Root Level Resources предлагает вашему вниманию материал, в котором рассмотрены ключевые причины и этапы развития индустрии программ-вымогателей, подробно разобрано деятельность некоторых партнерских программ изнутри и приведен анализ по самым атакуемым странам и отраслям в мире в 2 частях.

КИБЕРИМПЕРИЯ ШИФРОВАЛЬЩИКОВ

ROOT LEVEL RESOURCES

Часть 1

Мы полагаем, что анализ развития киберимперии даст возможность оценить предпосылки к ситуации, с которой бизнес во всем мире столкнулся сегодня, теряя миллионы долларов из-за атак шифровальщиков. Так, чтобы понять, как произошел переход киберпреступности от сложных целевых атак к нецелевым партнерским программам по распространению вредоносного программного обеспечения *(далее по тексту –ВПО)*, необходимо проследить историю развития подобных сервисов.

Для начала предлагаем Вам определится, 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 выкупа для восстановления доступа. Сама идея требования выкупа позаимствована из всем известных DDoS-атаки, которые были особенно популярны в начале 2000-х. Тогда злоумышленники высылали письма с угрозами совершения DDoS-атаки и требовали заплатить выкуп чтобы этого не произошло. Подобный шантаж приносил довольно неплохие доходы: бизнес был не готов ни к простоям, ни к отражению подобных атак. Однако коммерческий потенциал таких инцидентов снизился с появлением различных CDN-сервисов с интегрированными опциями защиты от DDoS. Поэтому преступникам пришлось искать новые способы атак с целью вымогательства.

Фактически класс ВПО, который мы называем программы-вымогатели, всегда делился на два подтипа:

Локеры

Цель — заблокировать доступ к самому устройству, например запретить жертве войти в MS Windows без ввода дополнительного пароля.

Шифровальщики

Цель — 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.

Именно подобную цепочку можно проследить далее, в подготовленном нами материале:

Ключевые тренды

- Впервые появился **Data Leak Site** (дальше по тексту - DLS) с ложными данными об атаках
- Примерно **30%** компаний соглашаются на условия и выплачивают выкуп.
- Лидерами стран-жертв по прежнему являются **США** (49,2%), **Канада** (5,6%) и **Франция** (5,2%) сменившая на этом месте Великобританию
- Атакуют самые монетизируемые отрасли, а именно: **Производство** (9,6%), **Недвижимость** (9,5%) и **транспорт** (8,2%).
- Новая тройку лидеров-вымогателей выглядит так: Conti (16,5%), Lockbit (11,5%) и Avaddon (7,5%). Обращаем Ваше внимание, что лидер прошлого года — группа **Maze** - прекратила свое существование.
- На DLS выкладываются данные только **10%** атакуемых компаний.
- Количество новых партнерских программ выросло на **23%**
- Количество DLS для публикации выгружаемых из зашифрованных сетей выросло на **115%**
- Количество жертв на DLS выросло на **935%**
- Большая часть партнерских (**87%**) программ уходит в приватную работу, однако в них по-прежнему можно вступить, если знать преступников лично.
- Выкуп не спасет от утечки данных, так как многие злоумышленники удаляют данные компаний с DLS, однако скомпрометированные файлы по-прежнему доступны по ссылкам.

Прогнозы развития рынка RANSOMWARE-AS-A-SERVISE (дальше по тексту RaaS)

- В результате запрета на андеграундных форумах публичных партнерских программ появился форум RAMP, где активность вымогателей была разрешена. Это дает нам основания предполагать, что количество новых партнерских программ сохранятся.
- Сохраняется высоким риск продажи скомпрометированных компаний на DLS. Такая деятельность злоумышленников и ранее была активной, но пока не стала трендом.
- Мы предполагаем, что основные атакуемые отрасли не изменятся, так как злоумышленники считают их наиболее монетизируемыми.
- Количество скомпрометированных данных компаний, публикуемых на публичных ресурсах операторов программ-вымогателей, будет расти. Также будет расти количество самих DLS.

История зарождение нового криминального мира И развития рынка RAAS 1989-2021

ROOT LEVEL RESOURCES

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
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

Самым первым «протошифровальщиком», напоминающий современные методы, был **AIDS Trojan**, который распространялся на дискетах или через CD-диски еще в 1989 г. 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. А до появления первых DLS — сайтов с публикацией данных компаний-жертв, отказавшихся платить выкуп, остается еще три десятка лет, в то время как до появления первых партнерских программ RaaS — порядка двадцати.

