АТАКИ С ИСПОЛЬЗОВАНИЕМ ШИФРОВАЛЬЩИКОВ

ROOT LEVEL RESOURCES

Когда мир сталкивается с неизвестной эпидемией, закрываются границы, бизнес балансирует на грани рентабельности, а политическое противостояние между странами приобретает все более острые формы, один показатель неизменно растет – уровень киберпреступности.

В период пандемии стремительно увеличивается количество кибератак от прогосударственных хакерских групп и киберкриминала, эксплуатирующих тему COVID-19 с использованием шпионского ПО, шифровальщиков, бэкдоров. Злоумышленники совершенствуют способ проникновения в сети предприятий, адресно атакуя сотрудников, работающих удаленно, путем заражения их компьютеров вредоносными программами, через которые получают доступ в корпоративную сеть.

Одна из основных проблем компаний — уязвимые версии ПО в публичных сервисах или слабые пароли, в то время как злоумышленниками создаются шифровальщики, нацеленные на остановку процессов, связанных с приложениями технологических сетей, что позволяет им более эффективно шифровать ценные данные производственных предприятий.

Шифровальщики стали настолько популярны, что в открытом доступе на GitHub стали публиковать готовые проекты Ransomware-As-A-Service для Linux, MacOS и Windows, например проект RAASNet.

Появление партнерских программ шифровальщиков

У разработчиков шифровальщиков не всегда есть средства и возможности для проникновения в корпоративные сети. Для решения этой проблемы они начали открывать партнерские программы двух типов:

Публичные

отличительной особенностью которых является открытый поиск партнеров на андерграундных форумах

К примеру: Revil; BuranZeppelin; NetWalker; Lockbit; Avaddon; Exorcist; Thanos; Phobos; SunCrypt.

Приватные

которые не афишируются и рассчитаны на сотрудничество с другими группами злоумышленников (например, APT-группами) и проверенными пользователями

К примеру: Maze; JSWORMNemty; Ako.

Стоит отметить, что многие партнеры предпочитают не афишировать свою деятельность, но анализ активности в хакерском сообществе, а также информации, полученной в результате реагирования на инциденты, позволяет обнаруживать некоторых из них.

Векторы компрометации

Предлагаем Вам ознакомится с таблицей, в которой раскрыты партнерские программы шифровальщиков и способы получения первоначального доступа, которые используют их операторы:

Шифровальщик	Фишинг	Взлом общедоступного приложения	Проникновение через внешнюю удаленную службу	Взлом в цепи поставок
Revil	✓	✓	✓	✓
MegaCortex	✓		✓	
Maze	✓	✓	✓	
Dharma			✓	
JSWORM → Nemty	✓	✓	✓	
Buran → Zeppelin	✓	✓	✓	
NetWalker	✓		✓	
Ako	✓	✓	✓	
Lockbit			✓	
Avaddon	✓	✓		
Thanos	✓		✓	
Ryuk	✓	✓		✓
REvil		✓	✓	
Megacortex	✓			
Maze	✓			
DoppelPaymer			✓	✓
Clop	✓	✓		
Lockbit			✓	

После компрометации

После изначальной компрометации многие операторы шифровальщиков сначала пытаются получить более высокие права доступа (с помощью эксплоитов или пост-эксплуатационных фреймворков), а после этого производят попытку получить доступ к другим учетным записям с помощью различного ПО (например, Mimikatz, LaZagne) или брутфорса.

Также производится разведка сети с использованием вполне легитимных сканеров сети или фреймворков (например, Cobalt Strike, Metasploit), что позволяет узнать информацию о системе, группах, сетевых ресурсах, политике паролей, domain trust relationships и т. п.

Ниже представлена таблица использования различных фреймворков операторами шифровальщиков:

Шифровальщик	Cobalt Strike	Metasploit	CrackMapExec	PoshC2	Koadic	PowerShell Empire
Ryuk	✓	✓				✓
REvil		✓	✓			
Megacortex	✓					
Maze	✓					
DoppelPaymer				✓	✓	
Clop	✓	✓				
Lockbit			✓			

Кража и публикация данных

Ранее злоумышленники только шифровали данные и требовали выкуп у пользователей, а с 2020 года появилась новая техника: перед шифрованием они копируют всю информацию на свои серверы с целью дальнейшего шантажа. Обычно для этого используются стандартные протоколы — HTTP, HTTPS, FTP и легитимные облачные хранилища (в редких случаях, задействуются электронная почта и мессенджеры).

