

# Актуальные киберугрозы

**I квартал 2021 года**

## Содержание

Резюме	3
Сводная статистика	4
Неуловимое вредоносное ПО	8
Суммы выкупов продолжают расти	10
Небезопасное ПО	13
Прицел на виртуальную инфраструктуру	14
Прицел на разработчиков ПО и облачные сервисы	15
Прослушка, перехват сообщений и новости о 5G	17
Госучреждения — самые часто атакуемые организации	19
Об исследовании	21

## Резюме

### Итоги I квартала 2021 года:

- Количество атак увеличилось на 17% в сравнении с I кварталом 2020 года, а относительно IV квартала 2020 года прирост составил 1,2%. Целенаправленными были 77% атак. Инциденты с частными лицами составили 12% от числа всех инцидентов.
- Вредоносное ПО, которое чаще всего используют злоумышленники, — это по-прежнему шифровальщики. В I квартале они запрашивали баснословные суммы выкупа, дорабатывали свои инструменты, в том числе добавляя новые способы сокрытия от средств защиты. Появилось множество новых шифровальщиков, например Crimg, Humble и Vovalex, а старичок WannaCry снова набирает обороты. Операторы программы-вымогателя Zigggy создали прецедент: вернули выплаченные выкупы жертвам и «перешли на светлую сторону».
- Наиболее популярными уязвимостями у злоумышленников в этом квартале стали бреши в программном обеспечении Microsoft Exchange Server (ProxyLogon) и устаревшей программе для обмена файлами Accellion FTA. В VPN-решениях компании SonicWall была обнаружена уязвимость нулевого дня, воспользовавшись которой злоумышленники не только взломали саму компанию, но и приступили к атакам на клиентов. Предполагается, что SonicWall своевременно не оповестила клиентов о выявленной уязвимости и необходимости реализации защитных мер. Такой инцидент подтверждает, что производители ПО должны как можно скорее доводить до клиентов информацию о существующих уязвимостях и о том, как защититься до выпуска патча.
- Все больше злоумышленников разрабатывают свое ВПО для проведения атак на среды виртуализации, и некоторые из них пытаются активно эксплуатировать уже найденные уязвимости в ПО для развертывания виртуальной инфраструктуры. В начале 2021 года наши специалисты помогли устранить критически опасные уязвимости в продуктах VMware. Мы настоятельно рекомендуем установить обновления безопасности как можно скорее.
- Количество атак, жертвами которых становятся ИТ-компании, остается стабильно высоким уже второй квартал подряд. В течение I квартала 2021 года в 15% случаев хакеры атаковали ИТ-компании, чтобы провести атаку на их клиентов или с целью кражи данных клиентов. В начале 2021 года в СМИ все еще появляются сообщения о новых жертвах атаки на SolarWinds: клиенты компании заявляют о компрометации своих сетей.
- Телекоммуникационные компании в два раза чаще подвергались атакам, чем в IV квартале 2020 года. В 71% атак хакеры были нацелены на получение данных, причем особый интерес они проявили к технологии 5G. В девяти из десяти инцидентов злоумышленники использовали вредоносное ПО; чаще всего это было вредоносное ПО для получения удаленного доступа, его доля составила 55%.

Для защиты от кибератак, прежде всего, мы советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. Также, учитывая специфику атак в этом квартале, настоятельно рекомендуем своевременно устанавливать обновления безопасности и уделять особое внимание защите виртуальной инфраструктуры. Укрепить безопасность на периметре компании можно с помощью современных средств защиты, к примеру web application firewalls для защиты веб-ресурсов. Чтобы предотвратить заражение вредоносным ПО, советуем использовать песочницы, которые анализируют поведение файлов в виртуальной среде и выявляют вредоносную активность.

## Сводная статистика

Количество инцидентов в I квартале 2021 года в сравнении с аналогичным периодом 2020 года увеличилось на 17%, а относительно IV квартала 2020 прирост составил 1,2%. На организации были направлены 88% атак. Чаще всего злоумышленники атаковали госучреждения, промышленные компании и организации в сфере науки и образования. Основным мотивом в атаках как на организации, так и на частных лиц остается получение данных. Главными целями злоумышленников являются персональные и учетные данные, а при атаках на организации к ним добавляется еще и коммерческая тайна.

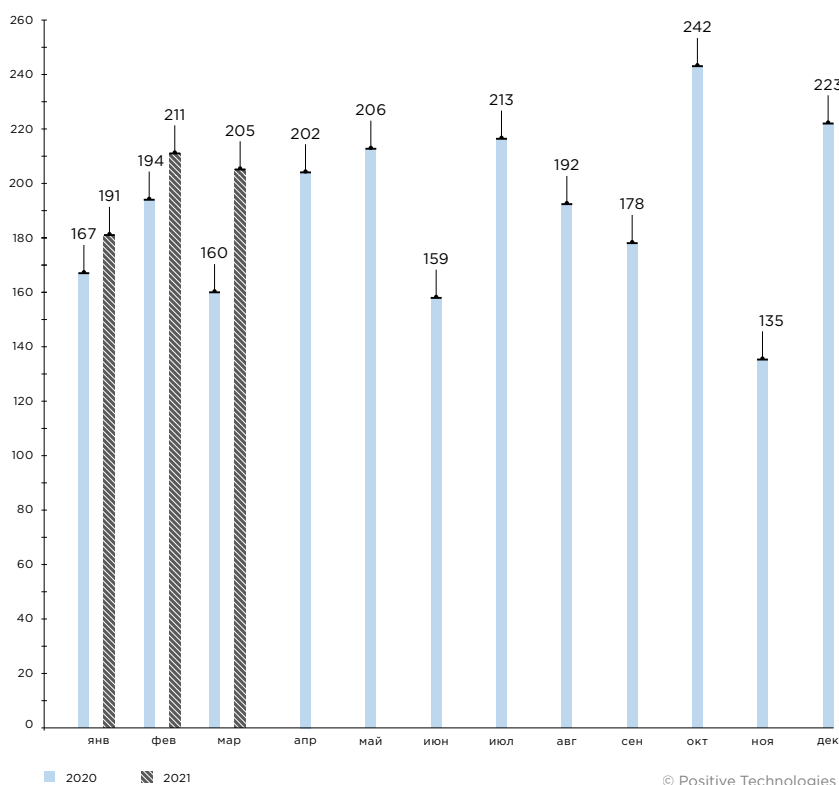


Рисунок 1. Количество инцидентов в 2020 и 2021 годах (по месяцам)

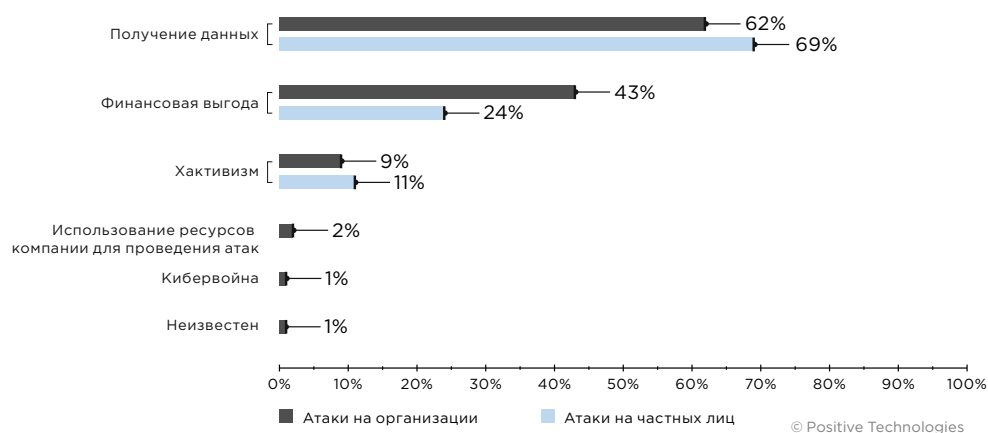


Рисунок 2. Мотивы злоумышленников (доля атак)