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. Выглядело это так:

2004 – 2008

Один из самых относительно современных шифровальщиков появился в конце 2004 г. Именно тогда на многих IT-ресурсах пользователи жаловались на то, что они «поймали» какое-то ВПО, зашифровавшее их файлы по алгоритму CRZ. У каждой из жертв на устройстве был сгенерирован специальный текстовый файл, который сегодня принято называть Ransom Note. Проще говоря - это «послание», в котором сообщалось что данные зашифрованы и для их расшифровки необходимо связаться по определенным email-адресам. Выполнив эти действия они получали ссылку на сайт, где можно было купить декодер. В начале каждого зашифрованного файла была подпись **PGPcoder**, благодаря которому первый шифровальщик и получил свое название. PGPcoder распространялся через рассылки в формате .doc с вредоносными макросами, но уже к 2006 г. разработчик усовершенствовал алгоритм шифрования и перешел на RSA.

Принято считать, что именно PGPcoder положил начало первой волне троянов-шифровальщиков, которая длилась с 2004 по 2008 г. Однако PGPcoder не получил широкого распространения, потому что был нацелен исключительно на физических лиц и перегружал низкопроизводительные компьютеры и его активность было достаточно просто обнаружить.

Новое ВПО под названием Cryzip появилось в марте 2006 г. Оно использовало элементарную логику для шифрования файлов: архивировало файлы в защищенный паролем ZIP-архив и удаляло оригинал. Данное ВПО содержало текстовый файл о выкупе на английском языке. Для разархивирования файлов требовался пароль, который можно было получить заплатив выкуп. В качестве платежной системы использовали E-Gold. После успешных атак Cryzip, такая схема требования выкупа стала популярной. Cryzip даже называли новым поколением троянов.

Большой интерес к ZIP-трояну Cryzip привел к появлению похожего ВПО – **Archiveus (aka MayArchive)**, который использовал RSA-1024 для шифрования файлов. Одним из самых сложных моментов такого ВПО было получение денежных средств (так как еще не было BTC). Принято считать, что распространялось такое ВПО в приватных сообществах, либо с ним работала только одна преступная группа, которая занималась и разработкой, и распространением, поскольку информация о его продаже не появлялась на IT-ресурсах.

Период локеров и появление партнерских программ

2009 – 2012

После PGPcoder, в 2005 г., появился еще один известный троян **Krotten**, который использовал совсем иную схему вымогательства. Он не зашифровал файлы, а редактировал реестр, приводя к невозможности нормального функционирования системы (блокировали работу ОС, после чего выводил сообщение с требованием выкупа). Данный троян принято относить к типу локеров.

Этой же схеме последовали трояны **SMS Lockers**. Самым известным их представителем был троян с название **Winlock (aka winlocker)**. До распространения данного ВПО среди пользователей была популярна программа Winlock Pro, которая блокировала доступ к ОС по истечению определенного периода времени. Много разновидностей подобных троянов появилось уже к 2009 г., но их суть не менялась.

Winlock стал первым ВПО, которое стали продавать и распространять на андеграундных форумах в мае 2009 г., что и стало причиной небывалого всплеска атак с его использованием. Кроме того, именно Winlocker начал развивать первые партнерские программы по вымогателям. Одна из первых партнерских программ по локерам появилась в январе 2010 г. Основная ее идея заключалась в том, что участнику выдавался троян, который он должен был распространять среди пользователей и получать процент от прибыли за разблокировку, а точнее за отправленные СМС.

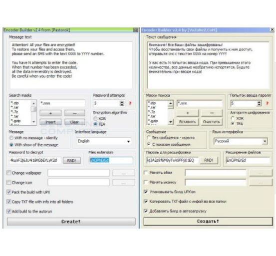
Исходя из опубликованных на форумах сообщений мы видим, что популярность локеров началась с 2009 г., а пик славы пришелся на 2012 г., после чего их популярность начала спадать:

Продолжение господства локеров и первые современные шифровальщики

2011 – 2013

Не успела популярность винлокеров сойти на нет, как на форумы вернулись трояны, которые позволяли шифровать данные пользователей и требовать выкуп. Так, наступила эпоха шифровальщиков.

