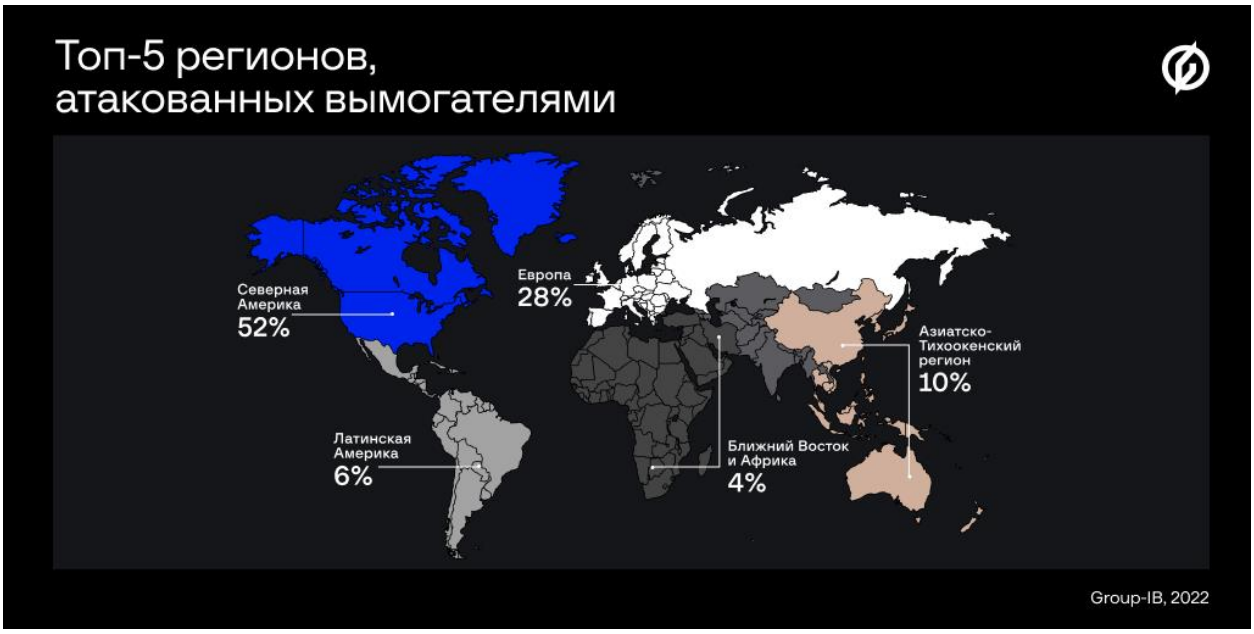
Аттракцион невиданной жадности: средний запрашиваемый выкуп вымогателей достиг $247 000

Москва, **19.05.2022** — Group-IB, один из лидеров в сфере кибербезопасности, второй год подряд выпускает отчет, посвященный одной из опасных угроз для бизнеса и госсектора во всем мире – шифровальщикам. В новом отчете **«Программы-вымогатели 2021-2022»** названы самые агрессивные операторы шифровальщиков, совершившие наибольшее число кибератак в мире: это группы **LockBit**, **Conti** и **Pysa.** Запрашиваемые злоумышленниками суммы выкупа достигли астрономических величин: средний размер требуемого выкупа составил **$247 000. В** России количество реагирований Лаборатории цифровой криминалистики Group-IB на атаки программ-вымогателей в первом квартале 2022 года выросло в 4 раза по сравнению с аналогичным периодом 2021 года.

