



PT

Актуальные киберугрозы

I квартал 2020 года

ptsecurity.com

Содержание

| | |
|---|----|
| Резюме | 3 |
| Сводная статистика | 4 |
| Спрятаться от антивируса: атаки с использованием вредоносного ПО | 7 |
| Фишинговые рассылки на тему COVID-19 | 8 |
| Вирус вносит коррективы | 10 |
| Уязвимость в Citrix взяли в оборот | 11 |
| Шифровальщики развивают новую стратегию шантажа | 12 |
| Отраслевая специфика | 13 |
| Государственные учреждения | 13 |
| Промышленные компании | 15 |
| Медицинские учреждения | 18 |
| Об исследовании | 20 |

Резюме

По итогам I квартала 2020 года мы отмечаем:

- Количество киберинцидентов стремительно растет: выявлено на 22,5% больше атак, чем в IV квартале 2019 года.
- Доля целенаправленных атак осталась на уровне IV квартала прошлого года (67%).
- В течение квартала высокую активность проявляли 23 АРТ-группировки, атаки которых были направлены преимущественно на государственные учреждения, промышленные предприятия, финансовую отрасль и медицинские организации.
- Около 13% всех фишинговых рассылок в I квартале были связаны с темой COVID-19. Около половины из них (44%) пришлись на частных лиц, а каждая пятая рассылка была направлена на государственные организации.
- Более трети (34%) всех атак на юридические лица с использованием ВПО — это атаки троянов-шифровальщиков. Наибольшую активность проявляли Sodinokibi, Maze и DoppelPaymer. Операторы этих и некоторых других шифровальщиков создали собственные сайты, на которых публикуют похищенную у жертв информацию в случае отказа платить выкуп.
- Доля атак, направленных на частных лиц, составила 14%. Половина всех украденных данных — логины и пароли. Это связано с высокой долей шпионского ПО (56%) во вредоносных кампаниях против частных лиц.

По нашим прогнозам, в мире будет нарастать число атак на удаленные рабочие места сотрудников. В связи с массовым переходом на удаленную работу в ближайшее время компании могут столкнуться с ростом попыток взлома корпоративных учетных записей и с эксплуатацией уязвимостей в системах удаленного доступа. Угрозы крайне актуальны для компаний, в которых нет строгой парольной политики и регулярного обновления ПО.

Заблокировать возможные атаки на веб-приложения сетевого периметра, в том числе на системы удаленного доступа, например Citrix Gateway, помогут межсетевые экраны уровня приложений (WAF). Для предотвращения заражения компьютеров сотрудников вредоносным ПО мы рекомендуем проверять вложения из электронных писем на предмет вредоносной активности с помощью решений класса sandbox (песочниц). Кроме того, мы советуем придерживаться общих [рекомендаций](#) по обеспечению личной и корпоративной кибербезопасности.

Сводная статистика

В I квартале 2020 года мы зафиксировали на 22,5% больше атак, чем в последнем квартале 2019 года. Начало года стало тяжелым периодом для всего мира. Эпидемия коронавирусной инфекции COVID-19 внесла коррективы в мировую экономику и в жизнь обычных людей. Ситуация отразилась и на информационной безопасности.

© Positive Technologies

На **22,5%**
больше кибератак,
чем в IV квартале
2019 года

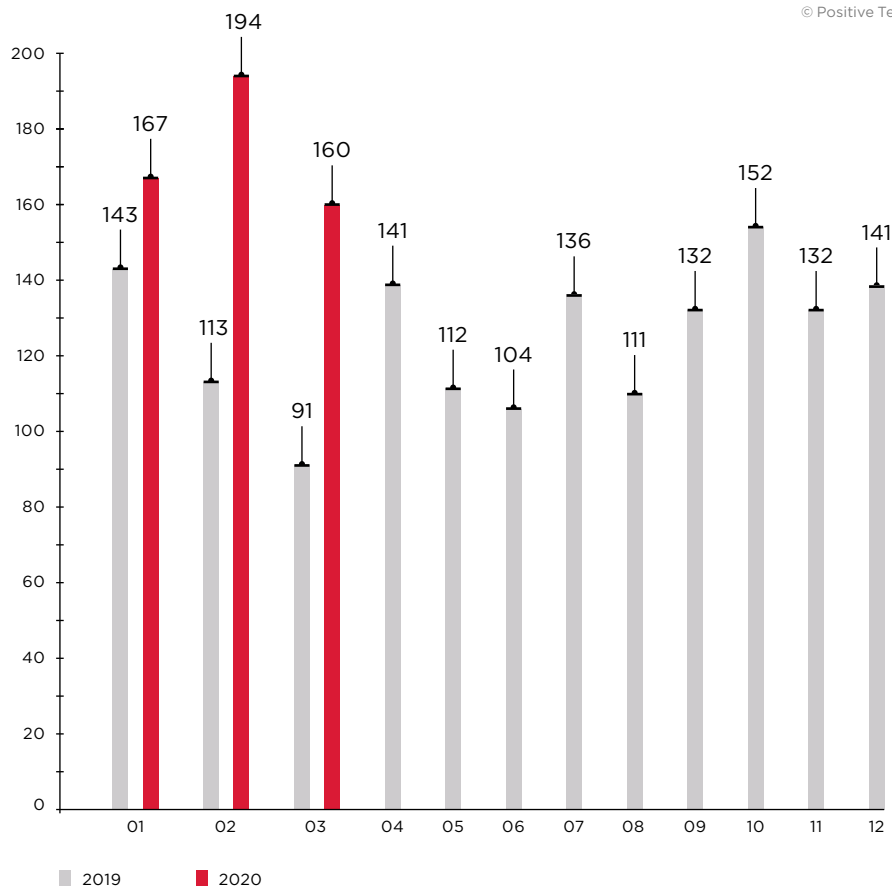


Рисунок 1. Количество атак в 2019 и 2020 годах по месяцам

© Positive Technologies

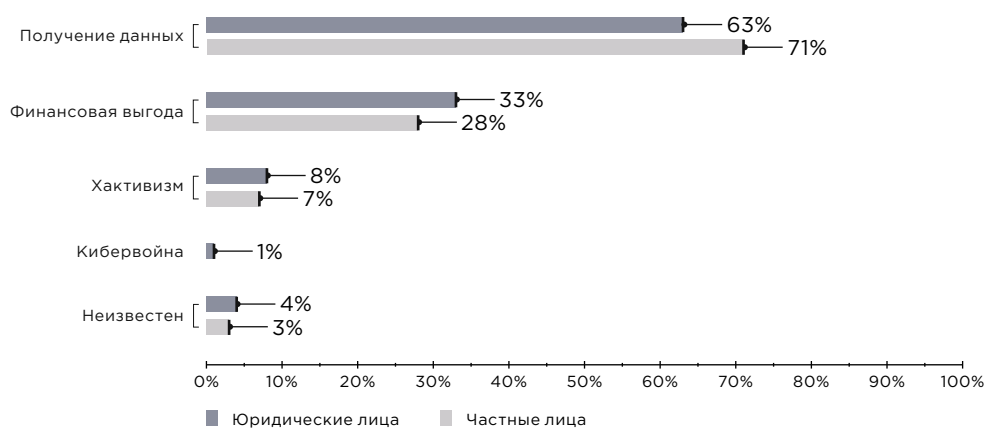


Рисунок 2. Мотивы злоумышленников (доля атак)

