КАК ОПЕРАТОРЫ ПРОГРАММ-ВЫМОГАТЕЛЕЙ АТАКОВАЛИ РОССИЙСКИЙ БИЗНЕС В 2021

→ GROUP-IB

НОЯБРЬ 2021

GROUP-IB

group-ib.ru

Дисклеймер

1. Технический обзор подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью обзора является предоставление сведений о тактике, об 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 обзоре приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в обзоре дано исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в обзоре информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Обзор 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, цитирования в объеме, оправданном правомерной целью цитирования, при условии, что сам обзор, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Обзор 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.

Обзор подготовлен экспертами Group-IB:

→ **Олег Скулкин**
руководитель лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB

Введение

2 года

операторы программ-вымогателей остаются угрозой номер 1 для компаний

RDP

Самый популярный способ компрометации. На него пришлось 60% всех атак, произошедших на территории России

на 200%

выросло количество атак на российские организации за 2021 год

40 млн рублей

максимальная сумма первоначального выкупа

250 млн рублей

максимально запрошенный выкуп операторами программ-вымогателей

Второй год подряд операторы программ-вымогателей становятся главной угрозой безопасности для большинства компаний.

В средствах массовой информации регулярно появляются новости о громких атаках, но все они происходят за рубежом. Исключением может показаться кейс металлургической компании **ЕВРАЗ**, которая была атакована операторами программы-вымогателя Ryuk в марте 2020, что привело к остановке производства на 3,5 недели. Но если изучить детали, становится понятно, что даже эта атака коснулась лишь инфраструктуры, расположенной в Северной Америке.

Означает ли это, что операторы программ-вымогателей обходят Россию стороной? Или дело в том, что пострадавшие организации просто не хотят предавать подобную информацию огласке?

Из-за того, что большинство атакующих русскоязычные и партнерские программы расположены на русскоязычных форумах, многие считают Россию источником этой угрозы. На самом деле первые атаки с использованием программ-вымогателей, нацеленные на корпоративные сети, были организованы группой из Ирана, распространявшей с 2016 по 2018 год шифровальщик SamSam.

По данным Лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB, количество атак на организации на территории России в 2021 году увеличилось **более чем на 200%**.

Россия следует мировым трендам – наиболее популярным способом проникновения в сетевые инфраструктуры организаций является компрометация публично доступных терминальных серверов (RDP). На них пришлось 60% всех расследованных атак. На фишинговые рассылки, где первичным вектором проникновения атакующих в сеть стала электронная почта, пришлось 22%, на эксплуатацию публично доступных приложений – 14%, на иные методы – 4%.

Размер запрашиваемого у российских компаний выкупа значительно варьируется и зависит от величины организации. Он колеблется от нескольких десятков тысяч до сотен миллионов рублей. Так, максимальный запрошенный выкуп составил 250 млн рублей.

В 2020-21 годах наиболее активными на территории России были операторы следующих программ-вымогателей:

Dharma **Crylock** **Thanos**

С использованием каждой из программ было совершено более 100 атак.