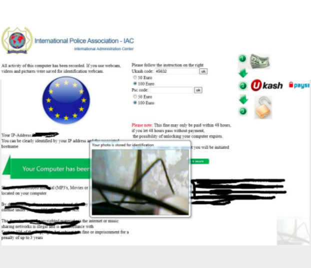
Первый известный троян, который работал по этой схеме появился в конце 2010 г. – **Encoder (aka xorist)**. Его автор выложил не только исходные коды ВПО, но и билдер, что позволяло пользователям автоматически генерировать вредоносные сэмплы со своими настройками:



Однако злоумышленники, которые тестировали данное ПО, считали, что у него слишком низкая конвертация. Проблема заключалась в том, что жертвы не понимали, что произошло, а также как работать с декодером.

Сперва, локеры и шифровальщики были крайне непопулярны так как считалось, что этот тип ПО привлекает слишком много внимания, а также оставался вопрос схемы получения выкупа. Судя по сообщениям на 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.

В июле 2012 г. появился новый локер **Ulocker**. Исходя из описания, он работал по следующим странам: Австрия, Германия, Греция, Испания, Италия, Кипр, Нидерланды, Польша, Португалия, Румыния, Финляндия, Франция, Швейцария, Швеция. Кроме всего у Ulocker'а были очень продвинутые лэндинги, которые позволяли отображать изображение с веб-камеры, перехваченное ВПО:



Немного позже некоторые локеры начали использовать новую тактику: они перезаписывали Master Boot Record (MBR), что в итоге приводило к тому, что пользователь не мог запустить даже ОС.

В это же время появляется еще один известный локер **Reveton**, который блокировал ОС и требовал выплатить штраф. Лендинг был выполнен в виде требования Министерства юстиции США и распространялся он через известное ВПО **Citadel**.

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

И только к концу 2012 г. жертвами атак шифровальщиков стали четыре австралийских компании:

TDC Refrigeration and Electrical	Byron Community Primary School	Deanes Buslines	Gold Coast medical centre
Сентябрь 2012	Октябрь 2012	Ноябрь 2012	Декабрь 2012
Сумма выкупа: 3 000	Сумма выкупа: 5 000	Сумма выкупа: 3 000	Сумма выкупа: 4 000
Отрасль: Производство	Отрасль: Образование	Отрасль: Перевозки	Отрасль: Здравоохранение

За расшифровку данных преступники требовали крайне небольшие денежные суммы. Однако именно тогда стало ясно, что атаки на бизнес могут быть гораздо более эффективными, чем атаки на физические лица. Настала пора переходить на криптолокеры.

Первые партнерские программы по шифровальщикам

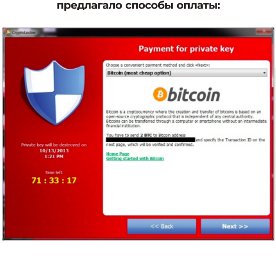
2012 – 2014

Одна из первых партнерских программ по локерам, связанная с шифрованием файлов, появилась в июне 2013 г. Такой 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.

Но уже в сентябре 2013 г. появился один из самых известных шифровальщиков с названием **CryptoLocker** (Кампания по его распространению началась 05.09.2013 г.). Сейчас его название превратилось в устойчивый термин и используется для любого ВПО подобного типа, однако ранее их называли либо «локерами», либо «шифровальщиками», а также «вымогателями» или ransomware.

Окно трояна после заражения выглядело следующим образом:

После продолжения оно предлагало способы оплаты:



Cryptolocker был одним из первых шифровальщиков, который за крайне короткий период времени заразил огромное количество жертв. По словам исследователей, к середине декабря 2013 г. (за 3 месяца) было заражено больше 200 000 компьютеров. В мае 2014 г. данный шифровальщик был изолирован в ходе операции Tovar. Тогда 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

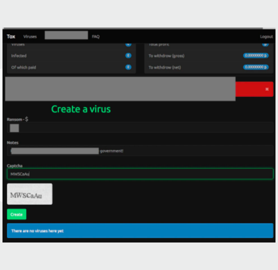
2014 – 2016

Популярность и эффективность Cryptolocker способствовала тому, что в 2013-2014 гг. увеличилось количество злоумышленников, которые продают различные версии ВПО с функцией шифрования файлов:

- Декабрь 2013 — **PowerLocker**
- Январь 2014 — **File encoder**
- Февраль 2014 — **TorrentLocker**, **Tor Locker**
- Май 2014 — **Obertone**
- Июнь 2014 — **CryptvouFiles**, **CTB-Locker**, **Gates of Cerberus**
- Июль 2014 — **Exaction Cryptolocker**
- Август 2014 — **RSA Locker**
- Ноябрь 2014 — **Coinvault**

Известный шифровальщик **VaultCrypt** начинает свою активность в феврале 2015 г. И уже в марте 2015 г. по данному шифровальщику запускается полноценная партнерская программа.

Самым распространенным криптолокером за 2014 г. был признан **TorrentLocker**. По итогам 2014 г. его владельцы заработали около 500 000 $.



Отдельно стоит отметить появление в мае 2015 г. партнерской программы **Tox Ransomware**, которая предлагала онлайн-конструктор ВПО, доступный на определенном сайте в .onion и выглядело следующим образом:

Так, любой пользователь мог сгенерировать себе сэмпл шифровальщика, указать сумму денежных средств для расшифровки и использовать его для получения прибыли.

Одна из крупных атак шифровальщиков произошла в мае 2015 г: были заражены компьютеры Министерства юстиции Вьетнама. Сумма выкупа названа не была. А уже в октябре 2015 г. зафиксировали атаку на школьную компьютерную сеть Нью-Джерси, и тут злоумышленники требовали и порядка 124 000 $, что уже начинает напоминать текущие расценки известных групп, атакующих с помощью программ-вымогателей.

Кроме того, в октябре 2015 г. пользователи жаловались, что их сервера под управлением Windows Server стали жертвами некоего ВПО **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.

Известный шифровальщик **Chimera** появился в ноябре 2015 г. У него было две отличительные особенности: с его помощью атаковали исключительно юридические лица и угрожали жертвам публикацией зашифрованных данных в открытом доступе.

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 г. появляется шифровальщик **Linux.Encoder**, нацеленный на систему под управление Linux, которые в основном принадлежат компаниям, а не частным лицам.

Однако самым известным шифровальщиком за 2015 г. стало ВПО под названием **CryptoWall**. Впервые его обнаружили еще весной 2014 г. По подсчетам экспертов за 2014 г. злоумышленники заработали $18 000 000 $, а уже в 2015 г. – 325 000 000 $. Судя по использованию одних и тех же Bitcoin-кошельков, предполагается, что у них не было публичной партнерской программы, а за программу отвечала одна группировка.

Таким образом, 2015 г. становится переломным для развития шифровальщиков – фокус злоумышленников все чаще смещается в сторону бизнеса. Финансово мотивированные группы начинают осознавать, что атаковать юридические лица значительно выгоднее.

Популяризация вымогателей, Wannacry

2016 – 2018

Как уже было сказано выше, в конце 2015 г. злоумышленники переключились на атаки компаний. Преступники начали «коллекционировать» email различных корпораций и государственных учреждений для проведения атак. 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.

Одна из самых известных и крупных партнерских программ по шифровальщикам на то время – **Cerber Ransomware** стартует 24.02.2016 г. и уже в июле 2016 г. она станет самым распространенным вымогателем. За расшифровку данных требовалось оплатить 500 $ на сайте, размещенном в сети Tor.

Первый полноценный шифровальщик для Mac OS X под названием KeRanger был зафиксирован в марте 2016 г. Для его распространения был взломан ресурс известной программы Transmission и заменен на свою копию.

В конце марта 2016 г. появляется троян **Petya**. Помимо шифрования он перезаписывал Master Boot Record (MBR), что в итоге приводило к тому, что пользователь даже не мог запустить ОС (подобная техника применялась обычными локерами в 2012 г.). Чуть позднее вместе с этим локером начал распространяться локер **Mischa**, который шифровал файлы без MBR, если прав было недостаточно.

В июле 2016 г. такую же технику начинает использовать другой шифровальщик – **Satana**.

Шифровальщик **ZCryptor** появляется в мае 2016 г. Он обладал новой техникой, свойственной классическим вирусам – самораспространением на различные устройства.