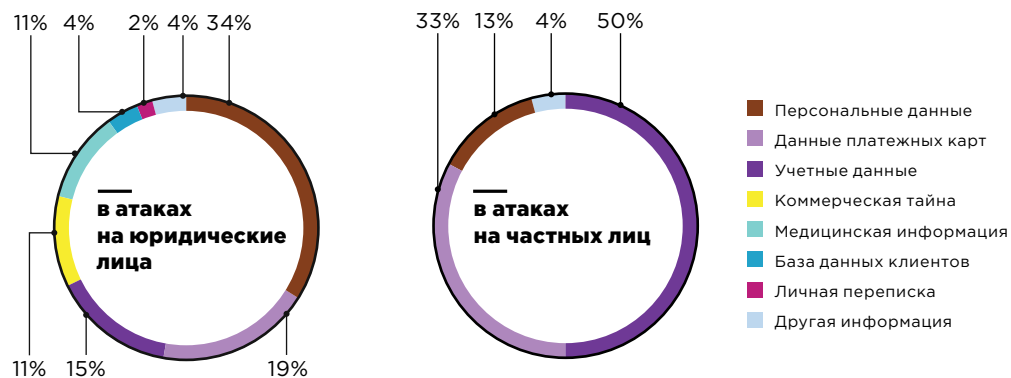


Рисунок 3. Типы украденных данных

67% атак
носят целе-
направленный
характер

14% атак
направлены
против
частных лиц

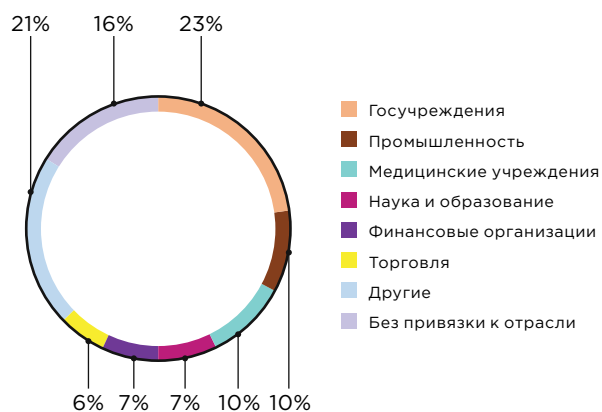


Рисунок 4. Категории жертв среди юридических лиц

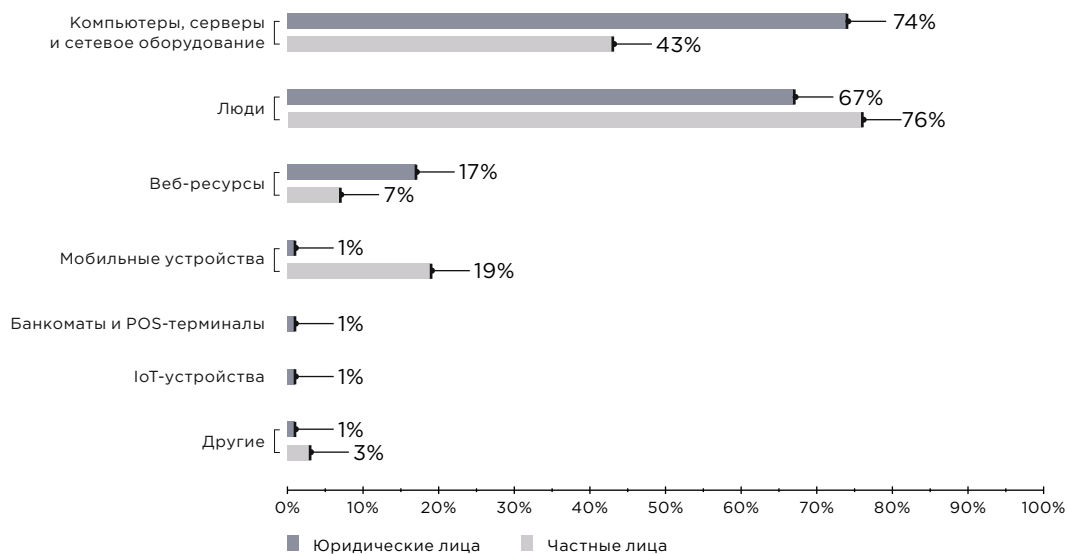


Рисунок 5. Объекты атак (доля атак)

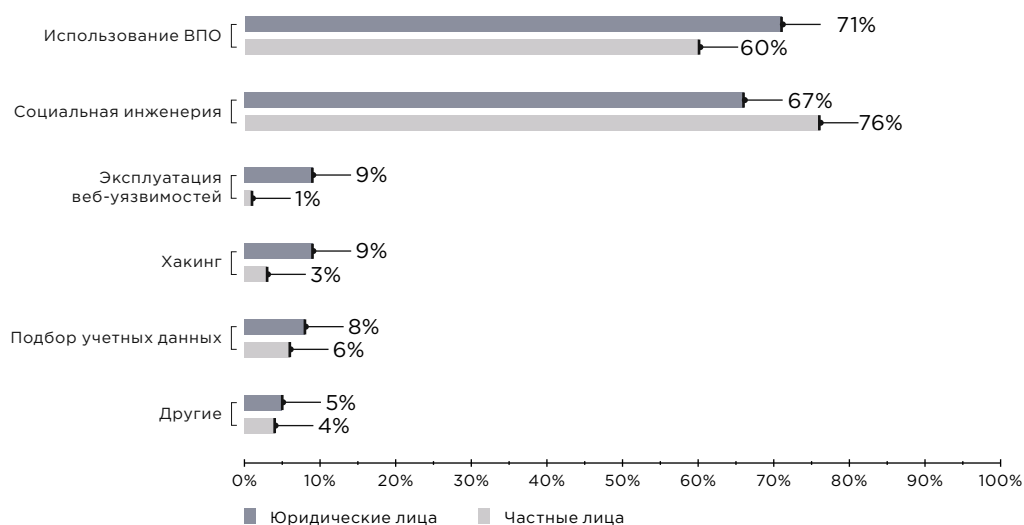


Рисунок 6. Методы атак (доля атак)