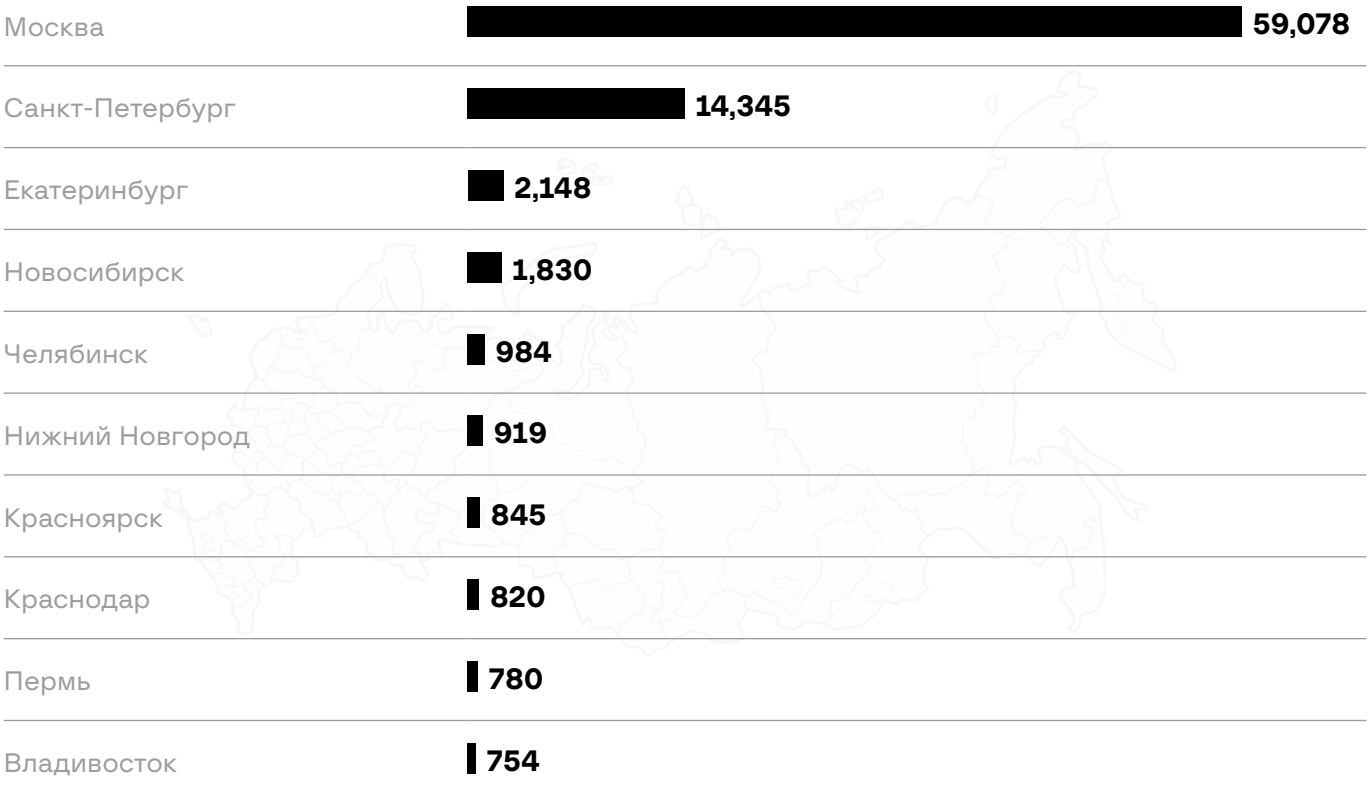
С точки зрения реализации атак и методов работы вымогателей существуют некоторые отличия от мировых трендов. Ни одна из групп, работающих на территории России, не использует публичные веб-сайты для публикации данных жертв, которые отказались платить выкуп. Также за отчетный период не проводилось ни одного открытого аукциона, где на продажу выставляли бы украденные у компании данные. Но это не означает, что данные не выгружаются – обычно злоумышленники предоставляют доказательства выгрузок непосредственно в ходе переговоров.

В данном обзоре мы разберем основные методы получения первоначального доступа, а также тактики, техники и процедуры, используемые злоумышленниками для достижения их цели. Указанные техники доступны в сформированной матрице MITRE ATT&CK®.

Публично доступные терминальные серверы

Компрометация публично доступных терминальных серверов, доступ к которым осуществляется посредством протокола удаленного рабочего стола, традиционно является наиболее популярным способом получения первоначального доступа.

Пандемия COVID-19 заставила многие организации быстро организовывать возможность удаленной работы для своих сотрудников. Из-за этого количество таких серверов увеличилось, а с ним – и количество атак на них.

