# Актуальные киберугрозы

## II квартал 2021 года

ptsecurity.com

# Содержание

# Резюме

Итоги II квартала 2021 года:

- Количество атак увеличилось лишь на 0,3% в сравнении с I кварталом 2021 года. Темп роста этого показателя замедлился; подобного следовало ожидать, так как компании успели адаптироваться к работе в условиях пандемии коронавируса, в том числе приняли меры по защите сетевого периметра и систем удаленного доступа.
- Объем целенаправленных атак растет с каждым кварталом. Во II квартале 77% атак были целевыми. Доля инцидентов, в которых злоумышленники были нацелены на частных лиц, осталась такой же, как и в предыдущем квартале, — 12%.
- Атаки с использованием ВПО по-прежнему занимают первое место в арсенале киберпреступников. В сравнении с I кварталом 2021 года доля этого метода выросла на 15 процентных пунктов и составляет 73%. Мы отмечаем, что тренд на создание вредоносов, нацеленных на Unix-системы, средства виртуализации и оркестраторы, окончательно укрепился.
- Во II квартале были побиты все рекорды по количеству атак с использованием шифровальщиков: их доля составила 69% среди всех атак с использованием ВПО. Пиковый прирост произошел в апреле. Однако в начале мая злоумышленники атаковали крупнейшую трубопроводную систему США Colonial Pipeline и полицию округа Колумбия, чем привлекли внимание правоохранительных органов. В итоге киберпреступники начали менять подходы к атакам, а также вносить изменения в партнерские программы. Мы предполагаем, что в перспективе операторы шифровальщиков могут вовсе отказаться от партнеров как отдельной роли и будут сами курировать команды распространителей.
- Обладателям устройств QNAP во II квартале пришлось держать ухо востро. Эти устройства позволяют агрегировать большие объемы данных компаний и частных лиц, поэтому они представляют большую ценность для злоумышленников. В основном клиентов QNAP атаковали с помощью программ-вымогателей, к примеру AgeLocker и eCh0raix.
- Доля атак на госучреждения среди всех атак на организации резко выросла с 12%, зафиксированных в I квартале 2021 года, до 20% во II квартале. В 73% инцидентов с использованием вредоносного ПО приняли участие злоумышленники, которые распространяют шифровальщики. Новый загрузчик Tomiris был обнаружен специалистами PT ESC; вредонос обладает функциями для закрепления и может отправить зашифрованную информацию о рабочей станции на подконтрольный злоумышленникам сервер.
- Ландшафт киберугроз для торговой отрасли претерпел изменения. Во II квартале мы отметили, с одной стороны, уменьшение количества атак типа Magecart, а с другой — увеличение доли атак, в которых злоумышленники использовали программы-вымогатели. Если раньше киберпреступники преследовали мотив кражи данных, сейчас они стараются получить прямую финансовую выгоду от атак.
- Промышленная отрасль в этом квартале также особо часто страдала от рук распространителей шифровальщиков. Они были причастны к 80% инцидентов с использованием вредоносов. Участились случаи использования хакинга: доля этого метода выросла с 29% до 34%. Специалисты PT ESC выявили новое вредоносное ПО для удаленного управления B-JDUN, замеченное в атаке на энергетическую компанию.

Для защиты от кибератак мы прежде всего советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. С учетом специфики атак в этом квартале настоятельно рекомендуем вовремя устанавливать обновления безопасности. Кроме того, мы советуем проводить тщательные расследования всех крупных инцидентов, чтобы выявить точки компрометации и уязвимости, которыми воспользовались злоумышленники, а также своевременно убедиться в том, что преступники не оставили себе запасных входов. 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 атак по сравнению с I кварталом 2021 года увеличилось на 0,3%. Доля атак, направленных на компрометацию компьютеров, серверов и сетевого оборудования, выросла с 71% до 87%, что связано с ростом количества атак с использованием программ-вымогателей. Увеличилась и доля атак, мотивом которых являлось получение финансовой выгоды (с 43% до 59%). Чаще всего злоумышленники атаковали медицинские и государственные учреждения и промышленную отрасль.

В атаках на частных лиц злоумышленники чаще руководствовались мотивом получения данных. Его доля в сравнении с I кварталом 2021 года выросла на 9 п. п. и составляет 78%, при этом более чем в два раза увеличился объем похищенных платежных данных.