| | | Категории жертв | | | | | | | |
|------------|--|-----------------|------------------------|----------------|------------------------|---------------------|----------|--------|------------------------|
| | | Госучреждения | Финансовые организации | Промышленность | Медицинские учреждения | Наука и образование | Торговля | Другие | Без привязки к отрасли |
| Всего атак | | 103 | 30 | 47 | 45 | 32 | 29 | 92 | 71 |
| Объект | Компьютеры, серверы и сетевое оборудование | 87 | 26 | 42 | 31 | 23 | 9 | 60 | 54 |
| | Веб-ресурсы | 12 | 3 | 3 | 3 | 5 | 18 | 20 | 11 |
| | Люди | 80 | 23 | 40 | 35 | 27 | 9 | 45 | 42 |
| | Мобильные устройства | | | | | | 1 | 2 | 14 |
| | Банкоматы и POS-терминалы | | 1 | | | | 1 | 1 | |
| | IoT-устройства | | | 1 | | | | 3 | |
| | Другие | | | | | | 3 | | 2 |
| Метод | Использование ВПО | 83 | 25 | 43 | 27 | 23 | 9 | 56 | 51 |
| | Социальная инженерия | 81 | 23 | 41 | 35 | 27 | 9 | 46 | 42 |
| | Подбор учетных данных | 2 | 1 | | 5 | 3 | 3 | 17 | 5 |
| | Хакинг | 6 | 4 | 3 | 3 | 1 | | 10 | 14 |
| | Эксплуатация веб-уязвимостей | 6 | 2 | 2 | | 3 | 15 | 6 | 6 |
| | Другие | 7 | 1 | | 3 | | 1 | 10 | 1 |
| Мотив | Получение данных | 67 | 19 | 36 | 32 | 8 | 28 | 56 | 39 |
| | Финансовая выгода | 25 | 10 | 15 | 18 | 21 | 3 | 37 | 19 |
| | Хактивизм | 10 | 2 | | 1 | 3 | | 11 | 8 |
| | Кибервойна | 1 | | 1 | | | | 2 | 1 |
| | Неизвестен | 2 | 1 | | 1 | 2 | | | 10 |

Градации цвета показана доля атак внутри одной категории жертв

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

Спрятаться от антивируса: атаки с использованием вредоносного ПО

С течением времени актуальность заражения вредоносным ПО только растет. Киберпреступники не ограничиваются одним типом ВПО: используют многофункциональные трояны либо загружают на скомпрометированные устройства целый букет из различных зловредов. Злоумышленники постоянно ищут приемы, с помощью которых можно обойти антивирусы и встроенные в ОС механизмы защиты. Например, с начала года мы видим попытки использовать новую уязвимость [CVE-2020-0601](#) в Windows CryptoAPI для подписи вредоносного ПО (уязвимость позволяет обходить механизм проверки сертификатов). Другой пример — ВПО для удаленного управления SysUpdate. Это уникальная разработка АРТ-группы Bronze Union, которую злоумышленники используют для доставки на подконтрольные им устройства другого ВПО (полезной нагрузки). Как правило, эта полезная нагрузка не детектируется антивирусами, так как файл имеет неопределенный формат и антивирус не может его распознать. Еще один пример — зловред FakeChmMsi со сложной цепочкой доставки трояна Gh0st, в ходе которой дважды применяется техника [DLL hijacking](#), затрудняющая анализ ВПО средствами антивирусной защиты. Эффективно противодействовать современному вредоносному ПО, которое способно обходить антивирусы, межсетевые экраны, IPS, почтовые и веб-шлюзы, помогают песочницы — решения, позволяющие запускать файл в изолированной виртуальной среде и анализировать его поведение на предмет вредоносной активности.

Наибольшее число атак на корпоративную инфраструктуру с использованием ВПО пришлось на долю троянов-шифровальщиков. Частные лица больше всего подвергались атакам с использованием инфостилеров, кейлоггеров и банковских троянов.

© Positive Technologies

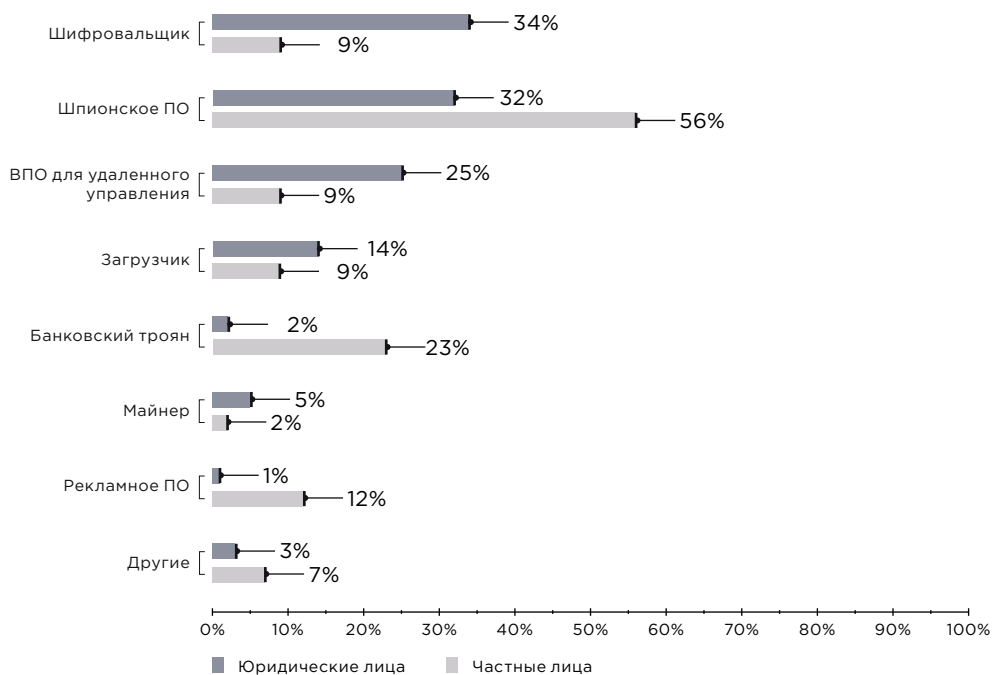


Рисунок 7. Типы вредоносного ПО (доля атак с использованием ВПО)

Как и прежде, вредоносные кампании, нацеленные на организации, в восьми из десяти случаев начинались с рассылки электронных писем с вложениями. Для частных лиц высок риск заразить компьютер не только через электронную почту, но и в результате посещения сайтов и загрузки программ с сомнительных веб-ресурсов. Например, в I квартале злоумышленники скомпрометировали ряд сайтов на базе WordPress и перенаправляли их посетителей на фишинговые страницы, где под видом обновления браузера Chrome распространялся бэкдор. Вредоносное ПО было загружено более 2000 раз.

© Positive Technologies

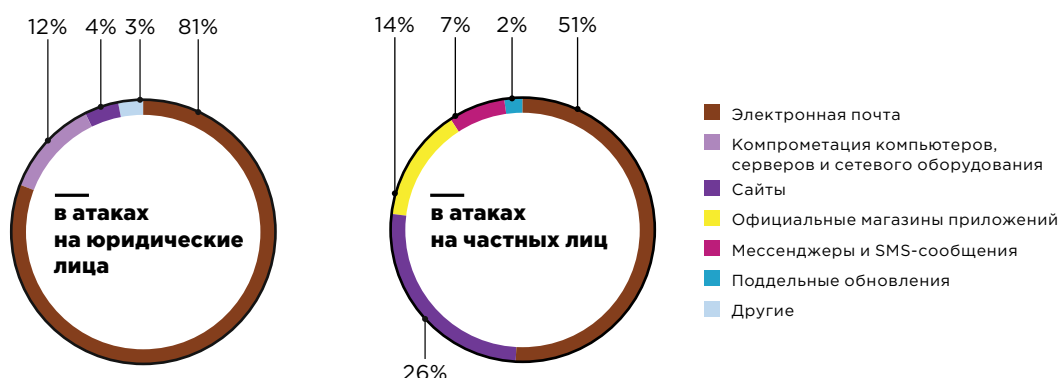


Рисунок 8. Способы распространения ВПО

Фишинговые рассылки на тему COVID-19

Злоумышленники быстро подхватили тему всеобщего беспокойства по поводу коронавирусной инфекции и стали использовать ее для фишинговых писем. По нашим подсчетам, в I квартале около 13% атак, в которых киберпреступники задействовали методы социальной инженерии, были связаны с коронавирусом.