Шифровальщики на карте мира

Третий год подряд атаки программ-вымогателей являются одной из самых серьезных и разрушительных киберугроз. Исследовав более 700 атак в 2021 году, эксперты Group-IB, выяснили, что основные цели вымогателей по-прежнему приходятся на **Северную Америку, Европу, Латинскую Америку, Азиатско-Тихоокеанский регион**. Среди нашумевших инцидентов 2021 года с участием шифровальщиков можно отметить нападения на концерн **Toshiba**, американскую трубопроводную систему **Colonial Pipeline**, крупнейшего производителя мяса **JBS Foods**, и IT-гиганта **Kaseya**. Рекорд по жадности поставили вымогатели из Hive: они потребовали от немецкого холдинга **MediaMarkt** выкуп в **$240** млн. Среднее время простоя атакованной компании в 2021 году увеличилось с **18** дней до **22** дней.



В 2021 году количество атак программ-вымогателей на российские компании увеличилось более чем на 200%. Наиболее активными в России оказались операторы шифровальщиков **Dharma**, **Crylock**, **Thanos**. А вот русскоязычная группа **OldGremlin** хотя в 2021 году заметно снизила свою активность — хакеры провели всего одну массовую рассылку (для сравнения: в 2020 году их было 10), однако атака оказалась настолько успешной, что кормила “гремлинов” весь год. Например, у одной из жертв вымогатели потребовали за расшифровку данных рекордную для России сумму — **250** млн рублей.

В первом квартале 2022 года количество реагирований экспертов Лаборатории цифровой криминалистики Group-IB на атаки программ-вымогателей в России выросло в **4** раза по сравнению с аналогичным периодом 2021 года. В последнее время шифровальщики нацелены в России исключительно на крупный бизнес — от 5000 сотрудников — из отраслей строительства, страхования, агропромышленного комплекса.

Охота за данными

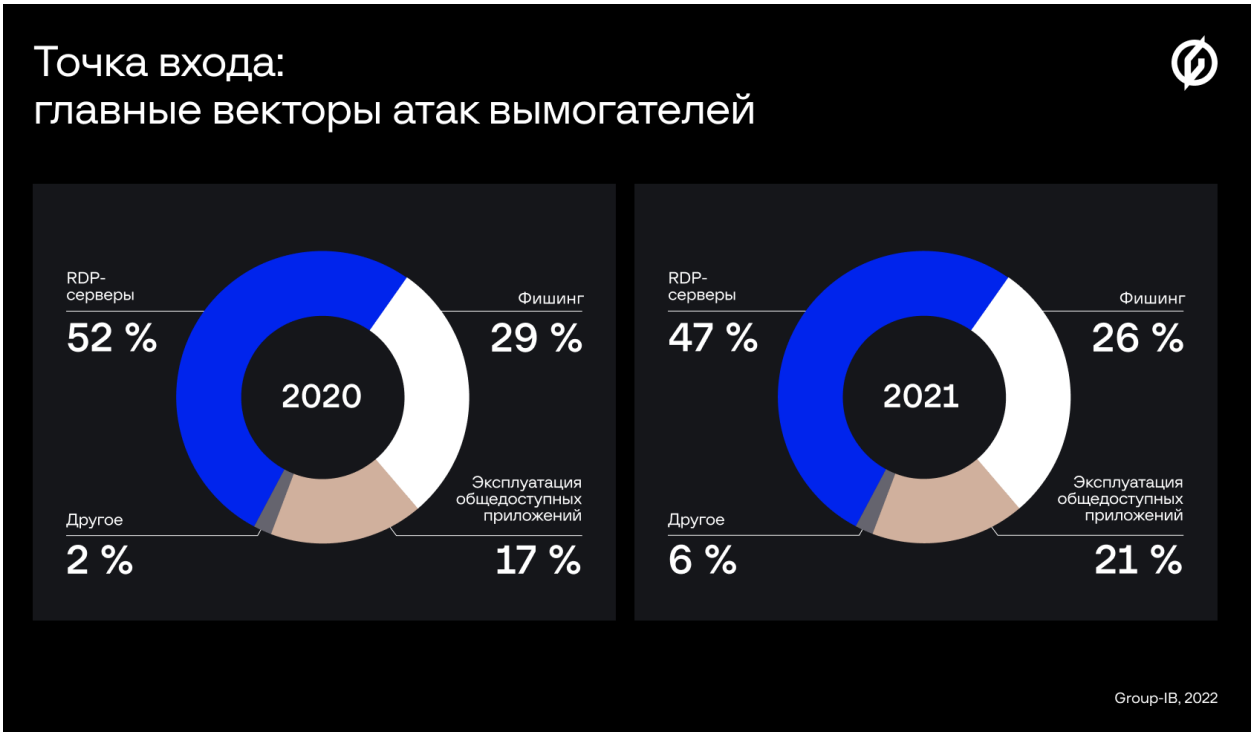
Новой тенденцией, согласно исследованию «**Программы-вымогатели 2021-2022**», стал отход на второй план шифрования, как инструмента давления на жертву. Теперь у компаний-жертв вымогают средства, угрожая выложить их конфиденциальные данные в публичный доступ на так называемые DLS **(Dedicated Leak Site). В 2021 году этим методом пользовалось подавляющее большинство шифровальщиков — 63%.**