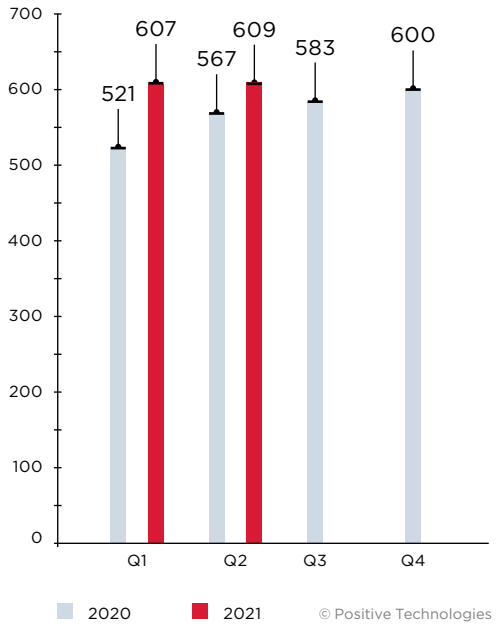


*Рисунок 1. Количество атак в 2020 и 2021 годах (по кварталам)*

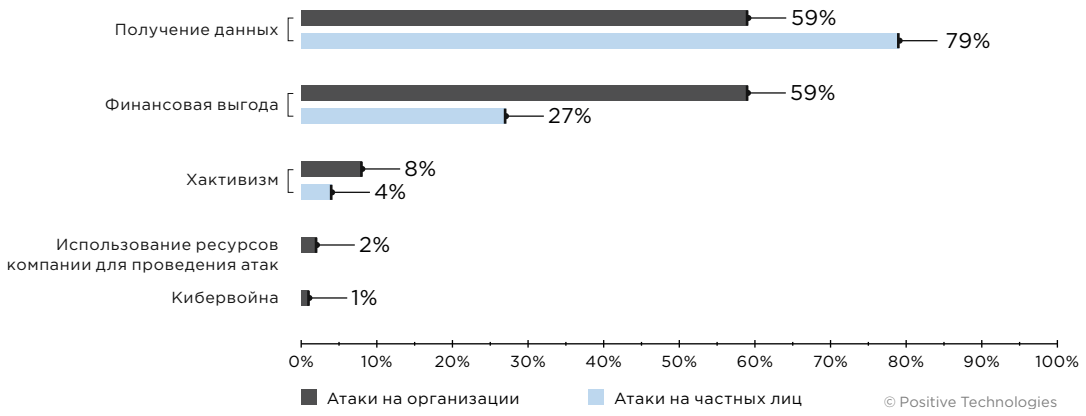


*Рисунок 2. Мотивы злоумышленников (доля атак)*

## *77% атак носили целенаправленный характер*

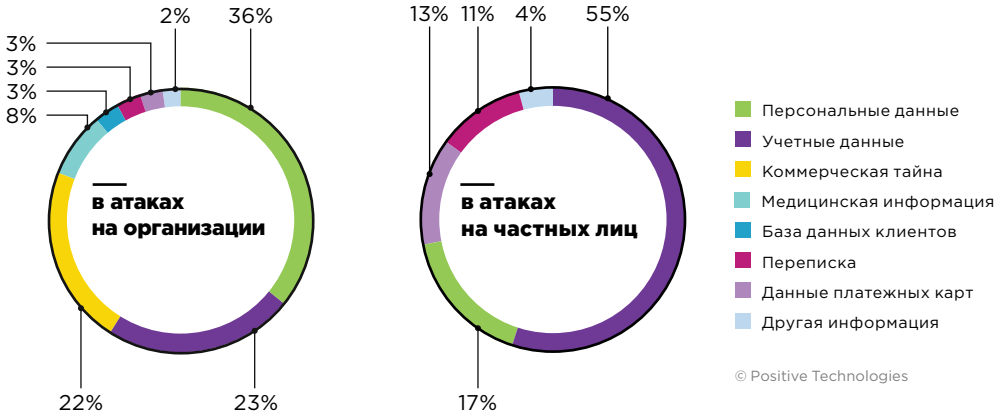


*Рисунок 3. Типы украденных данных*

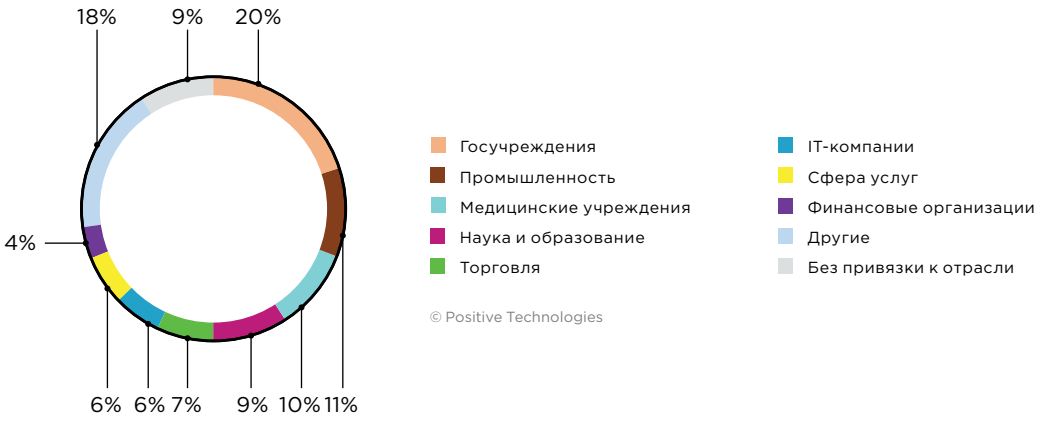


*Рисунок 4. Категории жертв среди организаций*

## *12% атак направлены против частных лиц*

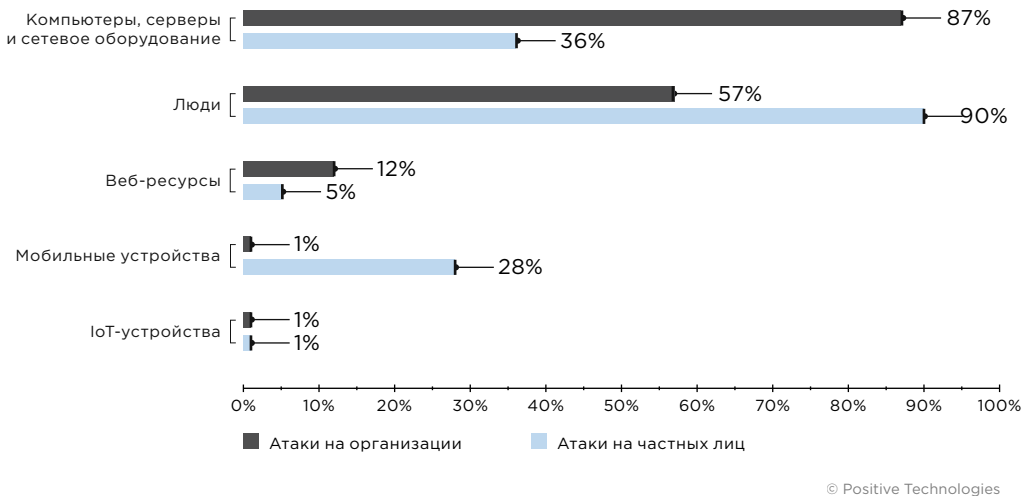


*Рисунок 5. Объекты атак (доля атак)*

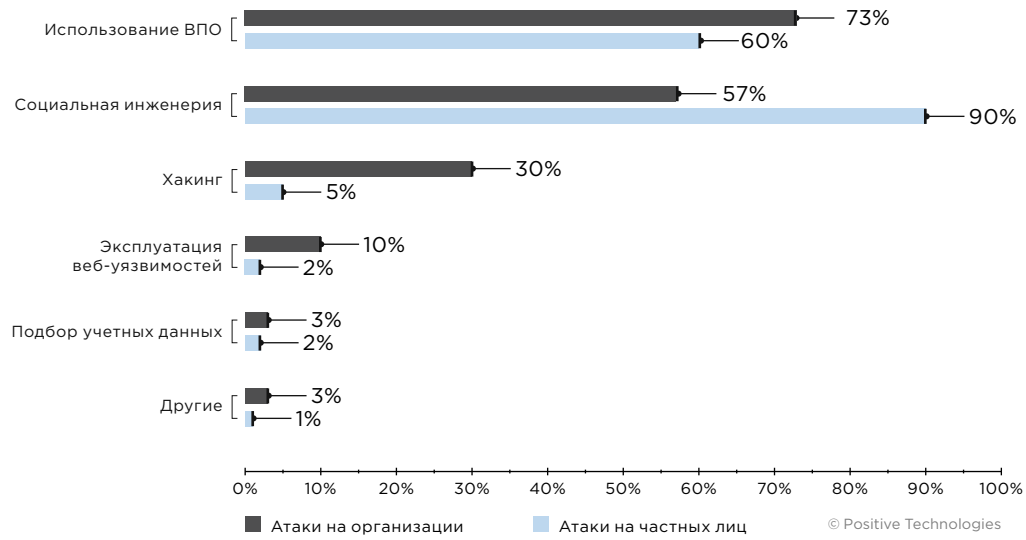


*Рисунок 6. Методы атак (доля атак)*

**Категории жертв**

| | Распределение кибериндидентов по метрикам (мотивы, методы, объекты атак) и внутри отраслей | Госучреждения | Финансовые организации | Промышленность | Медицинские учреждения | IT-компании | Наука и образование | Торговля | Сфера услуг | Другие | Без привязки к отрасли | Частные лица |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Всего атак** | **102** | **23** | **56** | **50** | **32** | **47** | **34** | **29** | **94** | **48** | **94** |
| **Объект** | Компьютеры, серверы и сетевое оборудование | 88 | 20 | 49 | 45 | 32 | 45 | 26 | 26 | 81 | 39 | 35 |
| | Веб-ресурсы | 19 | 1 | 2 | 3 | 2 | 3 | 7 | 4 | 16 | 5 | 5 |
| | Люди | 60 | 15 | 33 | 34 | 8 | 34 | 18 | 17 | 54 | 19 | 85 |
| | Мобильные устройства | 2 | | | | | | | | 1 | | 26 |
| | IoT-устройства | | | | | | | | | | 3 | 1 |
| **Метод** | Использование ВПО | 78 | 15 | 41 | 37 | 20 | 38 | 20 | 21 | 71 | 37 | 56 |
| | Социальная инженерия | 60 | 15 | 33 | 34 | 8 | 34 | 18 | 17 | 54 | 19 | 85 |
| | Подбор учетных данных | 4 | 1 | 2 | | 1 | 1 | | 2 | 4 | 2 | 2 |