© Positive Technologies

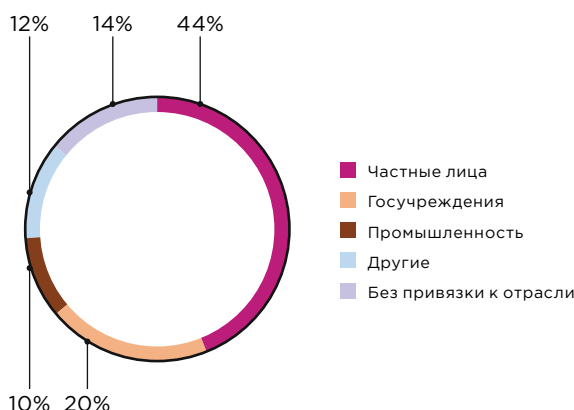


Рисунок 9. Категории жертв фишинговых рассылок на тему COVID-19

Рост числа фишинговых рассылок, посвященных COVID-19, мы отмечаем со второй половины января. Эпидемией пользовались как для проведения массовых вредоносных кампаний, так и для сложных целенаправленных атак (APT-атак). Под видом официальной информации о статистике заражений, о вакцине и мерах профилактики, рассылаемой якобы от имени государственных органов и медицинских учреждений, в I квартале распространялись трояны Emotet, Remcos, AZORult, Agent Tesla, LokiBot, TrickBot и множество других.

В феврале эксперты Positive Technologies Expert Security Center (PT ESC) выявили атаку группы TA428. В качестве текста приманки группа разослала документ со статистикой распространения коронавирусной инфекции. К слову, в январе эта группа использовала в качестве темы для писем обострение отношений между США и Ираном. Вредоносные документы доставляли на компьютер жертвы загрузчик с зашифрованным шелл-кодом Poison IVY.

| COVID-19 | | | | | | |
|---|-------|--------------------------------|------------|--------------------------------|---------------|--------------------------------|
| Daily update (FOR INTERNAL USE ONLY) | | | | | | |
| Ministry of Health Mongolia | | | | | | |
| Date: 17 February 2020, 01.00 pm (Ulaanbaatar time) | | | | | | |
| GLOBAL SITUATION (Table 1) | | | | | | |
| | WHO* | | MOH, PRC** | | MoH, Mongolia | |
| | total | new cases in the last 24 hours | total | new cases in the last 24 hours | Total | new cases in the last 24 hours |
| Number of confirmed cases | 51857 | 1278 | 70586* | 2002 | - | - |
| Number of deaths | 1666 | 142 | 1770 | 104** | - | - |
| Number of suspected cases | NA | NA | 8228 | -1918 | 137 | 1 |
| Number of severe cases | NA | NA | 11272 | 219 | - | - |
| Number of recovered cases | NA | NA | 10773 | 1348 | - | - |

*Clinically confirmed cases in addition to the lab confirmed cases
 **Lab confirmed cases

A total of 683 (157 cases in the last 24 hours) confirmed cases have been reported in 25 countries outside China. Third death outside China is reported in France. 355 confirmed cases reported in Diamond Princess Ship docked in Yokohama, Japan.

Рисунок 10. Документ со статистикой по COVID-19 из рассылки TA428

В марте специалисты PT ESC зафиксировали четыре фишинговые рассылки, с помощью которых злоумышленники распространяли бэкдор Chinoxu. В одном из документов группа киберпреступников использовала текст, связанный с экономией бюджетных средств на фоне распространения коронавируса.

President discusses budget savings due to coronavirus with Finance Minister

President of Kyrgyzstan Sooronbai Jeenbekov received a Finance Minister Baktygul Jeenbaeva. The Information Policy Department of the Presidential Administration reported.

They discussed the current situation with implementation of the republican budget and measures to save budgetary funds amid the situation associated with the spread of coronavirus in neighboring countries and in the world.

Minister of Finance Baktygul Jeenbaeva noted that taking into account the existing risks, according to forecasts, the implementation of the republican budget for 2020 may amount to about 85 percent of the previously approved plan. According to the results for January — February, it amounted to 96 percent.

Рисунок 11. Документ из рассылки Chinoxy

Рассылки писем с вредоносными вложениями на тему эпидемии проводили также группы TA505, Hades, Mustang Panda, APT36, Higaia, SongXY. О последних двух мы поговорим подробнее в разделе про атаки на государственные учреждения.

Вирус вносит коррективы

Из-за сложной эпидемиологической обстановки правительства многих стран отправили школьников и студентов на дистанционное обучение, а работодателей обязали по возможности перевести сотрудников на удаленную работу. В этой ситуации многие компании вынуждены использовать VPN для удаленного доступа сотрудников в корпоративную сеть. Как известно, в последнее время злоумышленники активно эксплуатируют уязвимости в VPN-решениях и системах для организации удаленного доступа, в частности в продуктах от Pulse Secure, Fortinet, Palo Alto и Citrix. Мы рекомендуем незамедлительно установить последние обновления, выпущенные этими производителями. В противном случае существует большой риск компрометации. Так, британская компания Finastra, ставшая в марте жертвой шифровальщика, использовала непропатченные версии Citrix ADC и VPN от Pulse Secure.

Опасные уязвимости в VPN-решениях и системах для удаленного доступа

| | |
|--------------------------------|---------------------------|
| CVE-2019-19781 | Citrix |
| CVE-2019-11510 | Pulse Secure |
| CVE-2019-11539 | Pulse Secure |
| CVE-2018-13379 | Fortinet |
| CVE-2018-13382 | Fortinet |
| CVE-2018-13383 | Fortinet |
| CVE-2018-1579 | Palo Alto Networks |

Злоумышленники, нацеленные на эксплуатацию

- Операторы шифровальщика Sodinokibi
- APT5
- APT33
- APT34
- APT39
- APT41

В связи с масштабным переходом на удаленную работу выросло число узлов российских компаний, доступных для подключения по протоколу RDP. По нашим прогнозам, компании по всему миру могут столкнуться с ростом количества атак на RDP начиная со II квартала 2020 года. Например, известный банковский троян TrickBot уже обзавелся новым модулем rdpScanDll, который подбирает учетные данные для подключения по протоколу RDP.