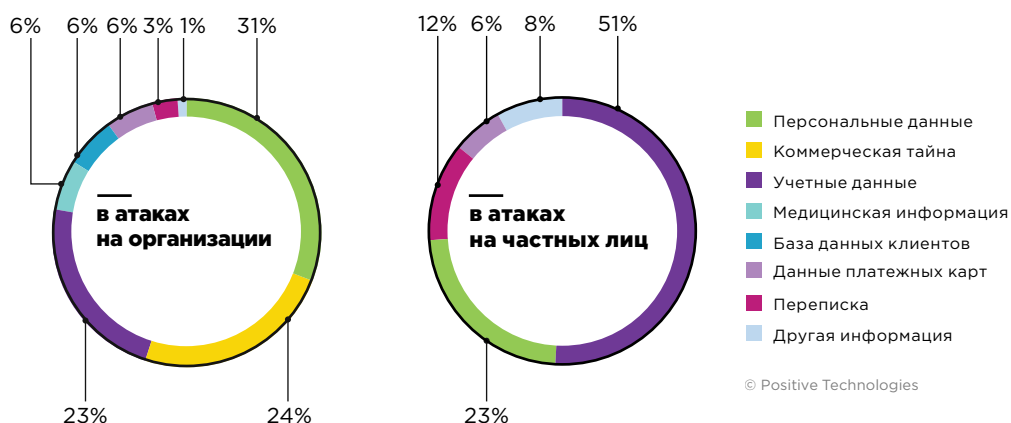


Рисунок 3. Типы украденных данных

**77% атак носили целенаправленный характер**

**12% атак направлены против частных лиц**



Рисунок 4. Категории жертв среди организаций

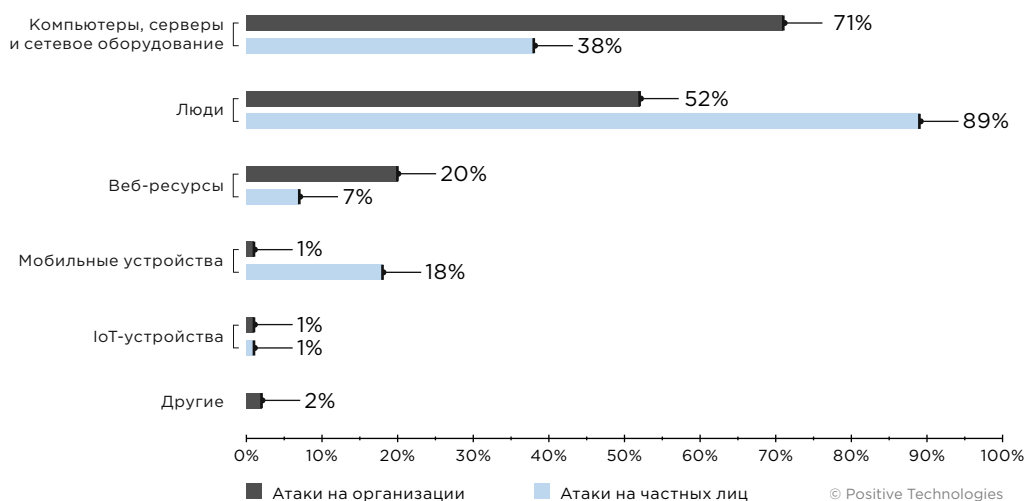


Рисунок 5. Объекты атак (доля атак)

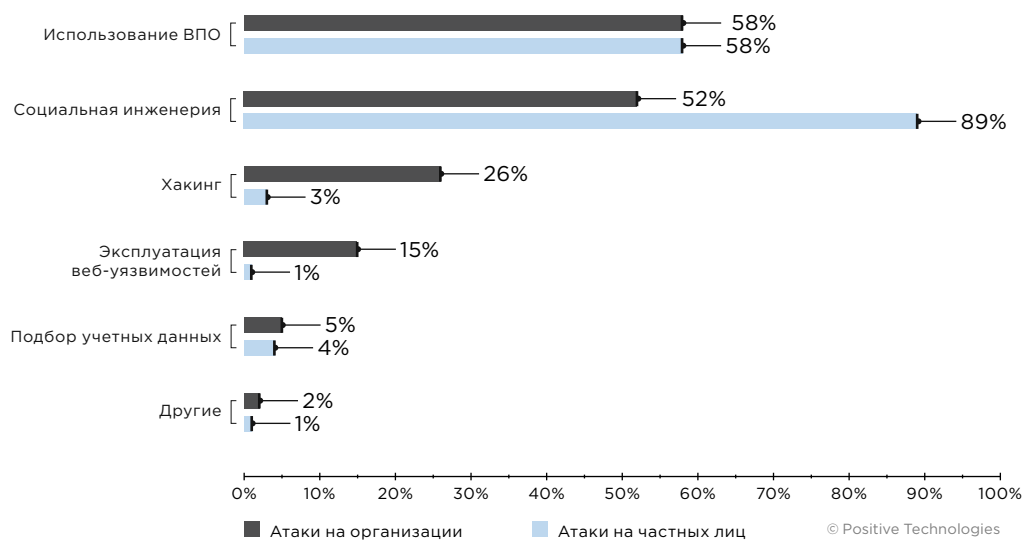
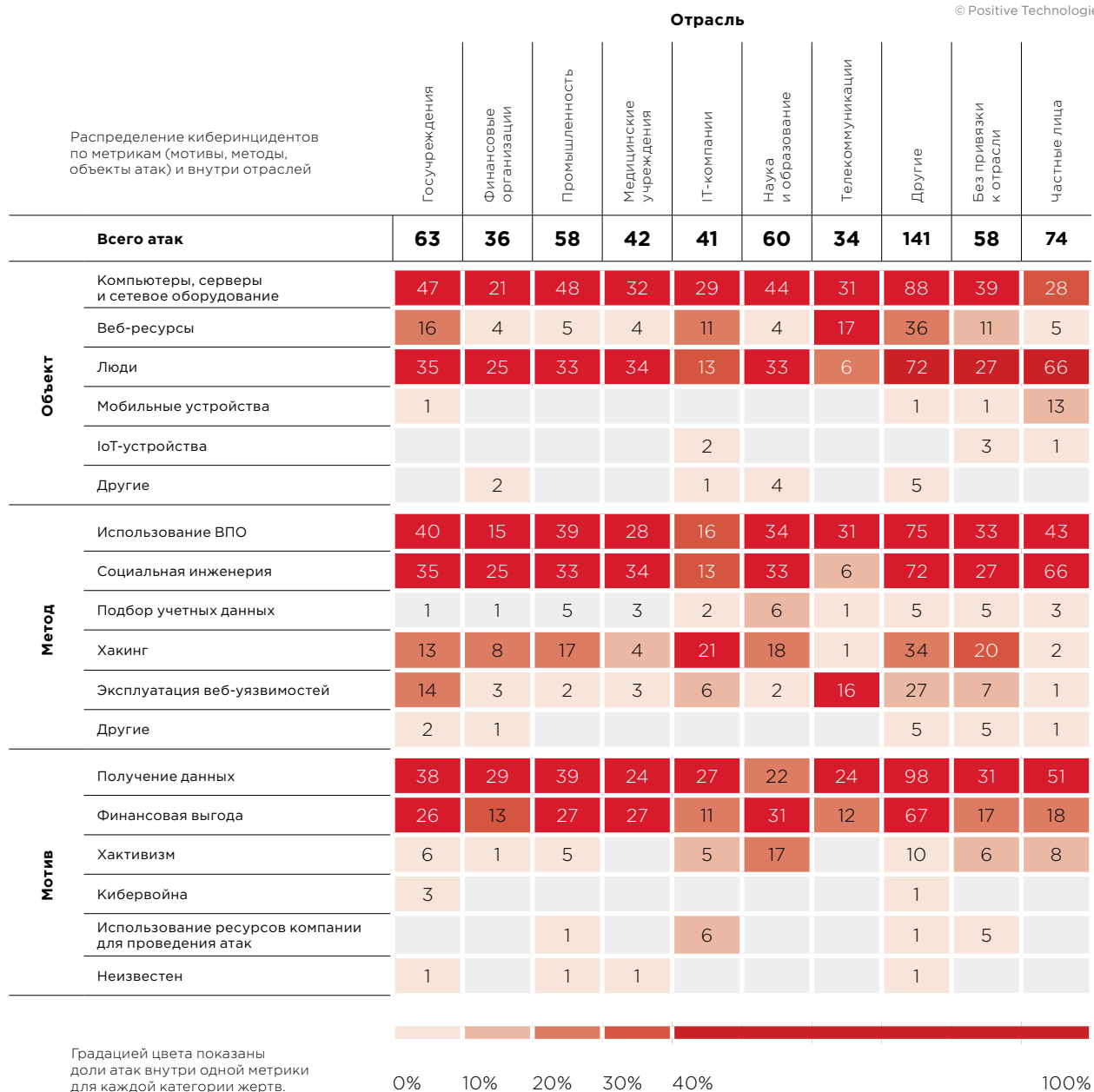