Как отмечала Group-IB в отчете Hi-Tech Crime Trends H2 2020/ H1 2021, использование вымогателями DLS для давления на жертву, чтобы заставить ее заплатить выкуп под угрозой обнародования похищенных данных в публичном доступе, достигло пика именно в 2021 году. Число новых DLS выросло более, чем вдвое — с **13** до **28**, при этом количество выложенных данных компаний за год увеличилось на беспрецедентные **935%** — с **229** жертв до **2 371**. При этом атакующие стали гораздо быстрее добиваться своих целей: если раньше среднее время нахождения шифровальщиков в сети жертвы составляло **13** дней, то в прошлом году оно сократилось до **9**.

Еще одной тенденций 2021 года стал «ребрендинг»: группы вымогателей сменили названия. Этим «маркетинговым» инструментом операторы шифровальщиков стали пользоваться в ответ на повышенное внимание к ним со стороны исследователей и правоохранительных органов. После того как **DarkSide** и **REvil** исчезли из публичного пространства, на сцене появился новой игрок – **BlackMatter, затем его сменил BlackCat**. Чуть ранее, весной группа **DoppelPaymer** переименовала свои новые программы-вымогатели в **Grief** (Pay OR Grief).

Точка входа: векторы атаки, тактики и инструменты

Как и в позапрошлом году, самым частым способом получения первоначального доступа в сети компаний стала компрометация публичных RDP-серверов. На этот вектор атаки приходится почти половина (47%) всех исследованных инцидентов — многие из сотрудников по-прежнему работали на удаленке. На втором месте — фишинг (26%), на третьем — эксплуатация общедоступных приложений (21%).



В 2021 году некоторые операторы шифровальщиков стали «работать» через 0-day (англ. zero day) — неустранённые или еще не выявленные уязвимости, которые

используют атакующие. Так, партнеры REvil атаковали тысячи клиентов Kaseya, эксплуатируя уязвимости 0-day в серверах VSA. Другой пример — группировка FIN11, стоящая за шифровальщиком Clop эксплуатировала ряд уязвимостей нулевого дня в устаревшем средстве для передачи файлов Accellion File Transfer Appliance (FTA).

Если в 2020 году отдельные вредоносные боты (Emotet, Qakbot, IcedID) были закреплены за определенными участниками партнерских программ шифровальщиков, то в прошлом году атрибуция стала не столь очевидной. Например, IcedID использовали для получения первоначального доступа в сети компаний несколько участников партнерских программ шифровальщиков — Egregor, REvil, Conti, XingLocker, RansomExx.

А вот партнеры вымогателя Ruyk для первоначального доступа в сети жертвы использовали бот BazarLoader и в весьма экзотической схеме. Он распространялся не только через фишинг — рассылку спам-писем о платных подписках, но и через вишинг. Во время телефонного разговора злоумышленники обманом заставляли жертву посетить подложный сайт и давали инструкции о том, как скачать и открыть вредоносный документ, который скачивал и запустил BazarLoader.