С ростом числа пользователей платформы для видеосвязи Zoom интерес к ней растет и со стороны злоумышленников. Так, в течение I квартала было зарегистрировано более 1700 фишинговых доменов, связанных с названием популярной платформы. Активное использование Zoom выявило в приложении ряд уязвимостей. Специалисты компании Check Point обнаружили в платформе брешь, позволявшую злоумышленникам без приглашения присоединяться к чужим видеоконференциям. Инциденты, связанные с несанкционированным вторжением в онлайн-конференции через Zoom, получили название Zoom-bombing. По заявлению ФБР, в США регистрируется большое число подобных инцидентов. Записи тысяч видеозвонков оказались размещены на YouTube и Vimeo. В свободный доступ попали частные видеозвонки, записи бизнес-собраний, сеансы у врачей, занятия в учебных заведениях. Кроме того, в конце квартала стало известно об уязвимости типа UNC path injection, которая позволяет злоумышленникам похищать через Zoom учетные данные Windows.

В условиях карантина и самоизоляции вырос спрос на услуги по доставке готовой еды и продуктов питания. Воспользовавшись ситуацией, злоумышленники устроили DDoS-атаку на сервис takeaway.com и потребовали 2 биткойна за ее прекращение. Киберпреступники не преминули вмешаться и в работу медицинских учреждений, об атаках на которые мы поговорим в разделе «Отраслевая специфика».

Уязвимость в Citrix взяли в оборот

В I квартале 12% вредоносного ПО доставлялось в инфраструктуру компаний путем компрометации сетевого оборудования, серверов или рабочих компьютеров. Одна из уязвимостей, которая в последнее время активно эксплуатируется для доставки ВПО, — это уязвимость в ряде продуктов Citrix (CVE-2019-19781). О ней стало широко известно еще в конце 2019 года. Напомним, что это критически опасная брешь, которая позволяет неавторизованному злоумышленнику выполнять произвольный код. Уязвимость затронула порядка 80 тысяч организаций по всему миру, причем больше всего потенциальных жертв в государственном секторе. Производитель выпустил финальные патчи 24 января 2020 года.

В течение I квартала брешь эксплуатировалась группой APT41 в целенаправленных атаках на государственные учреждения, финансовую отрасль, телекоммуникации, промышленность, медицину, СМИ. Кроме того, с помощью эксплуатации уязвимости CVE-2019-19781 были, предположительно, атакованы инфраструктура Потсдама и Управление радиотехнической обороны в Австралии.

В январе специалисты FireEye установили, что неизвестные киберпреступники загружают на уязвимые устройства Citrix бэкдор, получивший название NOTROBIN. Интересно, что NOTROBIN умеет выявлять и блокировать попытки эксплуатации CVE-2019-19781 со стороны других атакующих, обеспечивая своим владельцам единоличный контроль над скомпрометированным устройством.

Шифровальщики развивают новую стратегию шантажа

В первом квартале 2020 года атаки шифровальщиков, при которых злоумышленники требуют выкуп за неразглашение похищенных данных, набирали обороты. Для публикации украденных данных киберпреступники теперь создают собственные сайты. Такими сайтами уже обзавелись операторы Maze, Sodinokibi, Nemty, DoppelPaymer, Nefilim, CLOP и Sekhmet.

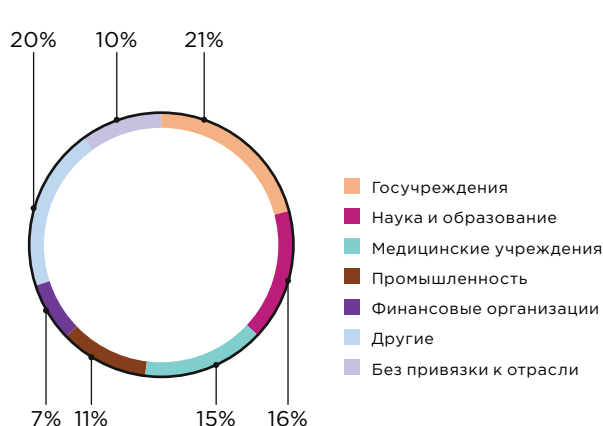


Рисунок 12. Категории жертв шифровальщиков среди юридических лиц

Операторы шифровальщика Sodinokibi ищут новые рычаги давления на скомпрометированные организации. В планах у злоумышленников оповещать фондовые биржи об атаках на крупные компании-жертвы в случае отказа последних платить. По задумке киберпреступников, возможное падение стоимости акций жертвы должно стать для нее дополнительным стимулом для уплаты выкупа.

NO AVATAR

Premium

Joined: May 12, 2019

Messages: 80

Reaction score: 118

Points: 38

Feb 26, 2020
Thread starter 🔊 🔖 #49

По всем ранее опубликованным заказам мы нашли исполнителей. Поставленные задачи трудны, но решаемы. Мы надеемся как можно скорее добавить весь функционал, как он будет готов. Также мы закончили работу над блогом, в котором будут публиковаться данные со скомпрометированных систем. Всех адвертов мы призвали как можно чаще копировать информацию, поэтому мы убеждены, что это будет весьма эффективное использование данного блога. Не вся информация блога доступна для просмотра - некоторая информация доступна предварительно сервисам по продаже СС и иной информации, что позволит получать достаточно высокий показатель доходности с данной информации. Теперь мы можем с уверенностью сказать - все фирмы, в которых есть наш продукт, имеют серьезные проблемы с конфиденциальностью данных. Очень рекомендуем данным компаниям переходить к переговорам достаточно быстро, поскольку данный блог мы планируем расширять и совершенствовать. Есть интересные мысли автооповещения e-mail адресов акционных бирж (например NASDAQ), что позволит влиять на финансовое состояние компании достаточно быстро и эффективно.

Теперь все данные будут публиковаться в этом блоге

Имеется 3 места в партнёрской программе. Интересуют **сети**. В скором времени, вероятно, мы покинем все площадки и прекратим набор. Поторопитесь.

Last edited: Feb 26, 2020

Рисунок 13. Сообщение о планах Sodinokibi

Отраслевая специфика

Далее мы подробно проанализируем атаки на отдельные отрасли, которые нам показались наиболее интересными в I квартале 2020 года.

Государственные учреждения

© Positive Technologies

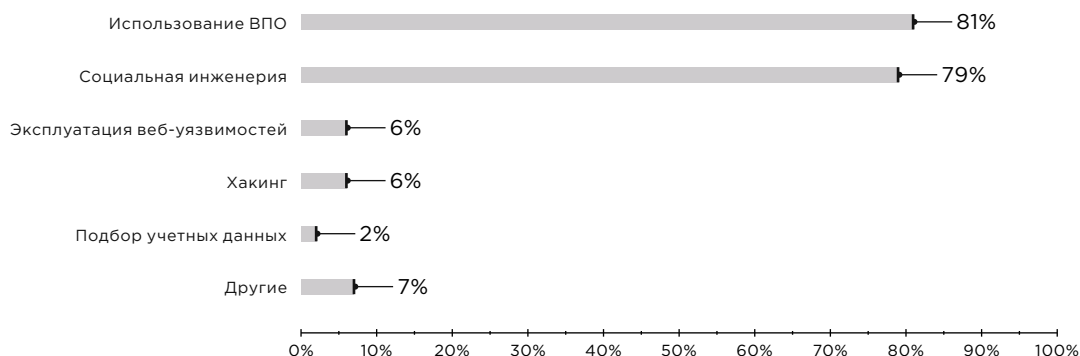


Рисунок 14. Методы атак (доля атак на госучреждения)