Рисунок 6. Методы атак (доля атак)



## Неуловимое вредоносное ПО

Наиболее популярным вредоносным ПО традиционно стали программы-вымогатели. Их доля среди прочего ВПО, применяемого в атаках на организации, увеличилась на семь процентных пунктов в сравнении с IV кварталом 2020 года и составляет 63%. Превалирующим способом доставки вредоносных остается электронная почта, злоумышленники использовали ее в шести из десяти атак на организации с применением ВПО. Частных лиц по-прежнему чаще всего атакуют используя банковские трояны, шпионское ПО и вредоносы, предоставляющие удаленный доступ к устройству.

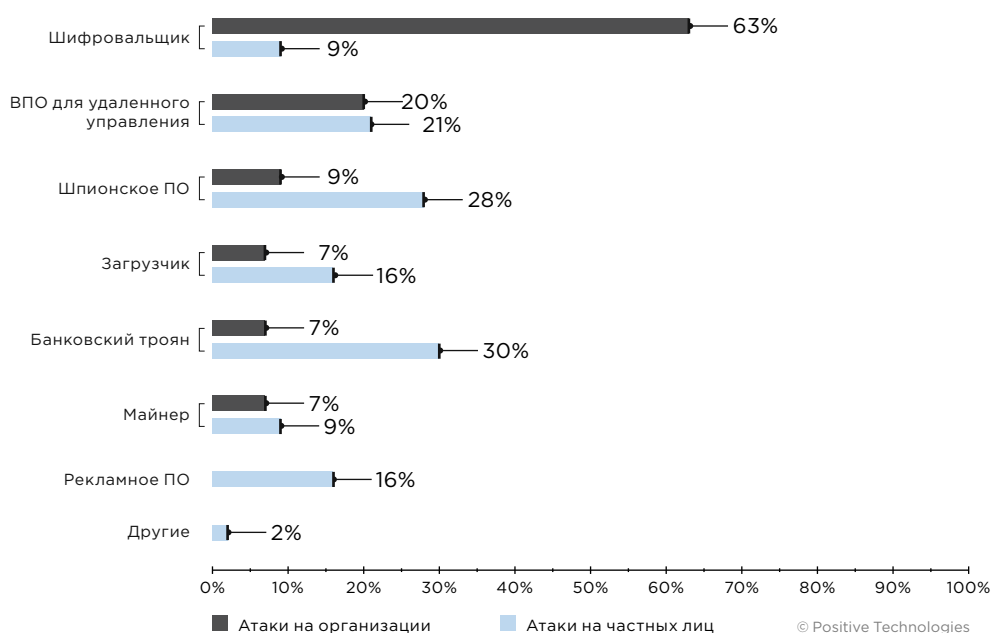


Рисунок 7. Типы вредоносного ПО (доля атак с использованием ВПО)

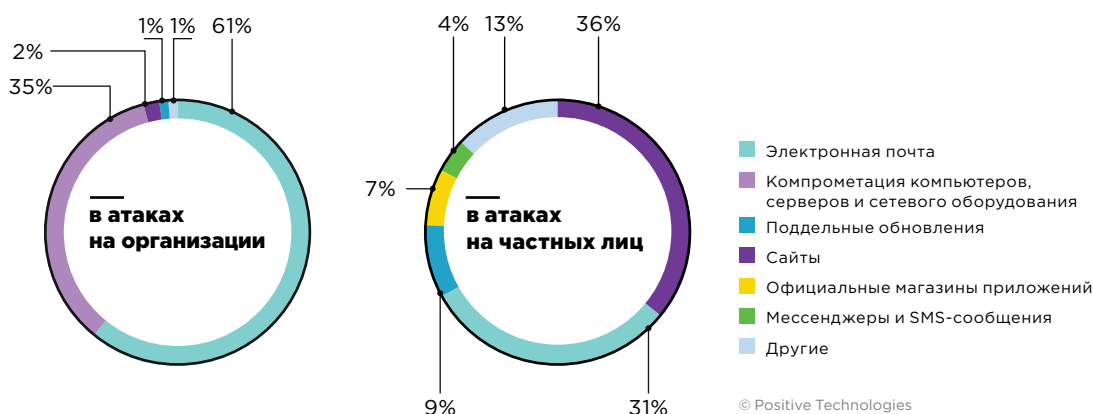


Рисунок 8. Способы распространения вредоносного ПО (доли атак с использованием ВПО)

Разработчики вредоносного ПО продолжают искать новые способы обхода средств защиты. Для достижения этой цели злоумышленники, к примеру, используют редкие языки программирования, как в случае с создателями ВПО для удаленного управления [BazarBackdoor](#), которые переписали его, используя язык Nim; операторы программ-вымогателей [Vovalex](#) и [RobbinHood](#) сразу выбрали такие редкие языки, как D и Golang соответственно.

