, где он рекламировал свой собственный маркет по продаже различных данных

Кроме этого он скупал 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 успедить за наиболее прибыльными трендами. Когда злоумышленник понял, что программы-вымогатели как раз такой тренд, то решил попробовать его.



Так, летом 2021 появилась его партнерская программа.

В ходе анализа сэмпла RTMTeam (aka BlackBet) установлено, что ВПО выполняет 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, 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, выполняется очистка корзины, журналов событий системы, приложений и безопасности зараженной системы, после чего проверяется наличие теневых копий, где содержится код для доступа и запроса теневых копий с использованием WMI в качестве интерфейса.

После завершения шифрования файлов - обои сменяются на jpeg-файл с требованием выкупа, а текстовый файл с запросом выкупа помещается в каждый каталог, где файлы были зашифрованы.

После заражения вредоносная программа удаляет себя из пути запуска.

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.

4 Groove и первая Fake DLS

Первое упоминание о них появилась летом 2021, когда главному администратору форума RAMP требовалась помощь в создании сайта для Groove. Долгое время сайт Groove был пуст, затем там появились несколько утечек. Сайт выглядел как обычная DLS.

Groove привлек много внимания как со стороны пользователей RAMP, так и со стороны СМИ после публикации 10 000 точек доступа к Fortinet.

Однако осенью 2021 владелец Groove (boriselcin) на форуме xss.is опубликовал пост, что вся это DLS фейковая и была создана исключительно для манипуляции СМИ, так как программы-вымогатели сейчас приковывают внимание.

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. Что же касается данных на Fake DLS, то они могут быть добыты при помощи OSINT, взяты у менее популярных вымогателей или вообще сгенерированы. В случае с Groove, Fake DLS была сделана ради эксперимента и манипуляции, что не исключает вероятности того, что киберпреступники могут воспользоваться данной тактикой.

ROOT LEVEL RESOURCES

Рекомендации по проактивному поиску угроз

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 обфусцированными 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\WindowsNT\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.
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 облачным хранилищам, и проверяйте, являются ли они легитимными.
20. Отслеживайте распространенные FTP-программы на конечных хостах для выявления событий установки файлов с вредоносными конфигурациями.