© Positive Technologies

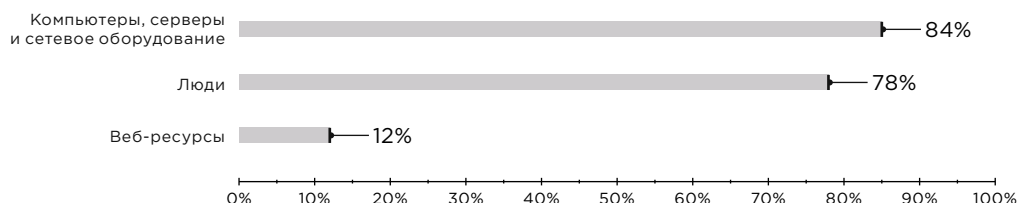


Рисунок 15. Объекты атак (доля атак на госучреждения)

По сравнению с последним кварталом прошлого года существенно выросла доля атак на госучреждения с использованием ВПО и методов социальной инженерии. Этому могла способствовать эпидемия. Многие злоумышленники рассылали в госучреждения разных стран письма с вредоносными вложениями на тему коронавирусной инфекции. В январе 2020 года специалисты PT ESC зафиксировали две атаки APT-группы [SongXY](#). В качестве приманки злоумышленники использовали текст на монгольском языке, что, вероятнее всего, говорит об их узкой региональной направленности. В тексте была информация о вспышке нового вируса COVID-19 в Китае. Документ в формате RTF с эксплойтом для уязвимости [CVE-2018-0798](#) сохранял на жесткий диск компьютера жертвы зашифрованный загрузчик, расшифровывал, запускал, после чего происходила загрузка основной полезной нагрузки.

**МОНГОЛ УЛСААС БНХАУ-Д СУУГАА
ЭЛЧИН САЙДЫН ЯАМ**

ШУУРХАЙ МЭДЭЭ

2020 оны 1 дүгээр сарын 22-ны өдөр №ШМ072004 Бээжин хот

Шинэ коронавирусын халдварын тархалтын тухай

БНХАУ-ын Төрийн зөвлөлийн Хэвлэл мэдээллийн албанаас өнөөдрийн 10.00 цагт хийсэн хэвлэлийн бага хурлын үеэр Хятад улсад шинэ коронавирусын халдварт хатгалгаагаар өвчилсөн 440 хүн байгаа бөгөөд 9 нас барсан тохиолдол байгааг мэдээллэв.

Хятадын Үндэсний эрүүл мэндийн хорооноос гаргасан статистик мэдээллээр өнөөдрийн байдлаар Хятад улсын өмнөд болон зүүн өмнөд хэсгийн 14 муж, хот мөн АНУ, Япон, Өмнөд Солонгос, Австрали (тус бүр 1), Сингапур (7), Тайланд (2) зэрэг улсад тархсан байна. Вирусын тархалтын явц хурдан байгаа бөгөөд дээрх 440 өвчтөний ойрын хүрээний нийт 2197 хүнд тандалт хийж, 765 хүний халдваргүйг тогтоож, 1394 хүнийг үргэлжлүүлэн хянаж байна.

Шинэ коронавирусын халдварын талаарх шуурхай мэдээллийг үргэлжлүүлэн хүргэх болно.

[Эх сурвалж: Хятадын Ардын өдрийн сонин цахим мэдээ](#)

БОЛОВСРУУЛСАН:

Рисунок 16. Документ-приманка в формате RTF на тему COVID-19 из рассылки группы SongXY

В I квартале специалисты PT ESC выявили две атаки группы Higaia. Эта группа атакует правительственные учреждения, дипломатические представительства и правозащитные организации в Китае, Северной Корее, Японии, Непале, Сингапуре, России и других странах. Обе кампании начинались с фишинговых рассылок. В первой использовался текст, связанный с северокорейскими национальными праздниками и актуальными новостями. Во второй рассылке группа маскировала вредоносный LNK-файл под PDF-документ, посвященный теме COVID-19.

Coronavirus disease 2019 (COVID-19)

Situation Report – 48

Data as reported by national authorities by 10AM CET 08 March 2020

HIGHLIGHTS

- 8 new countries/territories/areas (Bulgaria, Costa Rica, Faroe Islands, French Guiana, Maldives, Malta, Martinique, and Republic of Moldova) have reported cases of COVID-19 in the past 24 hours.
- Over 100 countries have now reported laboratory-confirmed cases of COVID-19.
- WHO has issued a [consolidated package of existing preparedness and response guidance](#) for countries to enable them to slow and stop COVID-19 transmission and save lives. WHO is urging all countries to prepare for the potential arrival of COVID-19 by readying emergency response systems; increasing capacity to detect and care for patients; ensuring hospitals have the space, supplies and necessary personnel; and developing life-saving medical interventions.

SITUATION IN NUMBERS

total and new cases in last 24 hours

Globally

105 586 confirmed (3656 new)

China

80 859 confirmed (46 new)

3100 deaths (27 new)

Outside of China

24 727 confirmed (3610 new)

484 deaths (71 new)

101 Countries/territories/areas (8 new)

WHO RISK ASSESSMENT

| | |
|----------------|-----------|
| China | Very High |
| Regional Level | Very High |
| Global Level | Very High |

Рисунок 17. Документ из рассылки APT-группы Higaia

Специалисты PT ESC выявили также 14 атак группы Gamaredon, направленных на госучреждения Украины и Грузии. Группа, как обычно, использовала технику template injection, о которой мы рассказывали в конце прошлого года. Техника позволяет группе доставить на скомпрометированный компьютер загрузчик вредоносного ПО, исполненный как VBScript (VBS-загрузчик). Для защиты загрузчика от обнаружения с середины февраля группа начала использовать обфускацию (запутывание кода). Кроме того, изменился способ закрепления в инфраструктуре: загрузчик создает ключ в реестре Windows, который обеспечивает его функционирование после перезагрузки компьютера.



Рисунок 18. Документ из фишинговой рассылки группы Gamaredon

Промышленные компании

Для промышленности по-прежнему актуальной угрозой является заражение вредоносным ПО. Наибольшую опасность представляют шпионское ПО и трояны-шифровальщики. Их доли в атаках на промышленность с использованием ВПО составили 42% и 28% соответственно. В течение первого квартала года мы отмечали атаки на промышленность с использованием шифровальщиков Maze, Sodinokibi, Ryuk и DoppelPaymer.