Некоторые злоумышленники дополнили свои инструменты функциями, стирающими следы вредоносной активности. Подобное обновление было замечено у майнеров [OSAMiner](#), [Black-T](#) и [Pro-Ocean](#). В коде криптомайнера OSAMiner, ориентированного на устройства на платформе macOS, заложены функции, позволяющие завершить процессы, связанные с инструментами



мониторинга, например Activity Monitor (аналог диспетчера задач в Windows), и очистить систему от других вредоносных. Майнер Black T, нацеленный на Unix-системы, очищает историю в bash после реализации полезной нагрузки и затирает все следы своей активности. Добавленная общедоступная функция для сокрытия процесса называется libprocesshider, в случае ее обнаружения специалисты по безопасности могут предположить наличие вредоносной нагрузки. Этим инструментом также пользуются и злоумышленники, распространяющие майнер Pro-Ocean, который атакует серверы Apache ActiveMQ, Oracle WebLogic и Redis, а перед установкой проверяет среду запуска. На этом этапе он определяет, нужно ли скрывать ВПО, а если, к примеру, вредонос оказался в среде Tencent Cloud или Alibaba Cloud — запускает процесс удаления агентов мониторинга.

Еще одним способом сокрытия деструктивной нагрузки является разбивка вредоноса на архивы. Пример — троян Masslogger для сбора учетных данных. Для доставки ВПО злоумышленники используют электронную почту, а для обхода средств защиты они разбили исполняемый файл на многотомные архивы с расширениями .r00, .r01 и т. д.

Специалисты РТ ESC, проанализировав последние атаки АРТ-группировки RTM, выяснили, что злоумышленники пользуются сервисами racker as a service для обхода средств защиты. Такой подход сильно усложняет поиск известных сигнатур, но поведенческий анализ файлов в песочнице позволяет распознать вредоносную деятельность; к тому же использование крипто-ров не влияет на взаимодействие ВПО с управляющими серверами, а значит их можно обнаружить путем анализа сетевого трафика.

## Криптор (пакер)

Криптор (пакер) — это программа, использующая методы криптографии для упаковки вредоноса с целью сокрытия от средств защиты при сигнатурном анализе.

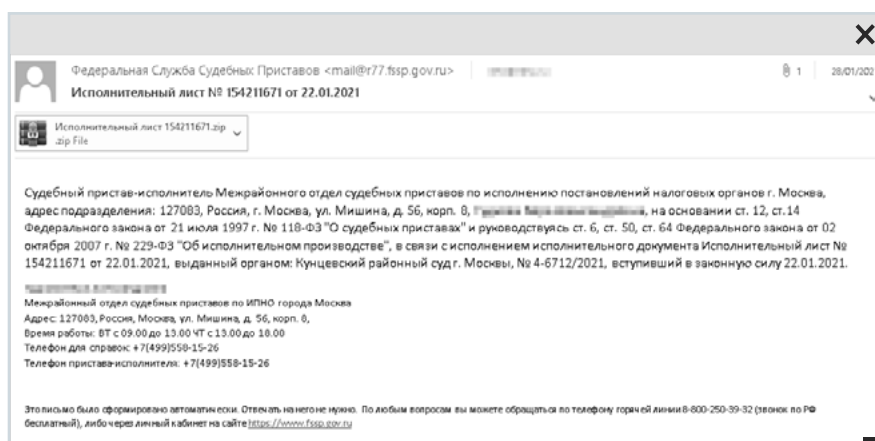


Рисунок 9. Фишинговое письмо, имитирующее предупреждение от судебных приставов, от группировки RTM

С начала 2021 года арсенал группировки RTM пополнился шифровальщиком Quoter. По сообщениям исследователей, если банковский троян не смог выполнить свои задачи и собрать информацию с зараженного узла, в качестве плана Б злоумышленники запускают в сеть компании Quoter. RTM последовала примеру других операторов программ-вымогателей и в атаках руководствуется стратегией двойного вымогательства. В качестве основного способа доставки группировка по-прежнему пользуется методами социальной инженерии — отправляет жертвам фишинговые письма.

Активность этой группировки в I квартале 2021 года по сравнению с IV кварталом 2020 года снизилась, но это может свидетельствовать о том, что злоумышленники пока заняты разработкой новых техник атак или доработкой уже имеющихся инструментов.

## Суммы выкупов продолжают расти

Каждая третья атака в I квартале происходила с участием операторов программ-вымогателей. По итогам 2020 года первое место в топе часто атакуемых отраслей занимали медучреждения, а в I квартале 2021 года первое место поделили между собой промышленность и организации в сфере науки и образования. Их суммарная доля составляет 30% всех инцидентов с участием шифровальщиков. Еще 28% атак были направлены на государственные и медицинские учреждения.

Примерно в семи из десяти атак с использованием программ-вымогателей, нацеленных на организации, в качестве способа доставки вредоноса использовалась электронная почта, в четверти случаев злоумышленники прибегали к эксплуатации уязвимостей и поиску незащищенных ресурсов, доступных из интернета.

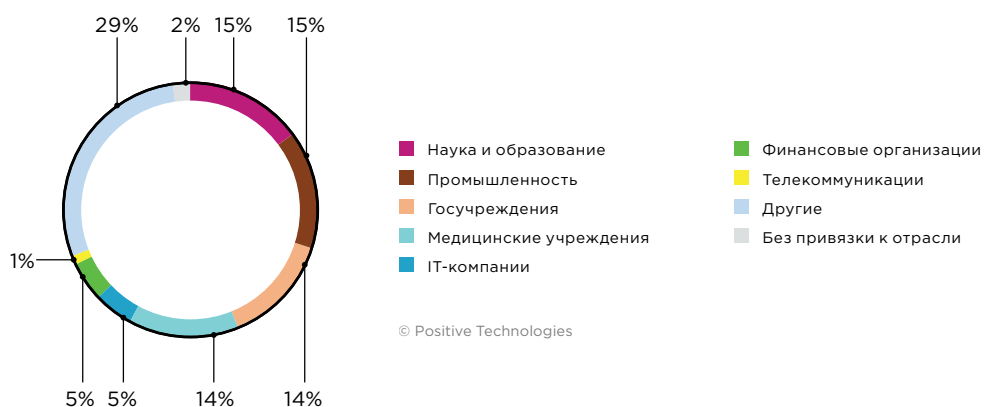


Рисунок 10. Распределение атак программ-вымогателей по отраслям

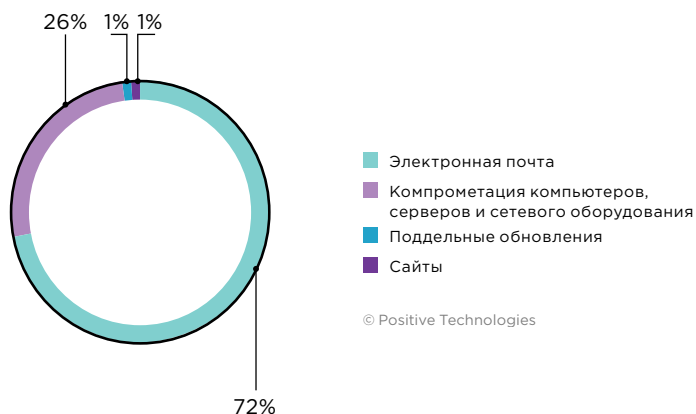


Рисунок 11. Способы распространения шифровальщиков в организациях

### Топ-5 программ-вымогателей в I квартале 2021 года

1. REvil
2. Clap
3. Conti (Ryuk)
4. Babuk Locker
5. DoppelPaymer

## Появление новых участников

В начале 2021 года появилось несколько новых программ-вымогателей: [Crimg](#), [Vovalex](#), [Babuk Locker](#), [Phoenix CryptoLocker](#), [Hog](#) и [Humble](#).