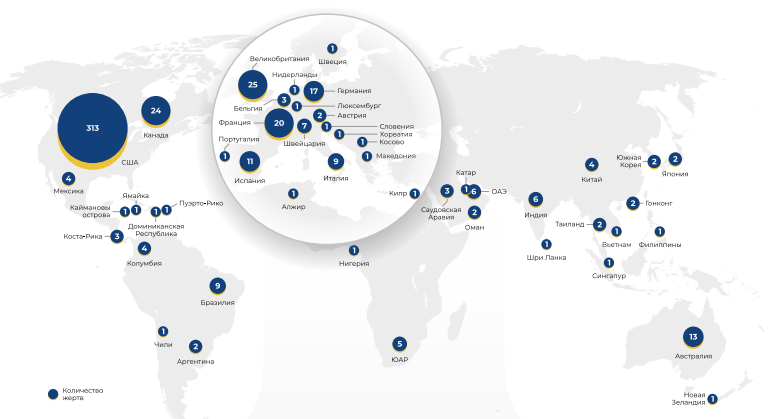
Теперь, если жертва не заплатит выкуп, она не только потеряет данные, но они будут еще опубликованы в свободном доступе операторами шифровальщика. Для увеличения прибыли некоторые группы не просто выкладывают данные, а проводят аукционы по их продаже.

Статистика атак

ROOT LEVEL RESOURCES

Среди жертв шифровальщиков есть как небольшие локальные компании, так и международные гиганты. Всего за последний год известно о более чем 500 успешных атаках шифровальщиков на компании в более чем 45 странах. Общее количество успешных атак значительно больше, но пострадавшие компании предпочитают не рассказывать об инциденте, заплатив вымогателям, либо атака не сопровождалась публикацией данных из сети жертвы.

Статистика по странам



Статистика по индустриям

Производство **94**

Торговля **51**

Государственный учреждения **39**

Здравоохранение **38**

Строительство **30**

Образовательные услуги **29**

IT **28**

Юридические услуги **20**

Логистика и хранение **18**

Административные и вспомогательные услуги, а также услуги по обращению с отходами и переработкой **14**

Телекоммуникации **12**

Бухгалтерские услуги **11**

Консалтинг **9**

Инженерное дело **9**

Обработка, хранение данных и связанные услуги **9**

Дизайн **8**

Агентства недвижимости **8**

Научно-исследовательские **7**

Страхование **7**

Инвестиции **6**

Кредитование **6**

Добыча природных ресурсов **6**

Другое **6**

Сельское хозяйство **5**

Энергетика **5**

Банковское дело **4**

Маркетинг **4**

Некоммерческие организации **4**

Группы компаний **3**

Издательства **3**

Турагентства **3**

Гостеприимство **3**

Искусство и развлечения **2**

Вещание **2**

Азартные игры **2**

Авиация **2**

Аукционные дома **1**

Автопром **1**

Продукты питания **1**

Менеджмент **1**

Транспорт **1**

Профессиональные организации **1**

Наиболее активными шифровальщиками с 2020 года являются Maze и REvil — на них приходится более 50% успешных атак. Во втором эшелоне идут Ryuk, NetWalker, DoppelPaymer.

Количество жертв и оценка ущерба

ROOT LEVEL RESOURCES

Самой атакуемой отраслью стало производство. В целом половина всех атак пришлась на производство, торговлю, государственные учреждения, систему здравоохранения, строительную отрасль и образовательные сервисы. При этом партнеры выбирают максимально доступные цели для своих атак, что объясняет большое распределение по разным отраслям.