© Positive Technologies

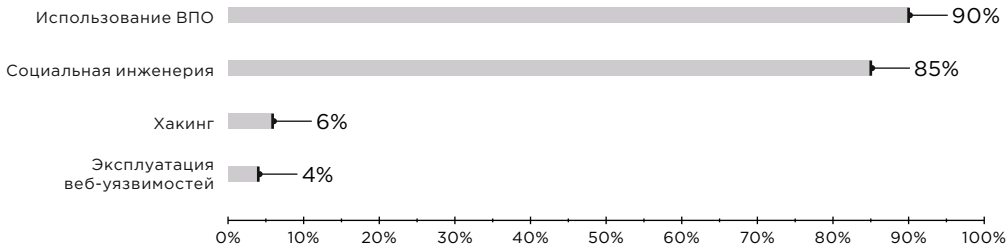


Рисунок 19. Методы атак (доля атак на промышленность)

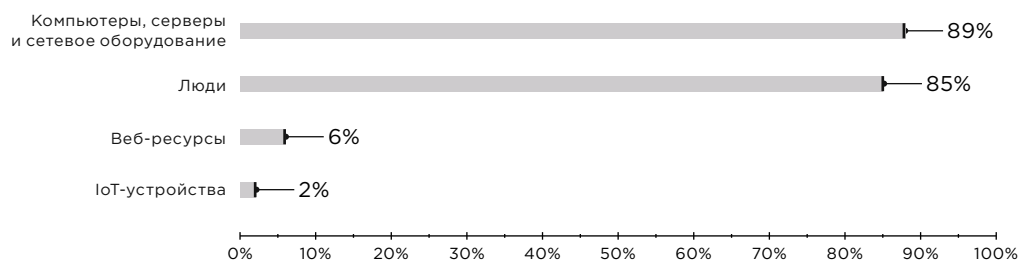


Рисунок 20. Объекты атак (доля атак на промышленность)

В начале года внимание многих специалистов по кибербезопасности привлек новый шифровальщик Snake, который умеет удалять теневые копии и останавливать процессы, связанные с работой промышленных систем управления. В частности, Snake останавливает процессы продуктов GE Proficy и GE Fanuc Licensing, Honeywell HMIWeb, FLEXNet Licensing Service, Sentinel HASP License Manager, ThingWorx Industrial Connectivity Suite. Вероятно, злоумышленники предполагают использовать Snake в целенаправленных атаках на промышленность. Шифровальщик оставляет на скомпрометированном компьютере файл с инструкциями для жертвы по дальнейшим действиям, где в качестве контактного адреса указан адрес электронной почты `barcocrypt@ctemplar[.]com`. По предположению специалистов PT ESC, это отсылка к компании Barco, которая в конце 2019 года была атакована вредоносным ПО Dustman, предназначенным для удаления данных. Не исключено, что Dustman и Snake связаны между собой, поскольку образцы этого ВПО появились в публичном доступе примерно в одно и то же время и были нацелены на промышленные предприятия.

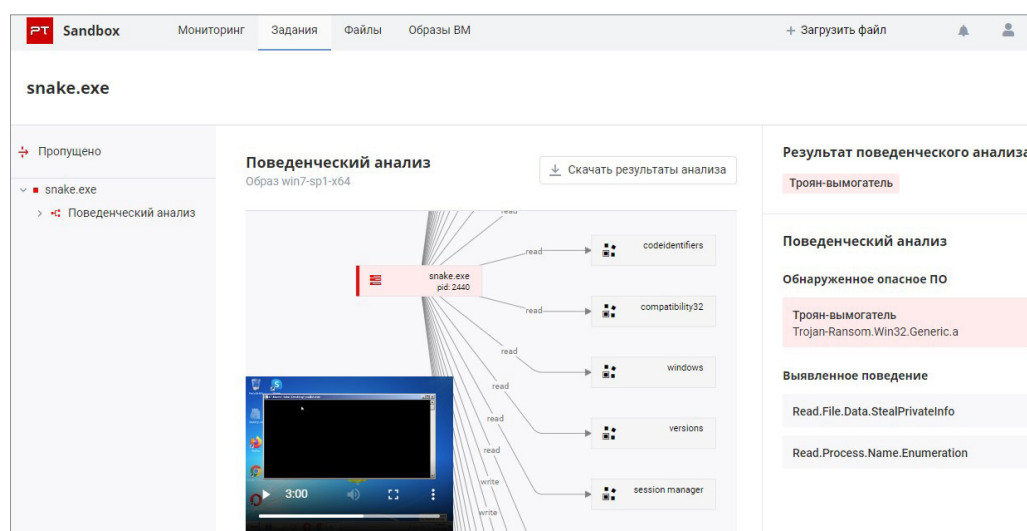


Рисунок 21. Детектирование Snake в PT Sandbox

Как и государственные учреждения, промышленность является целью многих АPT-групп по всему миру. Так, целью одной из АPT-атак группы Bivsonal в I квартале 2020 года стали российские организации авиационно-космической отрасли. Специалисты PT ESC установили, что в этой атаке вредоносное ПО для удаленного управления (RAT) доставлялось путем рассылки писем с вредоносными документами в формате RTF. Для создания этих документов группа использовала эксплойт-билдер Royal Road.



Рисунок 22. Документ из рассылки Bisonal

Для промышленности в России и СНГ не снижается актуальность атак группы RTM. В I квартале специалисты PT ESC выявили 29 фишинговых рассылок этой группы.

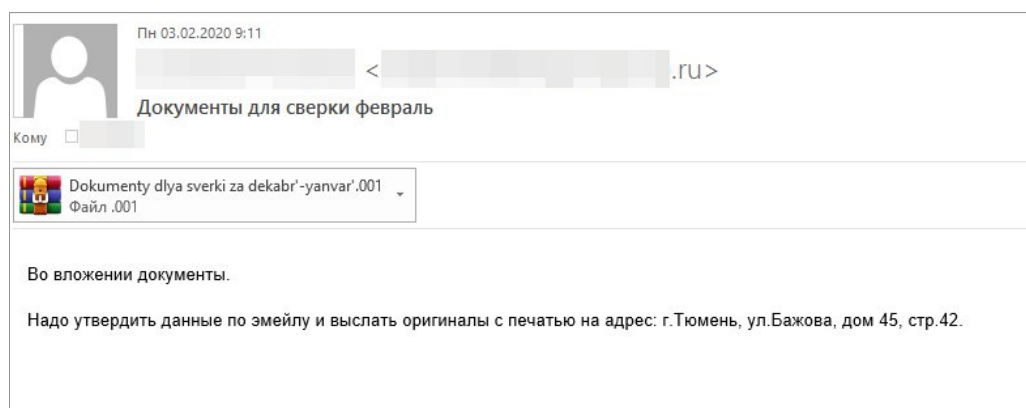


Рисунок 23. Письмо с вредоносным вложением из рассылки RTM в адрес промышленной компании

Медицинские учреждения

Число атак на медицину по сравнению с последним кварталом 2019 года существенно выросло. Это связано с повышенным интересом киберпреступников к медицинским организациям, которые сейчас находятся на передовой в борьбе с коронавирусной инфекцией. Рост числа успешных атак в условиях стресса и высокой нагрузки может быть связан со снижением бдительности медицинских работников, в адрес которых сейчас поступает большое количество писем от злоумышленников.