### Шифровальщик Hog

Шифровальщик Hog пока нацелен на частных лиц. Его операторы дешифруют устройства жертв только в том случае, если они присоединятся к их серверу в Discord. Использование Discord уже было ранее замечено в атаках других злоумышленников и становится частой практикой. Возможно, операторы Hog тестируют новые методы.

## Баснословные суммы выкупов

В I квартале 2021 года операторы программы-вымогателя REvil побили все рекорды по запрашиваемым суммам выкупа. Атаковав ИТ-компанию Acer они запросили выкуп в размере 50 млн долл. США, а зашифровав сеть паназиатской розничной сети Dairy Farm Group потребовали 30 млн за дешифровщик и нераспространение украденных данных. Такие суммы обусловлены тактикой «чем больше запросишь, тем больше получишь». Успешность кампании подтверждает инцидент с ретейлером FatFace. В начале января операторы шифровальщика Conti (Ryuk) в результате фишинговой атаки проникли в сеть компании, затем спустя семь дней разведки они извлекли 200 ГБ данных и запустили процесс шифрования. Изначально злоумышленники потребовали 8 млн долл. США, однако в ходе переговоров сумма была снижена до 2 млн — она устроила обе стороны.

Из-за того, что некоторые компании отказываются от уплаты выкупа, операторы программ-вымогателей вынуждены изобретать новые тактики. Теперь, если компания не собирается платить, злоумышленники угрожают ей тем, что сообщат о факте атаки и украденных данных ее клиентам. По замыслу мошенников, клиенты «угворят» компанию заплатить выкуп, чтобы не допустить разглашения своих данных.

## Возвращение старых участников

Программа-вымогатель WannaCry, прогремевшая на весь мир четыре года назад, снова в деле. По данным компании Check Point, количество пострадавших организаций в марте 2021 года относительно октября 2020 года увеличилось в 40 раз. Распространяется вредонос с помощью эксплойта EternalBlue. Чаще всего вымогатель атакует госучреждения и оборонные предприятия, на втором месте промышленность, а третье и четвертое занимают финансовые организации и медучреждения.

## Новые возможности

Программа-вымогатель REvil обзавелась новой функцией — возможностью запускать процесс шифрования в безопасном режиме Windows, благодаря этому ВПО может обойти средства защиты. Разработчики шифровальщика Conti (Ryuk) дополнили его функцией распространения на другие устройства в домене. По сети он распространяется через общие сетевые ресурсы, в которых создает свои копии, а запуск файлов обеспечивается при помощи создания задач в планировщике заданий Windows.

## Безопасное хранение украденных данных

Операторы программы-вымогателя Darkside, атаковавшие бразильскую электроэнергетическую компанию Companhia Paranaense de Energia (Copel) и похитившие у нее около терабайта конфиденциальной информации, используют собственный метод хранения данных. Они не размещают украденную информацию на специально созданных для этого закрытых сайтах, так как это небезопасно, для ее хранения они разработали распределенную базу данных: данные хранятся на разных серверах. Это позволяет избежать потери доступа к украденной информации из-за возможных блокировок.

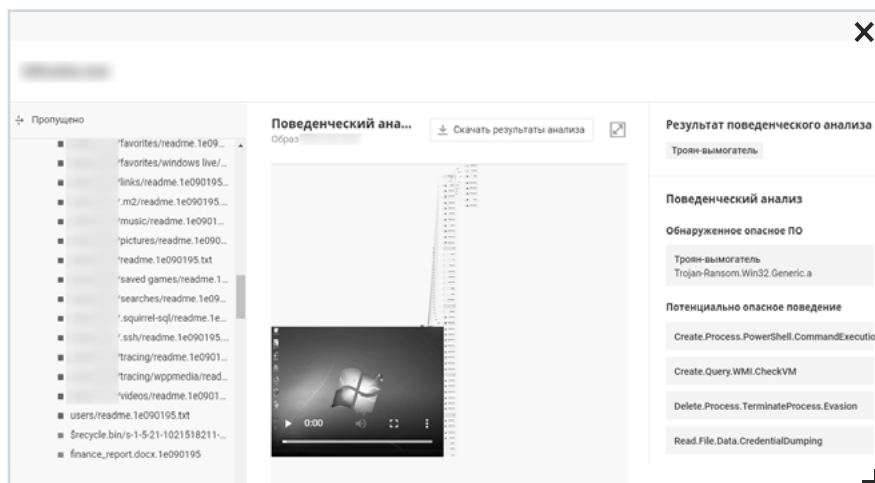


Рисунок 12. Программа-вымогатель Darkside, обнаруженная с помощью PT Sandbox

## Страх ответственности

Операторы программы-вымогателя Ziggy на волне новостей о поимке злоумышленников, распространяющих шифровальщик Netwalker, и разрушении инфраструктуры ботнета Emotet благодаря действиям правоохранительных органов, объявили об окончании своей карьеры злоумышленников и пообещали жертвам, которые заплатили им выкуп, вернуть деньги.

## Небезопасное ПО

Первый квартал 2021 года нам запомнится активной эксплуатацией уязвимостей в программном обеспечении Microsoft Exchange Server (уязвимости ProxyLogon) и Accellion FTA. Уязвимостями ProxyLogon воспользовались злоумышленники, распространяющие шифровальщик Black Kingdom и DearCry, криптомайнер Lemon\_Duck, а также APT-группировки.

Уязвимости в устаревшем программном обеспечении для передачи данных Accellion FTA эксплуатировали операторы программы-вымогателя Clor и киберпреступная группировка FIN11: жертвами стали около 100 организаций. Примерно четверть из этих организаций пострадали от серьезной утечки данных, например сингапурский мобильный оператор Singtel, юридическая фирма Jones Day, университеты в Майами и Калифорнии, Американское бюро судоходства, железнодорожный оператор CSX и авиастроительная компания Bombardier. Компания Centene, также пострадавшая из-за уязвимостей, подала на Accellion заявление в суд. В исковом заявлении изложено требование о возмещении расходов, связанных с устранением последствий атаки.

Обходить механизм защиты песочниц и выполнять произвольные команды злоумышленникам позволяет уязвимость CVE-2015-1427 в Elasticsearch. В этом квартале ее использовали операторы трех ботнетов — z0Miner, Skidmap, WatchDog. Другой ботнет, FreakOut, расширился с помощью уязвимостей в системах TerraMaster (CVE-2020-28188), Zend Framework (CVE-2021-3007) и Liferay Portal (CVE-2020-7961).

Говоря об уязвимостях, нельзя не упомянуть инцидент с производителем систем для ИБ — компанией SonicWall, которая в конце января была взломана посредством уязвимости нулевого дня в VPN-решениях NetExtender и Secure Mobile Access. Позже в СМИ начали появляться сообщения об атаках на клиентов компании, использующих уязвимые решения. Например, такой возможностью воспользовалась группировка UNC2447, распространяющая программу-вымогатель FiveHands (обновленная версия вымогателя DeathRansom) посредством загрузчика WarPrism или бэкдора SombRAT. По словам исследователей, злоумышленники эксплуатировали уязвимость еще до появления обновления безопасности. Предположительно, компания SonicWall своевременно не предупредила своих клиентов о выявленной бреши и о необходимости принять защитные меры.