| | Хакинг | 24 | 4 | 19 | 13 | 21 | 10 | 9 | 8 | 23 | 24 | 5 |
| | Эксплуатация веб-уязвимостей | 15 | 1 | 1 | 3 | | 3 | 7 | 4 | 14 | 5 | 2 |
| | Другие | 4 | 3 | 1 | | 1 | | | | 4 | 1 | 1 |
| **Мотив** | Получение данных | 56 | 14 | 33 | 35 | 18 | 20 | 18 | 20 | 61 | 29 | 74 |
| | Финансовая выгода | 60 | 11 | 38 | 34 | 16 | 32 | 21 | 17 | 54 | 23 | 26 |
| | Хактивизм | 8 | 4 | 6 | 2 | 1 | 5 | 4 | 2 | 7 | | 4 |
| | Кибервойна | 1 | | 1 | | | 1 | | | | | |
| | Использование ресурсов компании для проведения атак | | | 1 | | 3 | | | 1 | 2 | 6 | |
| | Неизвестен | | | | | 1 | | | | | | |

Градацией цвета показаны доли атак внутри одной метрики для каждой категории жертв.

0% 10% 20% 30% 40% 100%

# Вредоносное ПО с прицелом на средства виртуализации

Доля атак с использованием ВПО и направленных на организации в сравнении с I кварталом 2021 года увеличилась на 15 п. п. и составляет 73%. Лидирующую позицию среди ВПО, применяемого в атаках на организации, по-прежнему занимают программы-вымогатели. К слову, доля атак с использованием таких программ за квартал выросла с 63% до 69%. В сравнении с I кварталом более чем в два раза увеличилась доля атак с использованием загрузчиков.

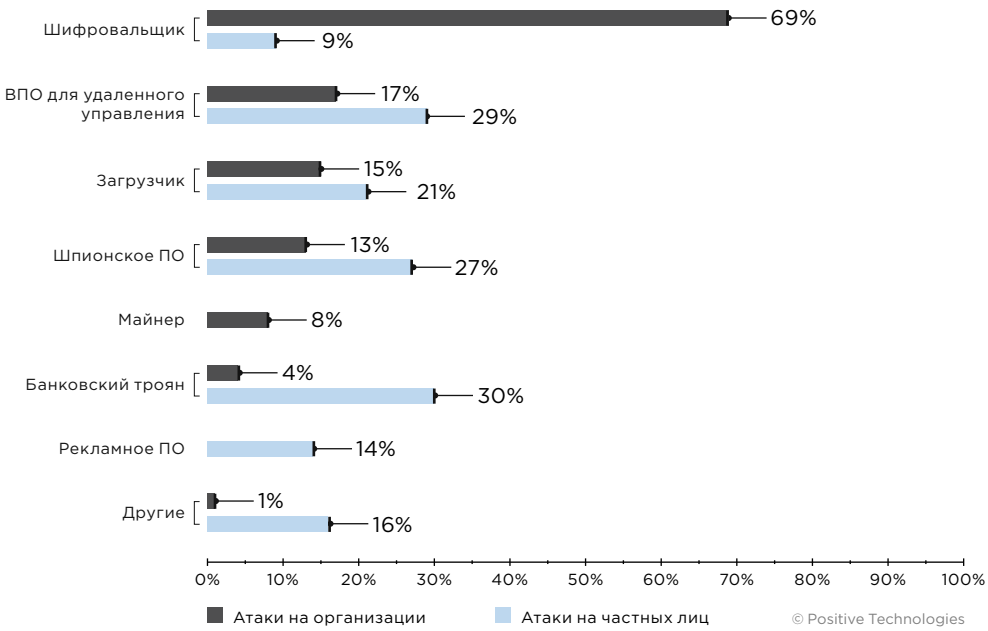


*Рисунок 7. Типы вредоносного ПО (доля атак с использованием ВПО)*

Основным способом распространения вредоносов в атаках на организации (58%) остается электронная почта. При этом доля использования сайтов для распространения ВПО в организациях выросла с 2% до 8%. К примеру, этим способом воспользовались злоумышленники, распространяющие шпионское ПО, нацеленное на программистов, которые работают с Node.js. Вредонос имитировал компонент Browserify в реестре npm.