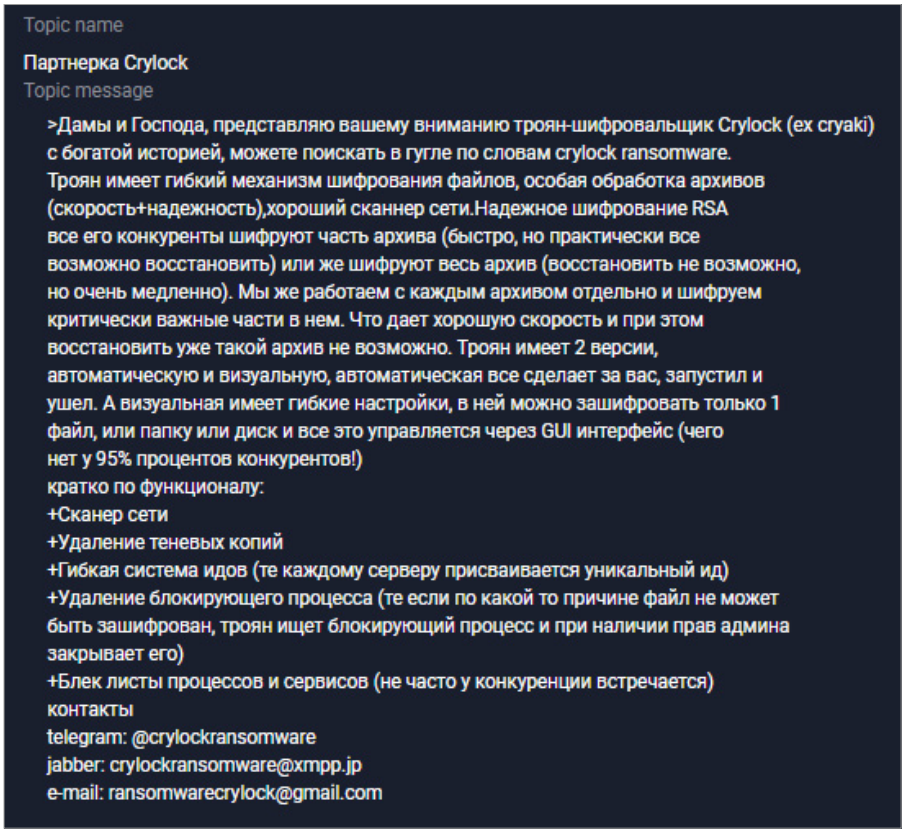


Публично доступные терминальные серверы на территории России, согласно Shodan

Зачастую причиной успешной компрометации является использование стандартных учетных записей и слабых паролей. Кроме того, ИТ-специалисты организаций используют терминальные серверы как временное решение и не воспринимают потенциальную угрозу утечки данных всерьез. В результате это играет на руку злоумышленникам.

В рамках реагирований на подобные инциденты специалисты Group-IB чаще всего встречали участников партнерских программ **Dharma** и **Crylock.**

Отдельного внимания заслуживает Crylock, чья партнерская программа активно рекламировалась на русскоязычных теневых форумах:


Topic name

Партнерка Crylock

Topic message

>Дамы и Господа, представляю вашему вниманию троян-шифровальщик Crylock (ex cryaki) с богатой историей, можете поискать в гугле по словам crylock ransomware.
Троян имеет гибкий механизм шифрования файлов, особая обработка архивов (скорость+надежность),хороший сканнер сети.Надежное шифрование RSA все его конкуренты шифруют часть архива (быстро, но практически все возможно восстановить) или же шифруют весь архив (восстановить не возможно, но очень медленно). Мы же работаем с каждым архивом отдельно и шифруем критически важные части в нем. Что дает хорошую скорость и при этом восстановить уже такой архив не возможно. Троян имеет 2 версии, автоматическую и визуальную, автоматическая все сделает за вас, запустил и ушел. А визуальная имеет гибкие настройки, в ней можно зашифровать только 1 файл, или папку или диск и все это управляется через GUI интерфейс (чего нет у 95% процентов конкурентов!)
кратко по функционалу:
+Сканер сети
+Удаление теневых копий
+Гибкая система идов (те каждому серверу присваивается уникальный ид)
+Удаление блокирующего процесса (те если по какой то причине файл не может быть зашифрован, троян ищет блокирующий процесс и при наличии прав админа закрывает его)
+Блек листы процессов и сервисов (не часто у конкуренции встречается)
контакты
telegram: @crylockransomware
jabber: crylockransomware@xmpp.jp
e-mail: ransomwarecrylock@gmail.com

Данные о партнерской программе Crylock, собранные системой Group-IB Threat Intelligence & Attribution

Несмотря на то, что эти атаки обычно не отличаются сложностью, все больше и больше компаний становятся жертвами групп кибервымогателей. Во многом это происходит из-за того, что компании используют примитивные средства защиты, обойти которые злоумышленникам не составляет труда.