В ноябре 2016 г. появились шифровальщики, использовавшие 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.**

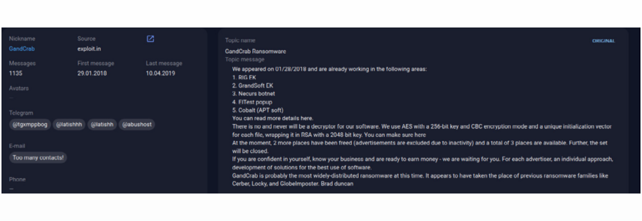
12.05.2017 г. на андеграундных форумах начали появляться жалобы пользователей, что их файлы зашифрованы новым шифровальщиком, который меняет расширение на WNCRY. За короткое время данным ВПО было зашифровано около полумиллиона устройств. Основной причиной столь быстрого распространения было то, что троян имел способность к самораспространению с помощью эксплойта **EternalBlue** и последующей установки бэкдора **DoublePulsar**. Эта история показала злоумышленникам, что для массового распространения ВПО можно использовать известные уязвимости. Поэтому чуть позднее, а именно 27.06.2017 г., другой шифровальщик **NotPetya** использовал ту же уязвимость для своих атак.

Формирование современных трендов RaaS: GandCrab

2018 – 2019

В январе 2018 г. появляется одна из самых известных партнерских программ **GandCrab.** Группа REvil использовала исходные коды именно этого ВПО для разработки своего трояна. Данная партнерская программа прослужила прародителем практически всех основных трендов, которые до сих пор используются.

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



Так, они начали набирать команды специальных партнеров, которые специализируются на крупных целях. Именно эта партнерская программа стала родоначальником **Big Game Hunting**.

28.02.2018 г. веб-панель GandCrab была взломана, в результате чего они потеряли около четверти своих приватных ключей. Но уже 07.03.2018 г. они перезапускают партнерскую программу и теперь хранят ключи на отдельном от административной панели сервере.

Данная партнерская программа отличалась от остальных постоянными улучшениями ВПО и поиском новых технологий с целью повышения конвертации загрузок в выплаты от клиентов (они первыми, еще в феврале 2018 г. вводят прием оплаты в криптовалюте DASH), а также продуманной работой с партнерами. Они сами подробно изучали разные методы получения доступа в сеть. Кроме стандартных фреймворков **Cobalt Strike** и **MSF** они использовали приложения, позволяющие использовать социальную инженерию как основной вектор атаки. К примеру, систему для целевых фишинговых атак - **Mephistophilus**. Также GandCrab были первыми, кто официально заявил, что они заключают договоры с Recovery компаниями по восстановлению данных.

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

Согласно приведенной статистики GandCrab 2018 г. по своим партнерам:

- В апреле их недельный оборот составлял более 100 000 $
- За май месяц некоторые из них заработали от 100 до 200 тысяч $
- За июнь месяц было инфицировано 315 365 компьютеров

За июль 2018 г. 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, которая позже 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. GandCrab были первой группировкой, которая начала постоянно скупать доступы таких пользователей.

В августе 2018 г. GandCrab меняет логику приема новых партнеров – теперь для участия в программе необходимо пройти собеседование. Подобная практика будет затем перенята другими злоумышленниками. Исходя из сообщений данной преступной группы, в качестве связки эксплойтов для получения доступа они использовали Fallout.

В сентябре 2018 г. выходит очередное обновление GandCrab в результате чего, их месячный доход составил более 1 млн $. Из новаторских особенностей необходимо выделить следующие:

- В административной панели новой версии появился билдер скрипта **PowerShell**, который позволял прогружать полезную нагрузку в обход антивирусных систем.
- Теперь зашифрованные файлы имели динамическое расширение (они менялось от машины к машине).
- GandCrab начали работать напрямую с крипт-сервисом **NTCrypt**.

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

17.10.2018 г. злоумышленники предоставили гражданам Сирии бесплатный декриптор. В результате, 27.10.2018 г. антивирусным компаниям удалось получить мастер-ключ путем анализа сгенерированных ключей и сделать универсальный декриптор. В связи с этим 28.10.2018 г. злоумышленники сделали новый мастер-ключ и стали переходить на новую схему шифрования, которая не зависела от него.