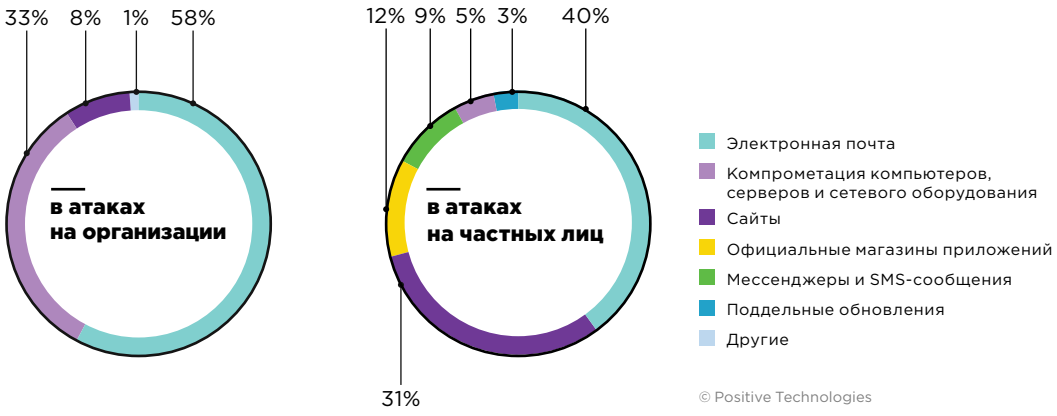


*Рисунок 8. Способы распространения вредоносного ПО (доли атак с использованием ВПО)*

## Ориентация на Unix-системы и средства виртуализации

Раньше многие считали, что злоумышленники, распространяющие ВПО, — проблема систем на базе Windows. Сейчас мы видим, что тренд на создание вредоносов для атак на Unix-системы, средства виртуализации и оркестраторы окончательно закрепился.

В I квартале этого года мы уже рассказывали о том, что многие злоумышленники нацелились на виртуальную инфраструктуру. Во II квартале к ним присоединилось множество операторов программ-вымогателей. К атакам на виртуальную инфраструктуру на базе VMware ESXi приготовились REvil, RansomExx (Defray), Mespinoza, GoGoogle, DarkSide, Hellokitty и Babuk Locker.

Исследователи компании Trend Micro проанализировали новый шифровальщик DarkRadiation, находящийся в стадии разработки, и выявили, что он заточен для атак на Red Hat, CentOS и Debian Linux. Сам вредонос представляет собой bash-скрипт, который может остановить или отключить все запущенные Docker-контейнеры. В качестве способа распространения этого шифровальщика злоумышленники используют скомпрометированные учетные записи и протокол SSH.

Помимо этого, на Unix-системы ориентированы злоумышленники, распространяющие:

- майнер Sysrv и ботнет-майнер, которые в своих атаках злоупотребляли легитимными DevOps-инструментами (Ansible, Chef, SaltStack);
- бэкдор RotaJakiro, который остается незаметным для антивирусных механизмов;
- бэкдор Facefish вкупе с руткитом, которые используются для доступа к интерфейсу управления веб-хостингом Control Web Panel на базе Linux;
- мультиплатформенное ВПО FreakOut, в том числе руткит в пользовательском режиме, нацеленное на виртуальные серверы VMware vCenter на базе Windows и Linux. FreakOut содержит функции, позволяющие запускать DDoS-атаки на мощностях жертв, загружать другие вредоносы, в том числе майнеры, а также перехватывать сетевой трафик.

В этом контексте нельзя не упомянуть и злоумышленников, распространяющих вредоносное ПО для удаленного управления Siloscape. Объектом атаки выступает контейнер с Windows. Но глобальная цель преступников — компрометация не отдельных контейнеров, а целых кластеров Kubernetes для проведения последующих атак на их пользователей, к примеру атак supply chain.

## Как усложнить жизнь разработчикам

Во II квартале был раскрыт интересный инцидент с участием злоумышленников, распространяющих майнеры. Преступники злоупотребляли бесплатным доступом к сервисам для организации непрерывной интеграции GitHub, Microsoft Azure, LayerCI, TravisCI, Sourcehut, CloudBees CodeShip и CircleCI, используя их вычислительные мощности для размещения и запуска майнеров. Таким образом на протяжении пробного периода доступа к сервисам генерировалась криптовалюта.

Как только об этой схеме узнали IT-компании, они ввели дополнительные ограничения, требуя предоставить данные платежной карты на этапе регистрации или вовсе убрав возможность бесплатного доступа к своим сервисам.

## Громкие возвращения

Ботнет TrickBot возвращается с новым шифровальщиком Diavol. Его разработчики использовали асимметричные алгоритмы шифрования, а исходный код был сокрыт в растровых изображениях.

Финансово мотивированная APT-группировка FIN7, прославившаяся своим ВПО Carbanak, также вернулась с обновленной версией загрузчика Tirion — Lizar. Распространяется новый вредонос под видом инструмента для проведения анализа безопасности. Жертвами новой вредоносной кампании стали несколько учебных учреждений, игорное заведение, фармацевтические компании в США, IT-компания со штаб-квартирой в Германии и финансовое учреждение в Панаме. Lizar содержит множество функций, направленных на сбор информации о зараженной системе, запуск различных плагинов, в том числе для сбора учетных данных, а также на загрузку дополнительного ПО, к примеру Mimikatz и бэкдора Carbanak. Модульная структура вредоноса позволяет злоумышленникам легко добавлять новые плагины.

## Атаки на частных лиц

В 60% атак на частных лиц мы отметили факт использования вредоносного ПО. Чаще всего злоумышленники распространяли банковские трояны (доля среди прочего ВПО составила 30%), вредоносы для удаленного управления (29%) и шпионское ПО (27%). Доля атак с использованием программ-шифровальщиков составляет лишь 9% среди прочего ВПО. Пример атаки шифровальщиков на частных лиц — распространение программ-вымогателей NitroRansomware. Злоумышленники распространяют это ВПО под видом инструмента, позволяющего генерировать бесплатные подарочные коды Nitro — надстройки в Discord. После запуска вредонос собирает данные из браузера, а затем шифрует файлы в системе жертвы. Для того чтобы получить дешифровщик, пострадавшему требуется приобрести подарочный код для активации Nitro и передать его злоумышленникам.

# Трансформации шифровальщиков

Во II квартале 2021 года в семи из десяти атак с использованием вредоносного ПО приняли участие злоумышленники, распространяющие программы-вымогатели. Этот показатель вырос на 30 п. п. в сравнении со II кварталом 2020 года (тогда их доля составляла лишь 39%). Чаще всего эти киберпреступники атаковали государственные и медицинские организации, промышленность и учреждения науки и образования.