## Прицел на виртуальную инфраструктуру

В IV квартале 2020 года наметилась, а в I квартале 2021 окончательно укрепилась тенденция среди злоумышленников на намеренную заточку своих вредоносов под атаки на виртуальную инфраструктуру. Прежде всего, мы можем это связать с глобальным процессом переноса ИТ-инфраструктуры компаний в виртуальную среду. Злоумышленники тщательно отслеживают информацию о новых уязвимостях и стараются как можно скорее найти им применение в своих атаках. В начале 2021 года наши специалисты помогли устранить несколько критически опасных уязвимостей в продуктах VMware, в том числе CVE-2021-21972 в vCenter Server, позволяющую удаленно выполнить код. На момент публикации, по нашей оценке, число устройств, уязвимых для CVE-2021-21972, во всем мире превышало 6000. После появления в начале февраля обновлений безопасности от вендора и публикации бюллетеня исследователи компании Bad Packets обнаружили множественные сканирования сетей с целью поиска уязвимых узлов.

Операторы вымогателей Darkside, RansomExx и Babuk Locker активно эксплуатируют другие уязвимости в продуктах компании VMware для шифрования данных, хранящихся на виртуальных жестких дисках, например уязвимости удаленного выполнения кода CVE-2019-5544 и CVE-2020-3992.

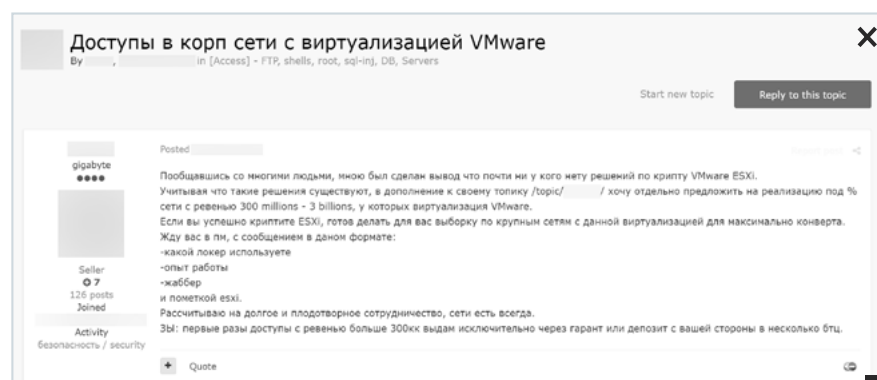


Рисунок 13. Объявление о продаже доступа к сетям, где используется VMware ESXi

Злоумышленники, распространяющие троян Hildegard, целенаправленно атакуют среду Kubernetes. Для сокрытия своего вредоноса они используют сразу несколько техник, в том числе шифруют полезную нагрузку, маскируют вредоносный процесс под процесс bioset в Linux и применяют технику Dynamic Linker Hijacking.

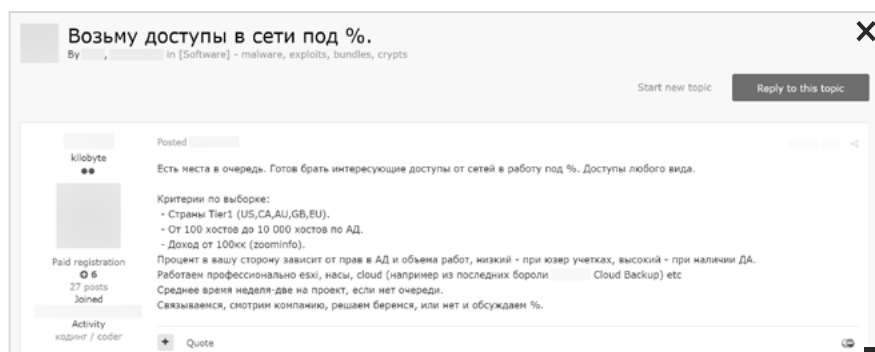


Рисунок 14. Объявление о предоставлении услуг по взлому виртуальной или облачной инфраструктуры

Получение доступа к виртуальной инфраструктуре и облачным сервисам — довольно популярная тема в дарквебе. Услугами так называемых «брокеров» пользуются и операторы программ-вымогателей, приобретая учетные данные для входа в систему. Помимо готовых доступов к определенным компаниям, на форуме в дарквебе злоумышленники размещают предложения по взлому компаний на заказ.

## Прицел на разработчиков ПО и облачные сервисы

Количество атак на ИТ-компании с начала IV квартала 2020 года не уменьшается. Основным мотивом злоумышленников, атакующих эту отрасль, остается получение данных (66%). В 27% инцидентов хакеры были нацелены на извлечение финансовой выгоды, а в 15% случаев компании взламывались для проведения последующих атак на клиентов.

Последствия атаки на компанию SolarWinds проявляются даже в начале 2021 года. Так, в начале марта в СМИ появилась новость об атаке на ИТ-компанию Robotron. Инцидент затронул и клиентов компании, установивших вредоносные обновления для сервера резервного копирования Werkzeugkasten. Расследование показало, что сеть компании была скомпрометирована в результате атаки на SolarWinds. По данным Robotron, первой жертвой, установившей вредоносные обновления, стала небольшая компания в Голландии (ни название, ни даже отрасль, в которой работает компания, не разглашаются). Под видом обновлений распространялся шифровальщик BlockKopieren.

Атаки типа supply chain не обошли стороной и компании в сфере информационной безопасности. В начале февраля о взломе своих систем сообщила французская компания StormShield. Хакеры взломали портал технической поддержки. В результате инцидента был похищен исходный код программного

межсетевого экрана Stormshield Network Security. Можно предположить, что украденный код будет исследоваться злоумышленниками для поиска уязвимостей в этом ПО. Компания [Malwarebytes](#), производящая средства защиты информации, в начале января 2021 года пострадала из-за уязвимости в приложении, имеющем привилегированный доступ к Microsoft Office 365 и Azure. К слову, в половине атак на эту отрасль злоумышленники эксплуатировали уязвимости в программном обеспечении.

К 56% атак с использованием ВПО были причастны операторы программ-вымогателей. Наиболее показательные с точки зрения последствий инциденты произошли с [американским провайдером ИТ-услуг CompuCom](#) и [канадским поставщиком IoT-решений Sierra Wireless](#). В первом случае из-за атаки шифровальщика DarkSide компания приостановила предоставление услуг некоторым клиентам. На устранение всех последствий, по оценкам компании, придется потратить до 20 млн долл. США, а ожидаемая потеря выручки составляет от 5 до 8 миллионов. Sierra Wireless, также пострадавшая от атаки программы-вымогателя, была вынуждена остановить производство, а сайт компании был недоступен в течение двух недель. Помимо этого, компании пришлось [отозвать](#) свой прогноз финансовых показателей на I квартал 2021 года, поскольку теперь его нужно корректировать.

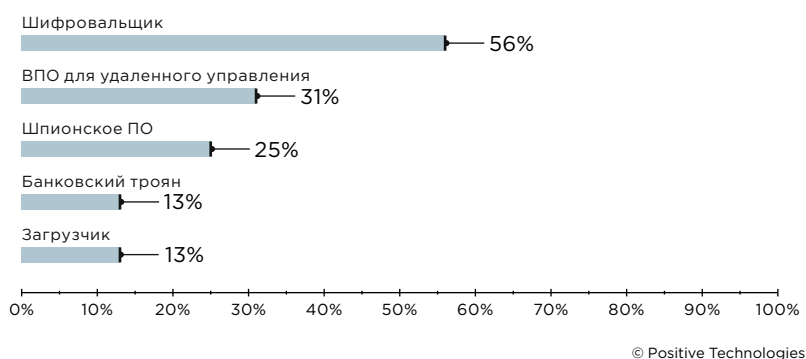


Рисунок 15. Вредоносное ПО, используемое в атаках на ИТ-компании

Доля вредоносного ПО для удаленного управления увеличилась на 23 п. п. в сравнении с IV кварталом 2020 года. В одной из кампаний злоумышленники распространяли его под видом бесплатной среды разработки приложений для экосистем Apple — Xcode. Исследователи SentinelOne обнаружили этот вредонос в легитимном проекте TabBarInteraction. Кампания ориентирована на разработчиков, которые в последующем непреднамеренно распространят вредоносное ПО для удаленного управления своим клиентам, как часть проекта. Еще одна атака, нацеленная на разработчиков ПО, заключалась во взломе [официального Git-репозитория РНР](#) и добавлении вредоносных коммитов. Примечательно, что злоумышленникам удалось подписать эти коммиты от лица известных разработчиков.