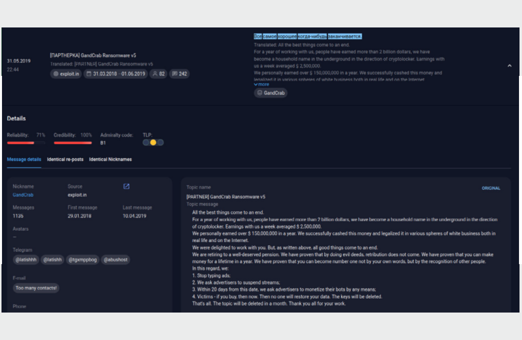
Уже в обновлении от 31.10.218 г. у шифровальщика появилась функция сканирования RDP и брутфорса RDP внутри сети с использованием паролей, который достал Mimikatz.

В январе 2019 г. 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.

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

31 мая 2019 GandCrab внезапно уходит с рынка.

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

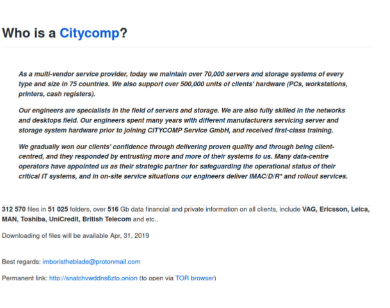


Современные тренды: double extortion, появление DLS, запрет партнерских программ

2019 – 2022

В марте 2019 г. на форуме exploit.in появляется реклама новой партнерской программы **Ransomware Snatch**. Ее отличительной чертой было то, что в ней не работали с трафиком и загрузками, а сфокусировались исключительно на атаках на корпоративные сети.

28.04.2019 г. пользователь под псевдонимом truniger публикует интересный пост на форуме exploit.in, где он сообщает, что сеть компании Citycomp была взломана и зашифрована, а все данные были выгружены. По его словам, компания отказалась выплачивать деньги за расшифровку, поэтому некая группа решила выложить их данные в публичный доступ:



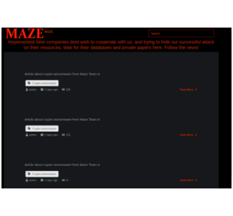
Как мы видим, там же был указан .onion домен, на котором они собирались хранить утечку в будущем – snatchvwddns6zto.onion. В ходе обсуждения данной утечки, автор поста уточнил, что данные и должны были быть опубликованы в случае отказа компании.

Вероятно, что Truniger ранее работал в GandCrab и занимался получением доступов к сетям (после чего 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.

Новый шифровальщик, который распространялся через набор эксплойтов Fallout, изначально назвали **ChaCha** (по названию алгоритма шифрования) появляется в мае 2019 г. Ранее его использовал также GandCrab. В июне 2019 г. операторы данного ВПО дали ему название **Maze**. Однако самое интересное произошло в ноябре 2019 г.: 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. 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 г. 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 09.12.2019 г. они регистрируют домен mazenews.top, который Maze использует для публикации утечек.

Первые публикации утечек там появляются 15.12.2019 г.:



Тактику 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 г. 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. И уже на следующий день к движению

"No more ransom!" присоединяется другой крупный андеграундный форум exploit.in. Однако это не остановило злоумышленников и в июле 2021 г. на DLS странице группы **Babuk**, вместо данных скомпрометированных компаний появляется реклама нового форума под название RAMP основной целью которого является создание новой площадки для рекламы партнерских программ вымогателей. Эта площадка сработала, там быстро появились следующие программы: **Lockbit v.2, Avos, Caodabi Locker, RTM, Hive.**

ROOT LEVEL RESOURCES

Синонимом кибервымогательства в сети стал термин Ransomware. По сути, он стал технологическим фундаментом масштабной теневой индустрии, а его атаки с использованием программ-вымогателей превратились в главную угрозу для государственного и коммерческого секторов во всем мире.

Операторы шифровальщиков и участники их партнерских программ зарабатывают миллионы долларов, нанося ущерб компаниям во всех странах мира. Это привело к тому, что тысячи злоумышленников, занимавшиеся взломами сетей, трафиком, загрузками, разработкой ВПО, целевыми атаками оказались востребованными в новой гигантской нише киберкриминального мира.

Так и появилась киберимперия шифровальщиков.