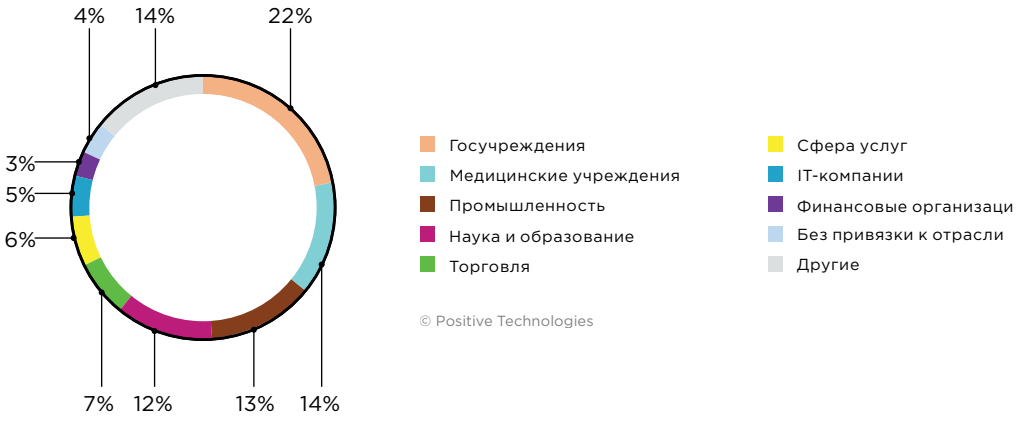


*Рисунок 9. Распределение атак программ-вымогателей по отраслям*

***Самые популярные программы-вымогатели во II квартале 2021 года***

- REvil
- Avaddon (в июне заявили о своем уходе)
- DoppelPaymer
- PayOfGrief[1]
- Conti (Ryuk)

## Трансформации операторов программ-вымогателей

В апреле мы зафиксировали рекордные показатели по количеству атак с использованием программ-вымогателей: они были причастны к 45% атак, выявленных в этом месяце. Взрывной рост числа атак вымогателей в начале II квартала отметили и исследователи компании BlackFog.

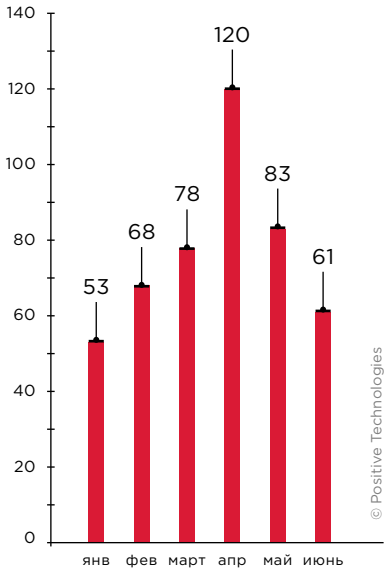


*Рисунок 10. Количество атак с использованием программ-вымогателей (по месяцам)*

Кульминацией «разгула» операторов программ-вымогателей стала атака на крупнейшую трубопроводную систему США Colonial Pipeline, которая произошла в начале мая. Ответственность за этот инцидент взяли на себя распространители шифровальщика DarkSide. В результате сеть компании была зашифрована, а преступники стали обладателями большого массива данных. Colonial Pipeline была вынуждена приостановить работу топливопровода. Спустя два дня после атаки власти объявили чрезвычайное положение в 17 штатах и округе Колумбия. За дешифровщик злоумышленники запросили 4,4 млн долл. США.

Правоохранительные органы быстро среагировали, и операторы DarkSide в считанные дни потеряли доступ к своим серверам. Преступникам ничего не оставалось, кроме как выпустить заявление о прекращении своей деятельности. К слову, их примеру последовали и другие операторы. Вследствие массового ухода с рынка бум атак с использованием программ-вымогателей, который мы наблюдали в апреле, начал постепенно стихать.

1 В июле исследователи пришли к выводу, что DoppelPaymer продолжают свою деятельность под названием PayOfGrief.

Еще один инцидент, привлекший особое внимание правоохранительных органов, — атака «дистрибьюторов» Babuk Locker на полицию округа Колумбия. К слову, операторы программы-вымогателя Babuk Locker после этого инцидента изменили свой подход к атакам. Новая методика называется PayLoad Bin; ее суть заключается в краже данных без шифрования инфраструктуры сети жертвы с последующим требованием выкупа за неразглашение украденной информации. Операторы программ-вымогателей сослались на то, что им стало трудно контролировать атаки злоумышленников, использующих их вредоносы, и из-за этого жертв атакуют по второму кругу, а предоставляемые инструменты для восстановления данных не работают. С подобными проблемами уже столкнулись операторы программ-вымогателей Conti, LockBit, Black Kingdom, REvil (Sodinokibi). После такого «пиара» сложно требовать высокие выкупы и заявлять о своей «безукоризненной репутации».

Все эти инциденты сказались на активности операторов и распространителей шифровальщиков. Уже в июне количество атак с их участием уменьшилось в два раза. А некоторые из них даже внесли изменения в свои партнерские программы, добавив ограничения на отрасль атакуемого предприятия; например, так сделали операторы REvil.

На форумах в дарквебе мы также видим споры на тему бизнеса операторов программ-вымогателей в целом. Некоторые участники форумов считают, что вымогателям необходимо прекратить свою текущую деятельность и найти другой способ зарабатывать деньги.

> На наш взгляд, наделавшие шума операторы программ-вымогателей не смогут бросить такой прибыльный бизнес и в ближайшее время лишь залягут на дно, чтобы шумиха вокруг них улеглась и они смогли разработать новую концепцию.

На форумах в дарквебе относительно недавно появился запрет на публикацию постов на тему партнерских программ операторов шифровальщиков. Этот шаг также немного усложнил жизнь операторов, поэтому мы полагаем, что в скором времени структура бизнеса операторов программ-вымогателей может измениться.

> Одним из сценариев подобных изменений может быть исчезновение так называемых партнеров как отдельной роли, а их задачи возьмут на себя сами операторы программ-вымогателей.

Таким образом, операторы будут собирать команды распространителей и курировать их напрямую, а не через посредника-партнера и активнее привлекать добытчиков доступов в свои цепочки атак.

## Клиенты на рынке доступов

Все чаще мы слышим о том, что высококвалифицированные злоумышленники редко самостоятельно добывают первоначальный доступ в сети компаний-жертв, предпочитая приобретать его на специализированных форумах в дарквебе. К примеру, исследователь фирмы CyberCX обнаружил, что злоумышленники, распространяющие шифровальщик Avaddon, очень часто прибегают к помощи «добытчиков» доступов. Этим же способом пользуются и распространители шифровальщика DarkSide, атаковавшие компанию Brenntag.

В нашем исследовании на тему теневого рынка доступов мы отмечали, что подобное развитие рынка доступов вносит коррективы в классический подход к построению модели нарушителя. Внешний нарушитель, который получает первоначальный доступ к сети компании, и нарушитель, который развивает атаку внутри, — совершенно разные по уровню подготовки. Другими словами, теперь нельзя отбрасывать высококвалифицированных и мотивированных злоумышленников по принципу «наша компания им не интересна».