© Positive Technologies

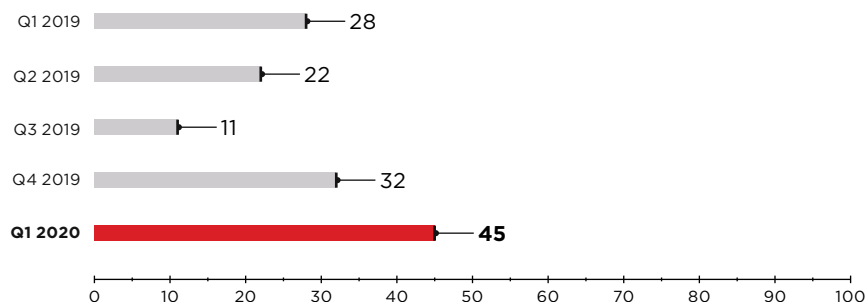


Рисунок 24. Число атак на медицинские учреждения

© Positive Technologies

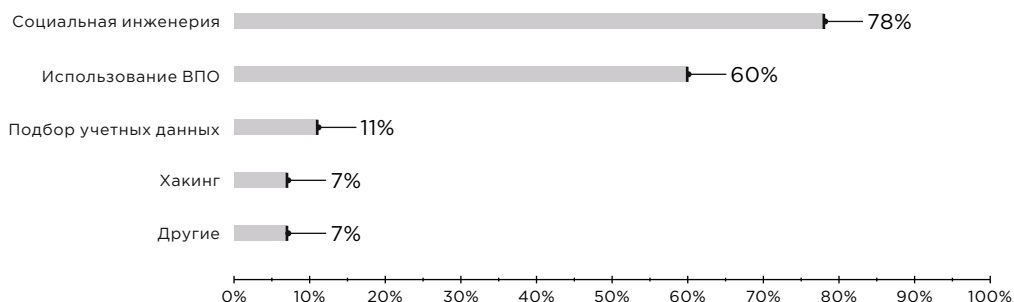


Рисунок 25. Методы атак (доля атак на медицинские учреждения)

© Positive Technologies

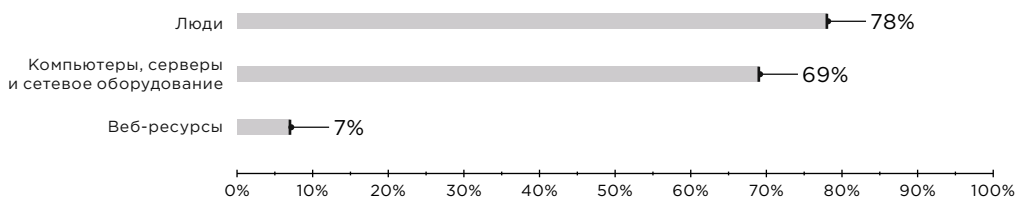


Рисунок 26. Объекты атак (доля атак на медицинские учреждения)

В 78% атак на медицинские учреждения были задействованы методы социальной инженерии. Злоумышленники рассылали сотрудникам фишинговые письма, цель которых — убедить получателя ввести корпоративные учетные данные в поддельную форму аутентификации.

Не менее актуальна угроза заражения вредоносным ПО. В ночь на 13 марта в результате кибератаки неизвестных злоумышленников была парализована работа компьютерной сети крупного медицинского центра в Брно (Чехия), где ежедневно проводилось тестирование граждан на заражение коронавирусной инфекцией. Днем позже стало известно, что британская медицинская компания Hammersmith Medicines Research, которая готовится к тестированию вакцины от коронавируса, была атакована операторами шифровальщика Maze. Напомним, что киберпреступники, стоящие за атаками Maze, одними из первых стали требовать от жертв выкуп за неразглашение похищенных перед шифрованием данных. В этот раз жертва отказалась платить и в кратчайшие сроки восстановила работу своих систем. Спустя несколько дней операторы Maze обещали прекратить атаки на медицинские учреждения на время эпидемии, однако уже после этого обещания опубликовали информацию, похищенную у Hammersmith Medicines Research. Это в очередной раз подтверждает, что не стоит верить киберпреступникам; никакие их обещания не дают гарантии, что зашифрованные данные будут восстановлены и не утекут в сеть.

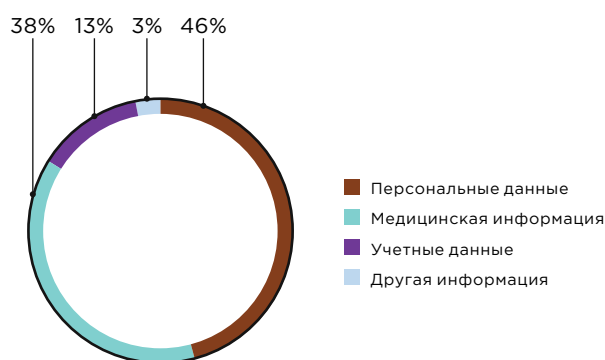


Рисунок 27. Украденные данные

Об исследовании

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

По нашей оценке, большинство кибератак не предаётся огласке из-за репутационных рисков, в связи с этим оценить 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. В исследовании мы используем следующие термины.

Киберугроза — это совокупность факторов и условий, создающих опасность нарушения информационной безопасности. Мы рассматриваем киберугрозы с точки зрения действий злоумышленников в киберпространстве, направленных на проникновение в информационную систему с целью кражи данных, денежных средств или с иными намерениями, которые потенциально ведут к негативным последствиям для государства, бизнеса или частных лиц. Действия злоумышленников могут быть направлены на IT-инфраструктуру, рабочие компьютеры, мобильные устройства, другие технические средства и, наконец, на человека как на элемент киберпространства.

Кибератака — несанкционированное воздействие на информационные системы и пользователей информационных систем со стороны киберпреступников с использованием технических средств и программного обеспечения в целях получения доступа к информационным ресурсам, нарушения нормальной работы или доступности систем, кражи, искажения или удаления информации.

Массовая атака — кибератака, которая направлена на широкий круг организаций и частных лиц. При проведении массовой атаки злоумышленники могут не ограничиваться одной отраслью экономики или вовсе не учитывать отраслевую принадлежность компаний, их задачей является компрометация максимального числа жертв.

Целевая атака — кибератака, которая направлена на конкретную компанию, отрасль экономики или на ограниченный круг частных лиц. В рамках целевой атаки злоумышленники, как правило, проводят предварительную разведку с целью собрать информацию о выбранной жертве.

Атака типа *advanced persistent threat* (АРТ-атака) — это хорошо организованная, тщательно спланированная многоэтапная целевая кибератака. За АРТ-атакой стоят преступные группировки (АРТ-группировки), участники которых отличаются высоким уровнем квалификации. АРТ-группировки, как правило, обладают значительными финансовыми ресурсами и техническими возможностями.

Объект атаки — объект несанкционированного воздействия со стороны киберпреступников, например веб-ресурс, компьютер, сервер, сетевое оборудование, мобильное устройство. Объектом атаки может быть и человек, если атака проводится с помощью методов социальной инженерии.

Метод атаки — совокупность приемов, которые используются киберпреступниками для достижения цели.

Хакинг — эксплуатация уязвимостей и недостатков защиты информационной системы для того, чтобы получить доступ к ресурсам или информации. В своих исследованиях мы выделяем некоторые методы хакинга в отдельные категории. Например, отдельно рассматриваем подбор учетных данных к доступным для подключения сервисам и эксплуатацию уязвимостей в веб-приложениях.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 18 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.