Часто хакеры копируют архив с широким набором инструментов, которые используют позже.

На первом этапе атакующие отключают средства защиты на первично скомпрометированном сервере, например при помощи Process Hacker или GMER. После этого они пытаются получить дополнительные учетные данные с помощью Mimikatz или утилит разработки NirSoft, например WebBrowserPassView, CredentialsFileView и других.

Получив привилегированные учетные данные, атакующие сканируют сеть при помощи SoftPerfect Network Scanner или KPortScan, чтобы определить доступные хосты.

Продвижение по сети чаще всего осуществляется с использованием протокола удаленного рабочего стола, при этом программа-вымогатель запускается вручную на каждом хосте.

До недавнего времени такие атаки не предполагали выплаты значительного выкупа, в среднем он составлял несколько сотен тысяч рублей. Тем не менее, в последние несколько месяцев ситуация изменилась – теперь размер выкупа может достигать 4 000 000 рублей.

Эксплуатация публично доступных приложений

Уязвимости в публично доступных приложениях также стали причиной многих успешных атак с применением программ-вымогателей в 2021 году по всему миру. Безусловно, многие из этих приложений не так популярны в России, но и здесь не обошлось без исключений.

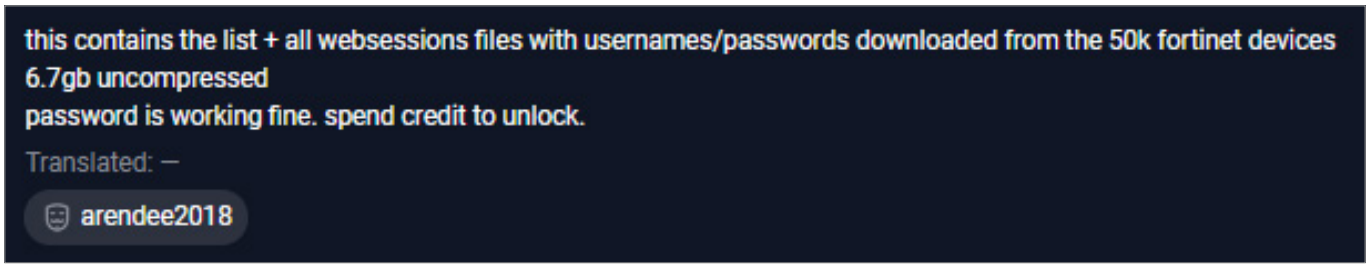
Ярким примером является уязвимость в VPN-серверах Fortigate, получившая идентификатор CVE-2018-13379. Несмотря на свой возраст, данная уязвимость остается актуальной и по сей день, в том числе и для организаций, расположенных на территории России.

Успешная эксплуатация данной уязвимости позволяет атакующим получить учетные данные прошедших аутентификацию пользователей. Благодаря этому они могут не только получить доступ в корпоративную сеть, но и в некоторых случаях осуществлять продвижение по ней.

Отметим, что при включенной мультифакторной аутентификации, таких последствий можно было бы избежать даже при успешной эксплуатации.

В одном из инцидентов, который расследовала Group-IB, атакующие воспользовались данной уязвимостью и получили доступ в корпоративную сеть организации. После этого они применили встроенное в операционную систему средство шифрования дисков – BitLocker, и в результате запросили выкуп за расшифровку, который составил 20 000 000 рублей.