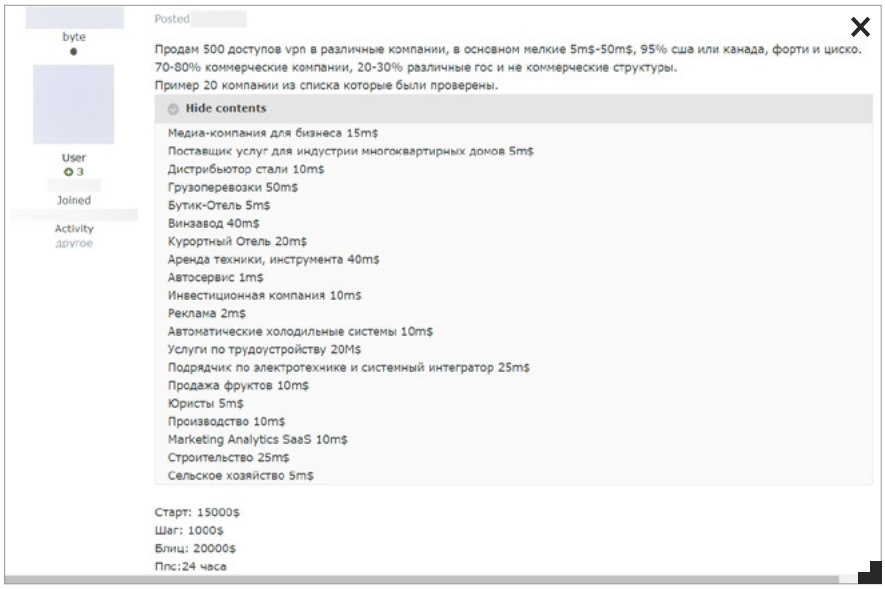


*Рисунок 11. Объявление в дарквебе о продаже доступов к различным компаниям*

## Атаки по второму кругу

По данным исследования компании Cybereason, 80% организаций, заплативших выкуп операторам программ-вымогателей, были атакованы повторно; 46% атакованных повторно считают, что пострадали от рук тех же киберпреступников, что и в первый раз. В целом если шифровальщикам удалось нанести значительный ущерб IT-инфраструктуре компании-жертвы, это означает, что в системе защиты компании есть существенные недостатки. Напоминаем, что важно провести тщательное расследование инцидента, чтобы выявить точки проникновения и уязвимости, которыми воспользовались злоумышленники, а также убедиться, что у них не осталось запасных путей для возвращения.

Однако даже если вас не атакуют во второй раз, нет гарантий, что вы восстановите утерянную в ходе атаки информацию. Так, 46% респондентов сообщили о том, что после уплаты выкупа и применения дешифровщика информацию восстановить не удалось.

## Громкое появление

Во втором квартале появилось множество новых участников рынка шифровальщиков, которые очень быстро набрали обороты. Например, операторы программы-вымогателя Lorenz, Epsilon Red, PayOrGrief, Prometheus и Xing Team. Каждый из них примечателен по-своему. К примеру, злоумышленники, распространяющие шифровальщик Lorenz, вместе с украденными данными продают и доступ во внутреннюю сеть компании-жертвы. Киберпреступники, распространяющие программу-вымогатель PayOrGrief, предупреждают, что не готовы участвовать в переговорах и снижать запрашиваемую сумму выкупа. «Дистрибьюторы» вредоноса Epsilon Red в своих атаках в качестве первоначального вектора доступа активно эксплуатируют уязвимости на серверах Microsoft Exchange. Одна из жертв, чье название не раскрывается, уже выплатила распространителям Epsilon Red около 210 000 долл. США.

# Резервные копии в опасности

Во II квартале 2021 года мы заметили большое количество атак на сетевые накопители QNAP. Эти устройства агрегируют большие объемы данных компаний и частных лиц, поэтому они представляют большую ценность для злоумышленников. В основном устройства компании QNAP подвергались атакам со стороны киберпреступников, распространяющих программы-вымогатели, например AgeLocker и eCh0raix.

Операторы шифровальщика Qlocker в ходе одной из своих кампаний вместо привычного своего шифровальщика использовали архиватор 7-Zip. Кампания была ориентирована на малый и средний бизнес, использующий в своей инфраструктуре устройства QNAP, поэтому в среднем они запрашивали у жертв выкуп в размере 557 долл. США — сумму, которую жертва точно сможет заплатить. По итогу за пять дней злоумышленники заработали 260 000 долл. США. Распространяются эти вымогатели посредством эксплуатации уязвимостей CVE-2020-2509, CVE-2020-36195 и CVE-2021-28799, позволяющих удаленно запустить встроенную утилиту для архивирования 7-Zip.

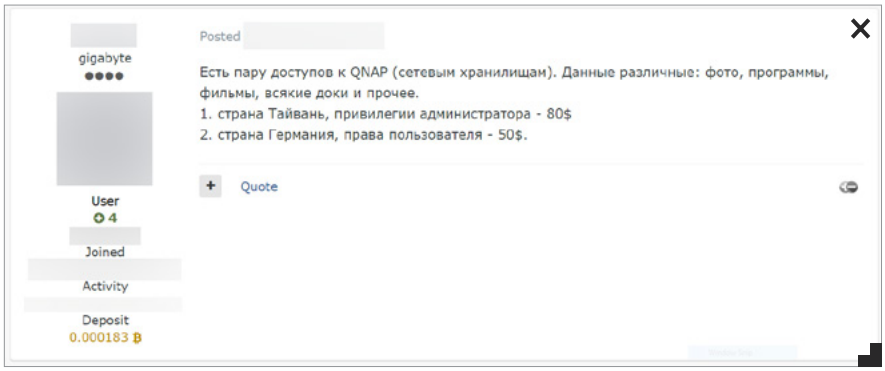


*Рисунок 12. Объявление о продаже доступа к устройствам QNAP*

Если в вашей инфраструктуре есть сетевой накопитель QNAP NAS и ПО для резервного копирования Hybrid Backup Sync, мы рекомендуем обновить версию Hybrid Backup Sync и установить обновления безопасности для QNAP NAS. В случае если вы обладатель QNAP NAS с Roon Server версии 2021-02-01 или ниже, настоятельно рекомендуем отключить сервер и использовать NAS только в локальной сети без доступа в интернет. Помимо этого, следует придерживаться общих рекомендаций: не использовать номера портов по умолчанию, ограничить количество попыток ввода учетных данных для подключения к устройствам, а также использовать надежные пароли, соответствующие современным парольным политикам.

# Проверьте обновления

В целом злоумышленники продолжают эксплуатировать и уязвимости в программном обеспечении Microsoft Exchange Server (уязвимости ProxyLogon), о которых более подробно мы рассказывали в исследовании за I квартал 2021 года. В новом квартале таким образом злоумышленники распространяют, например, вредоносное ПО для удаленного управления Turian и Lemon_Duck, шифровальщик Epsilon Red и майнер Monero.