Популярные сейчас облачные сервисы, облегчающие взаимодействие и упрощающие ИТ-инфраструктуру компании, также стали излюбленными целями злоумышленников. Причина этого феномена в том, что, атаковав поставщика облачных услуг, хакеры могут получить доступ к данным его клиентов, как это случилось, например, в ходе январского инцидента с магазином одежды Bonobos. Магазин [пострадал от утечки данных](#) из-за атаки на поставщика облачного сервиса, услугами которого компания пользовалась для хранения



учетных и персональных данных клиентов. Аналогичный инцидент произошел с производителем сетевого оборудования [Ubiquiti](#).

По данным Агентства по кибербезопасности и безопасности инфраструктуры США, хакерам удалось найти [способ обхода](#) двухфакторной аутентификации для компрометации облачных сервисов. Реализовать это удалось посредством атаки pass the cookie.

## Атака pass the cookie

В ходе атаки pass the cookie злоумышленники перехватывают сессию уже аутентифицированного пользователя или используют украденные сессионные файлы cookie для аутентификации на веб-ресурсе.

## Прослушка, перехват сообщений и новости о 5G

Количество атак на телекоммуникационные компании увеличилось вдвое по сравнению с IV кварталом 2020 года.

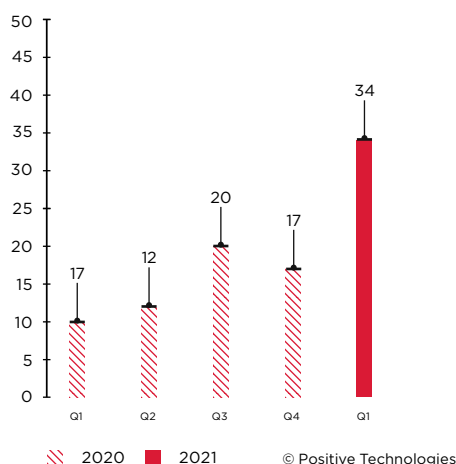


Рисунок 16. Количество атак на телекоммуникационные компании

В 71% атак злоумышленники преследовали мотив получения данных. По-настоящему интересной для хакеров оказалась тема, связанная с технологией 5G, возможно это связано с тем, что они хотят разобраться в особенностях ее реализации, чтобы впоследствии проводить атаки на абонентов. В рамках [крупной кибершпионской кампании](#) хакеры создали поддельный сайт, имитирующий официальный портал вакансий компании Huawei. При посещении данного ресурса на компьютер жертвы устанавливалось вредоносное Flash-приложение, выполняющее роль загрузчика для последующей установки Cobalt Strike Beacon. Жертвами этой кампании стали по меньшей мере 23 телекоммуникационные компании.

В начале 2021 года исследователи из ClearSky сообщили о выявленной кампании по сбору конфиденциальных данных, которую проводила киберпреступная группировка Volatile Cedar и которая началась в III квартале 2020 года и продолжается по сей день. В ходе атак злоумышленники эксплуатируют веб-уязвимости CVE 2019-3396 (Atlassian Confluence), CVE 2019-11581 (Atlassian Jira) и CVE 2012-3152 (Oracle Fusion). Жертвами этой кампании стали, к примеру, американская телекоммуникационная компания Frontier Communications, египетский оператор мобильной связи Vodafone Egypt, иорданский национальный информационно-технологический центр (National Information Technology Center), телекоммуникационные компании в Саудовской Аравии Mobily и Saudinet и другие крупные компании отрасли.

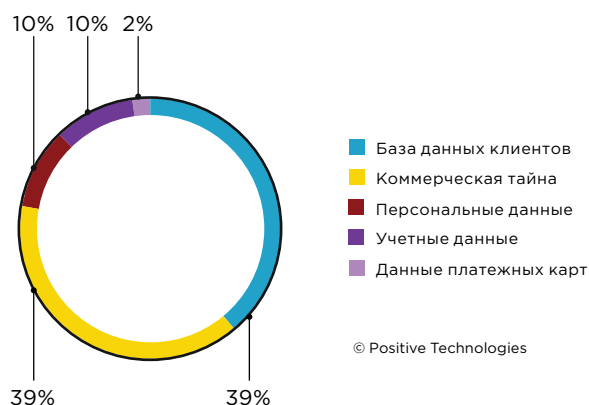


Рисунок 17. Данные, похищенные у телекоммуникационных компаний

В 91% атак использовалось вредоносное ПО. Чаще всего (55%) в инцидентах фигурировало ВПО для удаленного управления, как, например, в случае с компанией USCellular. Этот факт может свидетельствовать о том, что доступ в телекоммуникационные компании имеет высокую ценность для хакеров: его можно продать на форуме в дарквебе или использовать в дальнейших атаках на абонентов.

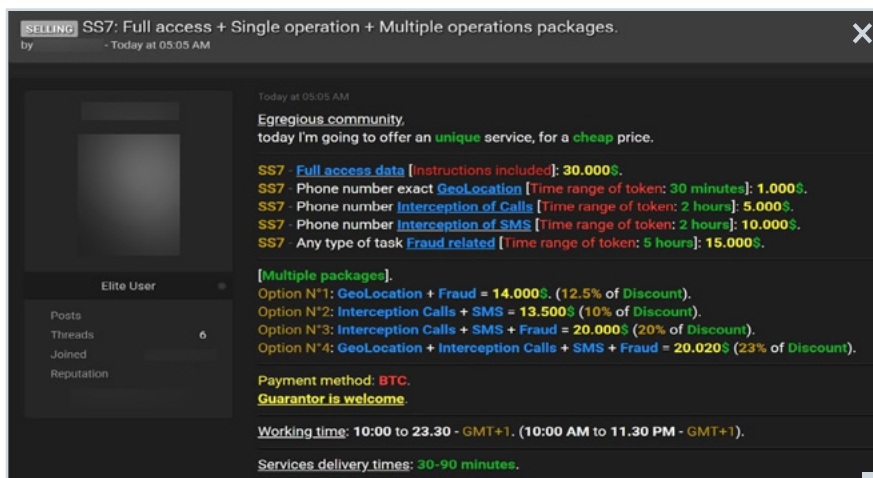


Рисунок 18. Объявление о продаже доступа к сети SS7 и услуг киберпреступников

Доступ к телекоммуникационному оборудованию может позволить злоумышленникам перехватывать звонки и сообщения абонентов, отслеживать их местоположение, проводить мошеннические операции.