Примечательным также является факт публикации на теневых форумах почти 50 000 логинов и паролей, полученных по результатам эксплуатации рассматриваемой уязвимости:



Сведения о распространении логинов и паролей, полученных по результатам эксплуатации уязвимости CVE-2018-13379, собранные системой Group-IB Threat Intelligence & Attribution

Безусловно, значительный размер выкупа мотивировал атакующих к увеличению активности. Специалисты Group-IB до сих пор наблюдают инциденты, где рассматриваемая уязвимость является причиной успешного получения первоначального доступа к скомпрометированной корпоративной сети.

Фишинговые рассылки

40 000 000 рублей

максимальный выкуп, полученный OldGremlin в результате одной из атак

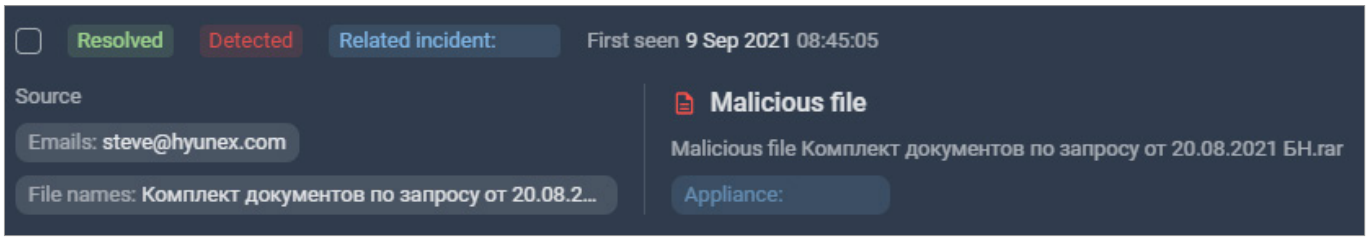
Тренд на использование массовых фишинговых рассылок для получения первоначального доступа к корпоративным сетям в 2021 году добрался и до России. Раньше основными игроками были русскоговорящие группы, которые принципиально обходили стороной страны СНГ и использовали для атак трояны Trickbot, Dridex, IcedID, Qakbot и другие. Теперь и группы, атакующие российские компании, начали применять фишинговые рассылки для получения первоначального доступа.

Согласно отчету Лаборатории Касперского, начиная с декабря 2020 года, русскоязычная группа RTM, ранее фокусирующаяся на дистанционном банковском обслуживании (ДБО), добавила в свой арсенал программу-вымогатель Quoter. Таким образом, даже если злоумышленниками не удавалось осуществить успешную атаку на ДБО, они могли продолжить пост-эксплуатацию и развернуть программу-вымогатель на всю сеть. На данный момент активность группы RTM прекратилась.

Другой пример – русскоговорящая группа **OldGremlin**, о которой мы **рассказывали** в августе 2020 года. За время своего существования группа успела совершить несколько успешных атак, а в некоторых случаях размер выплаченного выкупа достигал 40 000 000 рублей. В своих фишинговых рассылках OldGremlin использовали разные файлы: LNK-файлы, самораспаковывающиеся архивы и, ставшие традиционными, файлы Microsoft Office. В случае успешной компрометации на компьютер жертвы загружался TinyNode – бот, написанный на NodeJS. С его помощью злоумышленники осуществляли коммуникацию со скомпрометированным хостом через анонимные скрытые службы Tor.

Помимо популярных среди злоумышленников фреймворков, таких как Metasploit и Cobalt Strike, группа пользовалась встроенными инструментами Windows для решения пост-эксплуатационных задач. Например, для создания дампа lsass.exe (Local Security Authority Subsystem Service), атакующие использовали функцию MiniDump библиотеки comsvcs.dll. Как и в случае с Quoter, OldGremlin эксплуатировали системные службы для развертывания своей программы-вымогателя – TinyCryptor.

Как уже отмечалось ранее, некоторые группы вовсе не используют программу-вымогателя, заменяя их на легитимные средства шифрования. Специалистами Group-IB была обнаружена группа **Rat Forest**, которая получала первоначальный доступ через фишинговые рассылки, используя абсолютно легитимное программное обеспечение – RMS или TeamViewer. Данное ПО рассылалось в архивах, защищенных паролем, который находился в теле электронного письма:



Вредоносное вложение, заблокированное Group-IB Threat Hunting Framework Polygon

Несмотря на примитивность используемых методов, многие атакованные организации не устояли даже перед такими атаками из-за низкого уровня защищенности.