Если вы до сих пор думаете, что установку обновлений безопасности можно отложить, аргументируя это тем, что злоумышленники не бросятся атаковать сразу же, мы готовы вам доказать обратное. Двадцать четвертого июня 2021 года исследователи из команды PT SWARM опубликовали эксплойт для уязвимости CVE-2020-3580 в Cisco ASA, и буквально в этот же день исследователи Tenable сообщили о том, что злоумышленники начали активно использовать эту информацию для проведения атак. Стоить отдельно отметить, что уязвимость была выявлена еще за год до этого, в июне 2020 года, а первое обновление безопасности компания Cisco выпустила в октябре 2020 года. Это уязвимость среднего уровня риска, однако злоумышленники сразу начали использовать эксплойт для нее в своих атаках. Из этого мы можем сделать вывод, что эксплойты для более серьезных уязвимостей так же быстро войдут в оборот, стоит им появиться, поэтому не следует откладывать установку обновлений безопасности на потом.

# Волна атак на госучреждения

В сравнении с I кварталом 2021 года доля атак на госучреждения среди всех атак, нацеленных на организации, выросла с 12% до 20%. Чаще всего злоумышленники применяют вредоносное ПО: доля этого метода по сравнению с предыдущим кварталом увеличилась с 63% до 76%.

В основном атаки совершались с использованием программ-вымогателей: их доля среди прочего ВПО составила 73%. Чаще всего это были атаки Avaddon, DoppelPaymer (PayOrGrief). На втором по популярности месте находится ВПО для удаленного управления, которое применялось в 16% атак с использованием вредоносных программ. Например, APT-группировка BackdoorDiplomacy, использующая одноименное кроссплатформенное вредоносное ПО для удаленного управления, была замечена в атаках на министерства иностранных дел во многих африканских странах, на Ближнем Востоке, в Европе и Азии. В качестве первоначального вектора атаки они использовали уязвимости на сетевом периметре компаний, в том числе CVE-2020-5902 в F5 BIG-IP и ProxyLogon.

В мае в рамках исследования угроз сотрудники PT ESC обнаружили исполняемый файл с названием «Список разрешенных направлений для посещения во время ежегодных отпусков» с расширением .exe. В ходе анализа оказалось, что данный файл представляет собой загрузчик, написанный на языке Golang. Он обладает функциями для закрепления и может отправить зашифрованную информацию о рабочей станции на подконтрольный злоумышленникам сервер. В ответе от сервера ожидается файл, который будет запущен загрузчиком. Вредоносу было присвоено имя Tomiris по названию функций в коде. Примечательно, что один из вариантов загрузчика распространялся с IP-адреса, где располагались правительственные домены одной из стран СНГ.

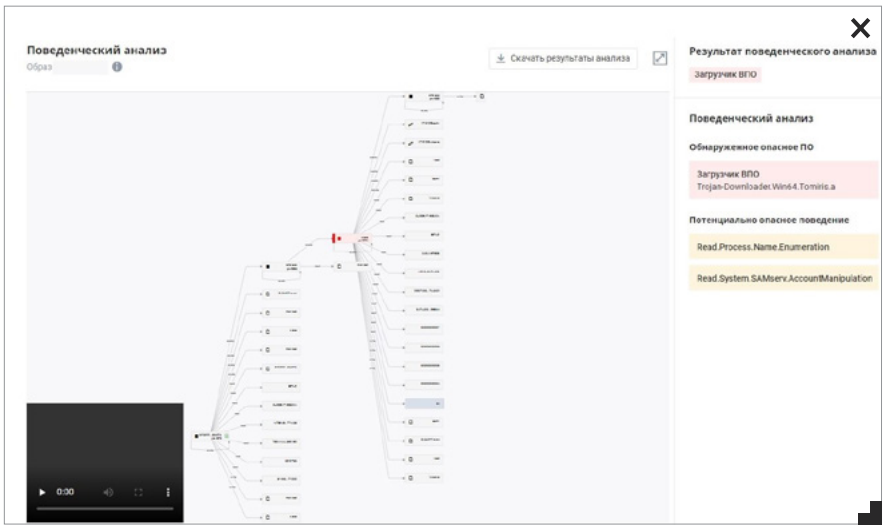


*Рисунок 13. Обнаружение Tomiris с помощью PT Sandbox*

# Новый ландшафт киберугроз для ретейла

Ландшафт киберугроз для торговли за год претерпел множество изменений. К примеру, мы отметили снижение количества атак типа Magecart. Возможно, это связано с повышенным интересом злоумышленников, распространяющих шифровальщики, к торговой отрасли: в шести из десяти атак было выявлено именно это вредоносное ПО. Наиболее часто встречались операторы REvil, DarkSide и ALTDOS.

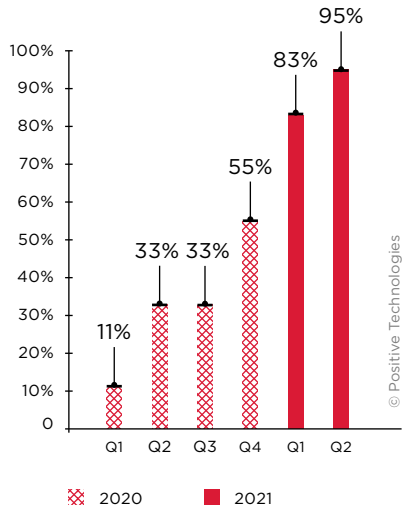


*Рисунок 14. Доля атак с использованием вымогателей среди атак с использованием ВПО*

Ранее основной целью злоумышленников, атакующих торговые компании, являлась кража данных — платежных реквизитов, персональных и учетных данных клиентов. Однако сейчас, с увеличением числа атак вымогателей, преступники все чаще преследуют прямую финансовую выгоду, рассчитывая получить крупный выкуп.

Во II квартале 2020 года доля атак с использованием ВПО среди прочих методов атак составляла лишь 26%. Аналогичный показатель в таком же периоде в 2021 году составляет уже 59%. Доля социальной инженерии также выросла с 36% в I квартале 2021 года до 53% во II квартале.