Наиболее популярным инструментом у вымогателей для пост-эксплуатации ожидаемо оказался Cobalt Strike — он был замечен в 60% исследованных атак шифровальщиков. Тем не менее, некоторые злоумышленники начали экспериментировать с менее распространенными фреймворками, чтобы снизить вероятность обнаружения. К примеру, группировка TA551 экспериментировала с доставкой вредоносного программного обеспечения на основе кроссплатформенного фреймворка Sliver.

«В 2021 году киберугроза №1 впервые получила серьезный отпор — начались аресты участников преступных групп, часть вымогателей вынуждены были залечь «на дно» или замести следы, проводя ребрендинг, — замечает **Олег Скулкин,** руководитель Лаборатории цифровой криминалистики Group-IB. — Однако, несмотря на некоторую обеспокоенность киберпреступного сообщества, атаки представителей других партнерских программ продолжаются — так что говорить о закате шифровальщиков пока еще рано. Почти 70% инцидентов, над расследованием которых работает наша Лаборатория, приходятся на атаки с использованием программ-вымогателей и мы полагаем эта тенденция сохранится и в текущем году».

Полученные в ходе исследования «Программы-вымогатели 2021-2022» результаты были сопоставлены и описаны в соответствии с матрицей MITRE ATT&CK®, публичной базой знаний, в которой собраны тактики и техники целевых атак.

О компании:

Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, исследования высокотехнологичных преступлений и защиты интеллектуальной собственности в сети. Штаб-квартира расположена в Сингапуре. Центры исследования киберугроз компании находятся на Ближнем Востоке (Дубай), в Азиатско-Тихоокеанском регионе (Сингапур), в Европе (Амстердам) и в России (Москва).

Group-IB Threat Intelligence – это система исследования и атрибуции кибератак, содержащая структурированные данные о тактиках, инструментах и активности злоумышленников с возможностью персонализации под конкретную отрасль или компанию. Group-IB TI позволяет выстроить проактивную систему ИБ, ориентированную на защиту активов компании с низким количеством ложных инцидентов.

Это результат объединения 19-летнего опыта Group-IB по расследованиям, сбору и анализу информации об инцидентах ИБ, атаках, злоумышленниках и их инфраструктуре. TI от Group-IB признана лучшей в своём классе аналитическими агентствами IDC, Forrester, Gartner.
Решение Group-IB THF для проактивного поиска и защиты от сложных и неизвестных киберугроз получило признание ведущего европейского аналитического агентства KuppingerCole Analysts AG, а компания Group-IB вошла в число лидеров рынка в категориях «Product Leader» и «Innovation Leader».
Технологии Group-IB по защите от онлайн-мошенничества в интернет-банкинге и сервисах электронной коммерции получили признание Gartner, агентство присвоило Group-IB статус надежного поставщика в категории «Решения по выявлению онлайн-мошенничества». Решение Digital Risk Protection для выявления и устранения цифровых рисков, а также противодействия атакам с неправомерным использованием бренда получило престижную премию Innovation Excellence от глобального консалтингового агентство Frost & Sullivan.
В основе технологического лидерства компании и возможностей в сфере научных исследований и разработки — 19-летний практический опыт исследований киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в одной из крупнейших лабораторий компьютерной криминалистики и круглосуточном центре оперативного реагирования CERT-GIB.
Компания является резидентом «Сколково», Иннополиса и партнером Europol.

Для получения дополнительной информации:

Комарова Ника
Head of Corporate Communications
+7 910 472 24 06 | +7 495 984 3364 ext. 910
komarova@group-ib.com

Седаков Павел
Press officer
+7 909 979 87 77
sedakov@group-ib.com
Подробнее:
https://www.group-ib.ru
https://www.group-ib.ru/blog/
telegram | facebook | twitter | linkedin