Для извлечения дополнительных учетных данных злоумышленниками использовался ставший классикой инструмент Mimikatz, который загружался ими напрямую с GitHub на скомпрометированном хосте. В арсенале атакующих были такие инструменты для сканирования сетей, как Advanced IP Scanner и LanSpy, а также контр-криминалистический инструмент CCleaner.

Целью атакующих, например, было поместить важные для жертвы данные в контейнер VeraCrypt, после чего попросить выкуп. В некоторых случаях он достигал 1 000 000 рублей.

Выводы

Несмотря на распространенное заблуждение, Россия активно подвергается управляемым человеком атакам с использованием программ-вымогателей.

Большую популярность таких атак можно объяснить солидной суммой выкупа, которую запрашивают злоумышленники. Подобный заработок привлекает преступников по всему миру. При этом группировки, находящиеся на территории России и СНГ, предпочитают атаковать зарубежные компании. А злоумышленники, находящиеся за пределами региона, наоборот, выбирают его своей целью.

Общий уровень кибербезопасности организаций остается низким. Его едва ли достаточно для противостояния даже низкоквалифицированным злоумышленникам, работающим с программами-вымогателями. Это сказывается на используемых тактиках и методах – зачастую они настолько просты, что часть из них можно было бы предотвратить только мультифакторной аутентификацией.

За последние два года несколько крупных российских организаций стали жертвами программ-вымогателей. Злоумышленники получили значительный выкуп, что благоприятно повлияло на их рост и мотивацию.

Учитывая низкий порог входа в эту теневую индустрию, а также игнорирование базовых норм информационной безопасности российскими организациями, специалисты Group-IB прогнозируют дальнейший экспонентный рост атак вымогателей.

Для минимизации рисков был разработан перечень основных рекомендаций, который необходимо выполнить ИТ-командам и службам безопасности компаний, независимо от их масштаба и профиля деятельности. Более подробные рекомендации вы найдете в отчете **«Программы-вымогатели: 2020/2021»**.

Для более глубокого понимания техник, тактик и процедур операторов программ-шифровальщиков, вы можете ознакомиться с матрицей MITRE ATT&CK® (Adversarial Tactics, Techniques & Common Knowledge). Данные в ней основаны на опыте Group-IB, по итогам реагирования и анализа атак с использованием программ-шифровальщиков на территории России.

Программы-вымогатели 2020/2021

Тепловая карта MITRE ATT&CK® для России и СНГ на 2021 год

Initial Access	Exploit Public-Facing Application **T1190**	External Remote Services **T1133**	Phishing **T1566**	Trusted Relationship **T1199**
	Valid Accounts **T1078**			
Execution	Command and Scripting Interpreter **T1059**	Native API **T1106**	Scheduled Task/Job **T1053**	System Services **T1569**
	User Execution **T1204**	Windows Management Instrumentation **T1074**		
Persistence	Boot or Logon Autostart Execution **T1547**	Create Account **T1136**	External Remote Services **T1133**	Scheduled Task/Job **T1053**
	Valid Accounts **T1078**			
Privilege Escalation	Exploitation for Privilege Escalation **T1068**	Process Injection **T1055**	Valid Accounts **T1078**	
Defense Evasion	Abuse Elevation Control Mechanism **T1548**	Access Token Manipulation **T1134**	Deobfuscate/ Decode Files or Information **T1140**	Domain Policy Modification **T1448**
	Exploitation for Defense Evasion **T1211**	File and Directory Permissions Modification **T1222**	Impair Defenses **T1562**	Indicator Removal on Host **T1070**