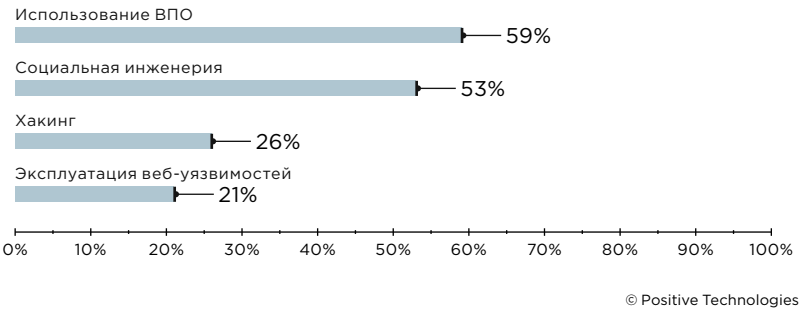


*Рисунок 15. Методы атак на торговую отрасль*

Во II квартале 21% атак были совершены с помощью эксплуатации веб-уязвимостей, например массовые атаки на компании, использующие на своих сайтах электронной коммерции плагин Fancy Product Designer. Киберпреступники воспользовались уязвимостью нулевого дня, позволяющей в обход процедуры аутентификации загрузить и выполнить произвольный код (CVE-2021-24370), и получили полный доступ к сайтам электронной коммерции различных компаний. Цель злоумышленников — извлечь информацию о заказах клиентов, в том числе их персональные данные. Если вы используете плагин Fancy Product Designer, мы настоятельно рекомендуем обновить его до версии 4.6.9.

# Угрозы для промышленности

Промышленность занимает второе место среди прочих отраслей по количеству атак. Относительно 2020 года мы наблюдаем увеличение доли хакинга с 29% до 34% во II квартале 2021 года. Доля атак с использованием ВПО выросла на 6 п. п. в сравнении с I кварталом 2021 года и составляет 73%.

Восемь из десяти атак с применением вредоносов были совершены злоумышленниками, распространяющими шифровальщики. Чаще всего в атаках на промышленную отрасль фигурировали шифровальщики REvil и DarkSide. Наиболее громкие случаи с их участием произошли с производителем продуктов питания JBS Foods, крупнейшей трубопроводной системой США Colonial Pipeline, европейскими дочерними компаниями Toshiba, дистрибьютором химических ингредиентов Brenntag, а также одним из поставщиков Apple, в результате атаки на которого были похищены чертежи новых продуктов. В ходе атаки на Brenntag злоумышленники, распространяющие DarkSide, похитили 150 ГБ данных; компания заплатила выкуп в размере 4,4 млн долл. США. В компании JBS Foods тоже приняли решение заплатить (в их случае — операторам REvil) выкуп в размере 11 млн долл. США.

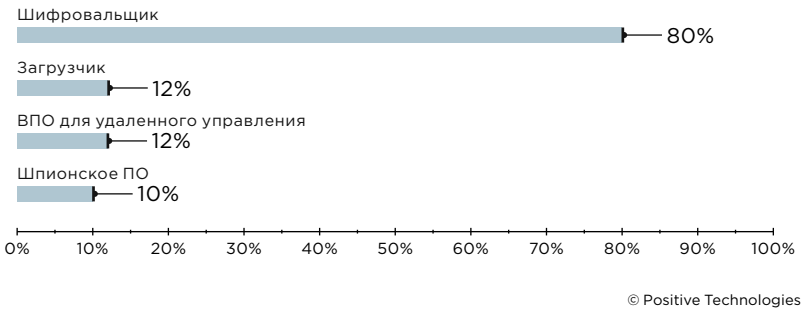


*Рисунок 16. Основные типы ВПО в атаках на промышленную отрасль (доля атак с использование ВПО)*

Во II квартале специалисты PT ESC выявили новое вредоносное ПО для удаленного управления B-JDUN, используемое в атаке на энергетические компании. Особенность этого бэкдора заключается в том, что он ждет от управляющего сервера специальный идентификатор, для того чтобы начать взаимодействие с ним и выполнять команды. Значение идентификатора задано в исходном коде ВПО. Если идентификатор, отправленный сервером, не совпадает, то вредонос прерывает соединение. Атака начиналась с отправки жертвам письма по электронной почте, к которому был прикреплен документ, содержащий эксплойт для уязвимости удаленного выполнения кода в Microsoft Office (CVE-2018-0798). Для генерации этого документа злоумышленники использовали сборщик Royal Road, который популярен у китайских группировок.

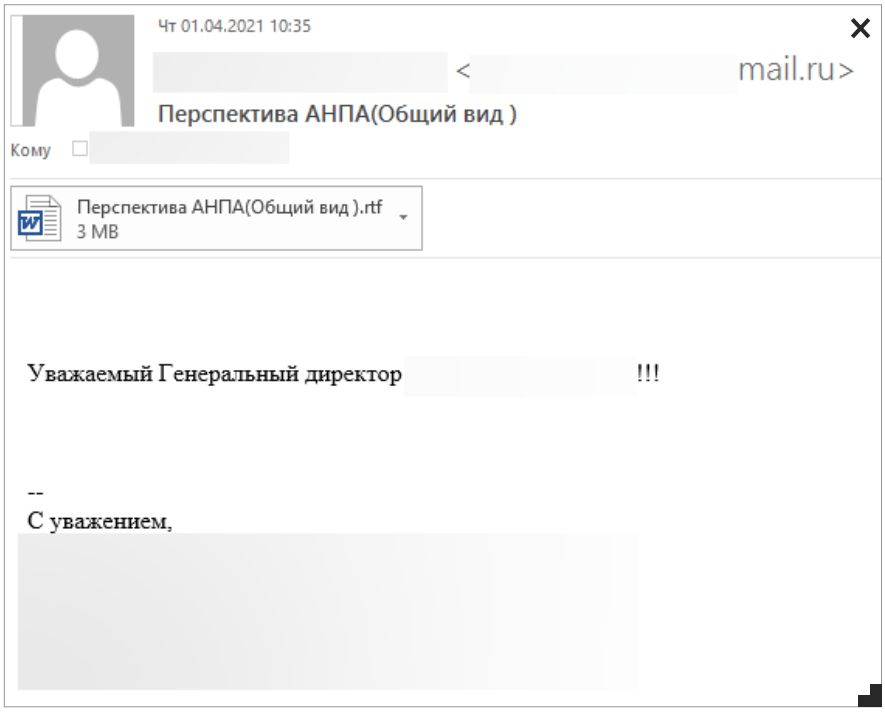


*Рисунок 17. Фишинговое письмо от злоумышленников, распространяющих троян B-JDUN*

Примерно в шести из десяти атак на промышленную отрасль злоумышленники преследуют цель получения данных; это касается, к примеру, APT-группировки RedFoxtrot, кибершпионскую кампанию которой обнаружили аналитики компании Recorded Future. В своих атаках группировка использует целое множество вредоносов для удаленного управления: IceFog, ShadowPad, RoyalRoad, PCShare, PlugX и Poison Ivy.

# 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 предается 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 компаний 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.