Шифровальщик/ Общее количество жертв	Страны	Индустрии	Средняя сумма выкупа/ Потенциальный ущерб
Maze **155**	93 США 8 Канада 6 Франция 6 Италия 6 Великобритания	30 Производство 19 Торговля 15 Строительство 8 Административные и вспомогательные услуги, а также услуги по обращению с отходами и переработке 7 Здравоохранение	**$2 420 000** **$375 100 000**
REvil **103**	63 США 7 Великобритания 5 Австралия 4 Швейцария 3 Канада	20 Производство 17 Торговля 10 IT 6 Юридические услуги 4 Государственные учреждения	**$300 000** **$30 900 000**
Ryuk **62**	53 США 5 Испания 1 Австралия 1 Великобритания 1 Германия	16 Государственные учреждения 14 Образовательные услуги 14 Здравоохранение 3 Издательства 3 IT	**$1 451 500** **$89 993 000**
NetWalker **49**	28 США 6 Франция 4 Канада 2 Великобритания 1 Австрия	14 Производство 6 Здравоохранение 5 Образовательные услуги 4 Торговля 3 Логистика и хранение	**$720 000** **$35 280 000**
Pysa **25**	5 США 3 Великобритания 2 Канада 2 Франция 2 Мексика	5 Здравоохранение 3 Государственные учреждения 3 Производство 2 Строительство 2 Образовательные услуги	**Неизвестно** **Неизвестно**
DoppelPaymer **53**	35 США 5 Франция 3 Канада 1 Саудовская Аравия 1 Катар	8 Торговля 7 Государственные учреждения 6 Производство 4 Логистика и хранение 3 Строительство	**$1 143 500** **$60 605 500**
Nefilim **13**	3 Бразилия 3 Индия 1 Германия 1 Франция 1 Швейцария	4 Производство 2 Строительство 2 Добыча природных ресурсов 1 Логистика и хранение 1 Административные и вспомогательные услуги, а также услуги по обращению с отходами и переработке	**$100 000** **$1 300 000**
Ragnar **10**	7 США 1 Португалия 1 Германия 1 Сингапур	2 Маркетинг 2 Юридические услуги 1 IT 1 Производство 1 Строительство	**$7 750 000** **$77 500 000**
Clop **15**	7 Германия 2 США 1 Испания 1 Австрия 1 Великобритания	6 Производство 2 IT 2 Логистика и хранение 1 Азартные игры 1 Государственные учреждения	**$400 000** **$6 000 000**
Ako **9**	6 США 2 Великобритания 1 Канада	2 Строительство 1 Юридические услуги 1 Дизайн 1 Инженерное дело 1 Производство	**$300 000** **$1 800 000**
Avaddon **1**	1 США	1 Строительство	**$7 500** **$7 500**
Sekhmet **6**	3 США 1 Бразилия 1 Великобритания	2 Производство 1 Юридические услуги 1 IT	**Неизвестно** **Неизвестно**
Snake **3**	1 Германия 1 Аргентина 1 Япония	1 Здравоохранение 1 Энергетика 1 Группы компаний	**Неизвестно** **Неизвестно**
MegaCortex **1**	1 США	1 Обработка и хранение данных и связанные услуги	**Неизвестно** **Неизвестно**
Conti **16**	13 США 2 Канада 1 Испания	3 Производство 2 Гостеприимство 1 IT 1 Страхование 1 Здравоохранение	**$200 000** **$3 200 000**
SunCrypt **2**	1 США 1 Канада	1 Производство 1 Дизайн	**$400 000** **$800 000**
WastedLocker **1**	1 США	1 Производство	**Неизвестно** **Неизвестно**

К сожалению, оценить реальный ущерб достаточно сложно. Оценка ущерба должна складываться из: сумм, выплаченных жертвами, потерь в случае простоя, а также трат на восстановление нормального функционирования внутренних систем. Дополнительная сложность — получить информацию об атаках, так как многие компании платят злоумышленникам выкуп и не сообщают об этом.

Данные, приведенные выше, описывают только известные инциденты и показывают нижнюю границу ущерба. Но это лишь верхушка айсберга. Например, известно всего лишь о 62 инцидентах с использованием Ryuk, который активно распространялся с помощью банковского трояна Trickbot. При этом, по данным специалистов Group-IB, владельцы бот-сети Trickbot за последний год успешно зашифровали более 2500 разных сетей, используя такие шифровальщики, как Ryuk (позже Conti), Kraken, Thanos. 62 известных инцидента — это лишь 2,5% от общего числа, а значит, и реальный ущерб гораздо больше.

Продажа данных спецслужбам

ROOT LEVEL RESOURCES

Некоторые прогосударственные группы пытаются найти дополнительное финансирование. Как и обычный криминал, они начинают продавать доступ в корпоративные сети или используют программы-шифровальщики. Известными примерами заработка с использованием шифровальщиков для прогосударственных групп являются случаи:

Группа Lazarus вновь вернулась к разработке вымогателей и атаковала европейские компании шифровальщиком VHD Ransomware. Хакеры получали доступ с помощью уязвимого VPN-шлюза, повышали права до администратора и устанавливали бэкдор DadS. Они перемещались по сети жертвы и шифровали файлы комбинацией AES-256 в режиме ECB и RSA-2048.

В мае 2020 года, китайские хакеры из APT41 по предположению тайваньских властей стояли за атакой вымогателей на энергетические и технологические компании острова. Так пострадала тайваньская компания CPC Corp., которая отвечает за доставку нефтепродуктов по Тайваню. Атака не повлияла на производственные процессы CPC, но помешала клиентам использовать платежные карты CPC Corp. для покупки газа. В ходе этой волны атак был задействован новый шифровальщик — ColdLock. Анализ указывает на сходство между ним и двумя ранее известными семействами вымогателей, в частности Freezing и образовательным набором вымогателей EDA2.

Весной 2020 года, группа китайских хакеров IronTiger стояла за использованием шифровальщика HybirdRansom против компаний Азиатско-Тихоокеанского региона. Шифровальщик состоит из нескольких компонентов, последовательно запускающих друг друга для блокировки машины и шифрования файлов: Locker, Loader и Cryptor.

ROOT LEVEL RESOURCES

Мы уверены, что постоянный обмен данными, совместные усилия по поддержанию киберстабильности в мире, создание и развитие партнерских отношений между частными компаниями и международными правоохранительными органами — эффективный путь борьбы с киберпреступностью. Осознанное отношение мирового сообщества к кибербезопасности поможет сохранить и защитить глобальные возможности цифрового пространства и свободу коммуникаций.