Defense Evasion	Masquerading **T1036**	Modify Registry **T1112**	Obfuscated Files or Information **T1027**	Signed Binary Proxy Execution **T1218**
	Template Injection **T1221**	Use Alternate Authentication Material **T1550**		
Credential Access	Brute Force **T1110**	Credentials from Password Stores **T1555**	OS Credential Dumping **T1003**	Unsecured Credentials **T1552**
Discovery	Account Discovery **T1087**	Domain Trust Discovery **T1482**	File and Directory Discovery **T1083**	Network Service Scanning **T1046**
	Network Share Discovery **T1135**	Permission Groups Discovery **T1069**	Remote System Discovery **T1018**	
Lateral Movement	Lateral Tool Transfer **T1570**	Remote Services **T1021**	Use Alternate Authentication Material **T1550**	
Collection	Archive Collected Data **T1560**			
Command and Control	Application Layer Protocol **T1071**	Proxy **T1090**	Remote Access Software **T1219**	
Exfiltration	Exfiltration Over Web Service **T1567**			
Impact	Data Destruction **T1485**	Data Encrypted for Impact **T1486**	Inhibit System Recovery **T1490**	Service Stop **T1489**

Рекомендации для защиты от программ-вымогателей

1. Обезопасьте используемые средства удаленного доступа. Используйте мультифакторную аутентификацию или как минимум сложные и регулярно сменяемые пароли.
2. Незамедлительно устраняйте уязвимости в публично доступных приложениях, особенно те, которые могут позволить атакующим преодолеть внешний периметр.
3. Внедрите комплексную защиту электронной почты, **которая позволит обнаруживать и блокировать самые сложные угрозы**.
4. Контролируйте работу подрядчиков вашей сети. Удаленный доступ с их стороны должен быть строго регламентирован.
5. Убедитесь, что учетные записи имеют минимальные привилегии в системах. В случае компрометации это затруднит атакующим продвижение по сети.
6. Незамедлительно устраняйте уязвимости на узлах внутренней сети, которые могут позволить атакующим повысить привилегии или продвинуться по сети.
7. Осуществляйте мониторинг использования инструментов двойного назначения, которые могут помочь атакующим провести сетевую разведку, получить аутентификационные данные и пр.
8. Ограничьте доступ к облачным хранилищам. Это может затруднить атакующим выгрузку данных из корпоративной сети.
9. Используйте отдельные учетные записи с мультифакторной аутентификацией для доступа к серверам, содержащим резервные копии. Убедитесь, что у вас также есть офлайн-копии.
10. Внедрите современное **средство мониторинга и блокирования угроз**, которое позволяет локализовать и нейтрализовать атаку на любом этапе ее жизненного цикла.

Подверглись кибератаке?

Сообщите об инциденте:

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

Что делать, если ваша компания стала жертвой атаки с применением шифровальщиков?

С такой ситуацией может столкнуться бизнес любого размера и отрасли. Для оперативного решения проблемы обратитесь к Group-IB

СООБЩИТЬ ОБ АТАКЕ

Круглосуточная линия
+7 (495) 984-33-64

Почему заплатить выкуп – не выход

1. Нет никакой гарантии, что вы получите декриптор для расшифровки данных.
2. После оплаты выкупа злоумышленники могут атаковать вас снова.
3. Вы не знаете, какие еще данные оказались у злоумышленников.
4. Выкуп мотивирует злоумышленников на новые преступления.

Что даст реагирование на инцидент от Group-IB

1. **Вы вернете контроль над своими данными.** Специалисты проанализируют инцидент и сообщат, продолжают ли злоумышленники находиться в скомпрометированной сети, а также расскажут, как он произошел.
2. **Вы получите необходимые средства защиты сети.** В ходе работы эксперты используют собственные разработки Group-IB, позволяющие обнаружить потенциально вредоносную активность, а также повторные попытки компрометации.
3. **Подробные рекомендации для предотвращения атак в будущем.** Вы получите список рекомендаций по оптимизации ИТ-инфраструктуры и проведению профилактических мероприятий для недопущения повторной компрометации.