## Госучреждения — самые часто атакуемые организации

С 2017 года госучреждения возглавляют наш рейтинг наиболее часто атакуемых организаций. Для своих злонамеренных действий хакеры в основном использовали вредоносное ПО (63% атак) и методы социальной инженерии (56%). На третьем месте — эксплуатация веб-уязвимостей: доля этого метода выросла на 13 п. п. в сравнении с IV кварталом 2020 года и составляет 22%. Наиболее активно злоумышленники применяли популярные в I квартале 2021 года уязвимости ProxyLogon, например в инциденте с парламентом Норвегии, и уязвимости в Accellion FTA, в результате эксплуатации которой пострадала аудиторская служба штата Вашингтон. АРТ-группировки LuckyMouse, Tick и Calypso, нацеленные на организации в США, Европе, Азии и на Ближнем Востоке, в том числе на госучреждения, были также замечены за использованием уязвимости удаленного выполнения кода CVE-2021-26855, относящейся к ProxyLogon. Целью этих кампаний было получение данных.

В атаках на госучреждения увеличивается доля операторов программ-вымогателей: они встречались в 70% атак с применением вредоносного ПО. Помимо шифровальщиков злоумышленники использовали также банковские трояны (18% атак с использованием ВПО), вредоносные программы для удаленного управления (13%) и шпионское ПО (8%).

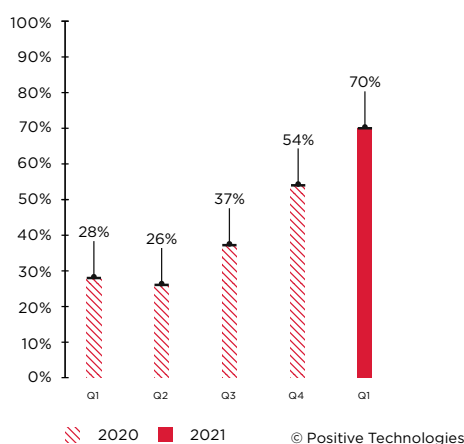


Рисунок 19. Доля атак шифровальщиков в атаках ВПО на госучреждения

В этом контексте нельзя не отметить февральскую атаку на системы умного города в Индии. Издание The Economic Times подчеркнуло, что это первая в истории атака на инфраструктуру умного города. Операторы программы-вымогателя потребовали 646 000 долл. США за устранение созданных

ими неполадок. Не менее интересный пример — атака хакерской группировки Notarus Corp, которой удалось взломать сеть Министерства экономики и финансов Эквадора и распространить свой шифровальщик Ronggolawe (AwesomeWare). Особенность этого шифровальщика в том, что он создан на PHP и шифрует файлы веб-приложений компании-жертвы. В ходе этой атаки были скомпрометированы учетные данные более 6500 пользователей, а также похищена конфиденциальная информация, в том числе электронные письма и персональные данные сотрудников.

Методы социальной инженерии применялись в 56% инцидентов. Использует их для доставки вредоноса, к примеру, APT-группировка SideWinder, деятельность которой отслеживали специалисты PT ESC. На протяжении I квартала 2021 года были зафиксированы атаки этой группировки на госучреждения в Юго-Восточной Азии. На первом шаге злоумышленники прикрепляли к фишинговому письму файл с расширением .lnk. Если пользователь открывал файл, то запускалась утилита mshta.exe, и уже с ее помощью отображался документ-заглушка для жертвы, чтобы у нее не возникло подозрений, а в это время отработывал основной скрипт, разворачивающий троян. Подобной техникой пользуются многие APT-группировки, про которые мы рассказывали во II и III кварталах 2020 года.

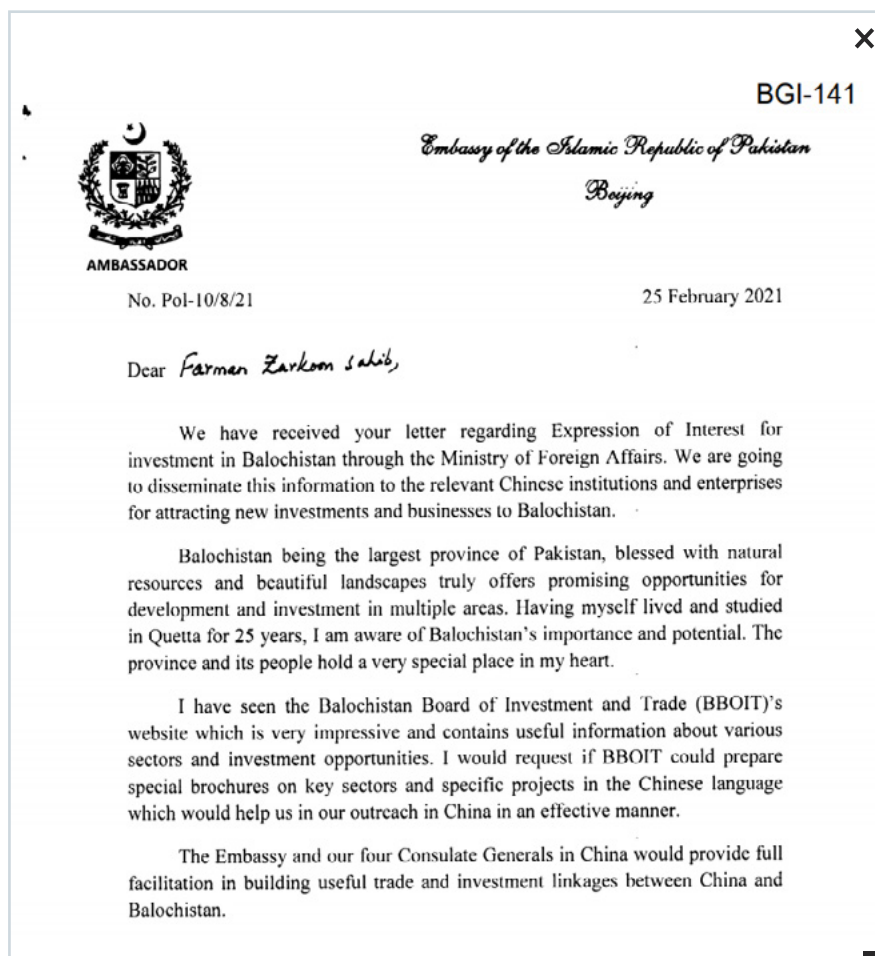


Рисунок 20. Фишинговое письмо от APT-группировки SideWinder для целенаправленной атаки на посольство Пакистана в Китае

## Об исследовании

Данный отчет содержит информацию об общемировых актуальных угрозах информационной безопасности, основанную на собственной экспертизе компании Positive Technologies, результатах расследований, а также на данных авторитетных источников.

По нашей оценке, большинство кибератак не передается огласке из-за репутационных рисков, в связи с этим подсчитать точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. Наше исследование проводится с целью обратить внимание организаций и обычных граждан, интересующихся современным состоянием информационной безопасности, на наиболее актуальные методы и мотивы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз.

В рамках отчета каждая массовая атака (в ходе которой злоумышленники проводят, например, фишинговую рассылку на множество адресов) рассматривается как одна отдельная, а не как несколько. Термины, которые мы используем в исследовании, приведены [в глоссарии на сайте Positive Technologies](#).

---

### О компании

[ptsecurity.com](https://ptsecurity.com)  
[pt@ptsecurity.com](mailto:pt@ptsecurity.com)  
[facebook.com/](https://facebook.com/PositiveTechnologies)  
[PositiveTechnologies](https://facebook.com/PHDays)  
[facebook.com/PHDays](https://facebook.com/PHDays)

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «[Новости](#)» на сайте [ptsecurity.com](https://ptsecurity.com).