Если вы стали жертвой атаки с применением шифровальщиков, предоставьте специалистам Group-IB данные для **первичного анализа инцидента – это бесплатно.**

ЗАКАЗАТЬ

Приложите к заявке файл с требованиями выкупа и пример зашифрованного файла

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

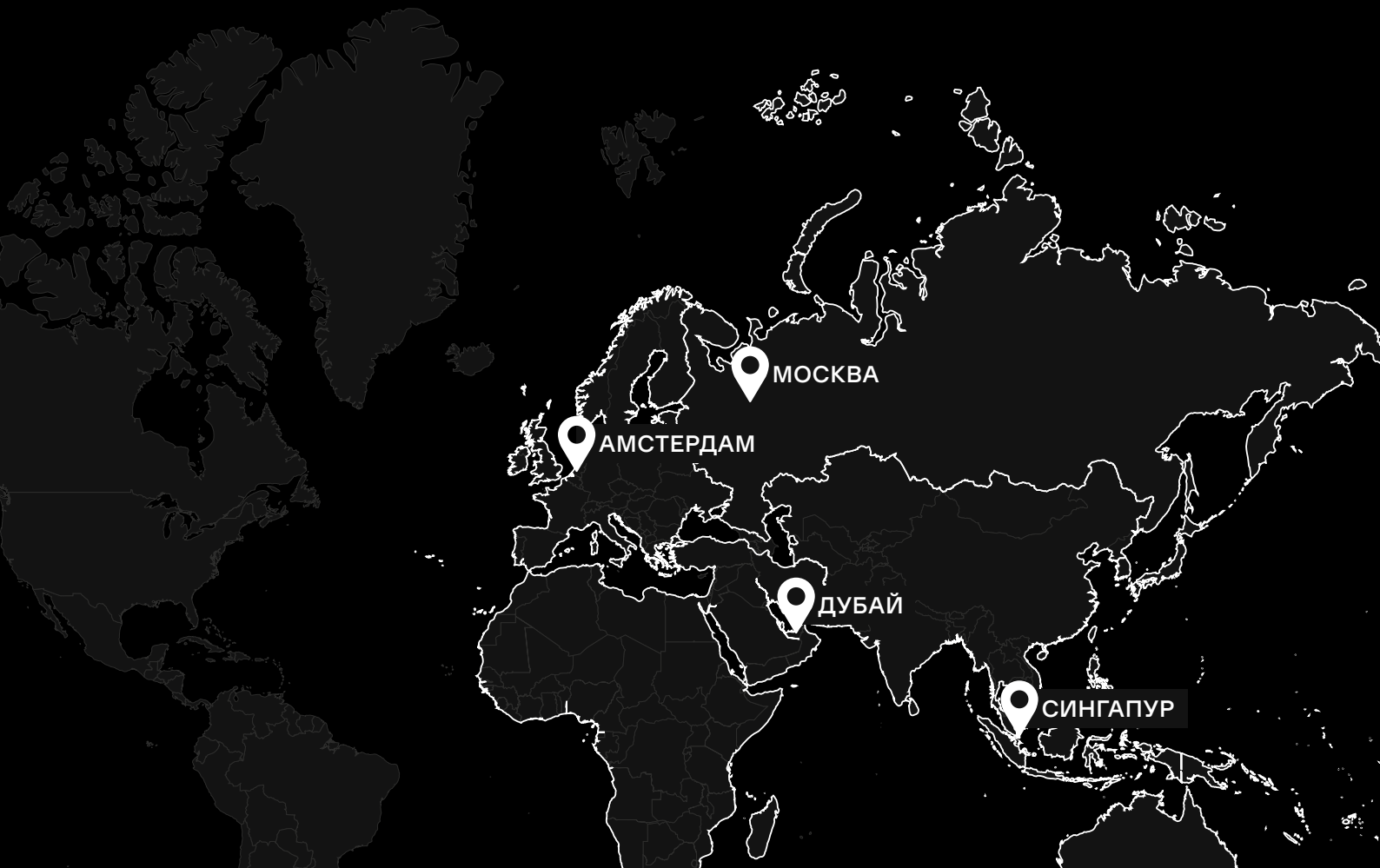
ТОП-10 В APAC

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+	70 000+	1 300+	18 лет
экспертов международного класса	часов реагирования на инциденты информационной безопасности	успешных расследований по всему миру	практического опыта

Intelligence-driven services

FORRESTER
GARTNER

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.

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.