

Актуальные киберугрозы

IV квартал 2020 года

Содержание

Резюме	3
Сводная статистика	4
Атаки с использованием вредоносных программ	8
Новый пик шифровальщиков	10
Атаки на промышленные объекты	13
Атаки по цепочке	15
Опасный шоппинг	16
Предвыборная суэта	18
Тысяча и один способ эксплуатировать COVID-19	20
Об исследовании	22

Резюме

Итоги IV квартала 2020 года:

- В сравнении с предыдущим кварталом количество инцидентов выросло на 3,1%. Сохраняется тенденция к увеличению доли хакинга в атаках на организации: доля этого метода в IV квартале увеличилась на 6 процентных пунктов и составляет 36%. В атаках на частных лиц, напротив, отмечен резкий всплеск применения техник социальной инженерии: их доля выросла с 67% в III квартале до 85% в четвертом.
- На протяжении всего года мы наблюдали неуклонный рост числа атак с использованием программ-вымогателей, и IV квартал не стал исключением. Доля шифровальщиков среди всех атак с использованием вредоносного ПО составила 56% (+5 п. п.). В собранной нами статистике чаще всего фигурировали инциденты, связанные с программой-вымогателем Ryuk.
- Промышленность уже на протяжении двух лет входит в тройку наиболее часто атакуемых отраслей. Инциденты, связанные с деятельностью операторов шифровальщиков и APT-групп, составляют большую часть атак на эту отрасль. Особенно активной в минувшем квартале была группировка RTM: специалисты [PT Expert Security Center](#) зафиксировали 61 фишинговую рассылку, затрагивающую, в числе прочего, промышленные компании.
- Нельзя не отметить и нашумевшую атаку на цепочку поставок, от которой пострадали клиенты компании SolarWinds. Инцидент затронул более 40 организаций, установивших скомпрометированное обновление Orion — платформы для мониторинга локальных сетей. Похищенные в ходе этого инцидента инструменты компании FireEye, предназначенные для тестов на проникновение, могут еще очень долго всплывать в последующих атаках.
- Резкий рост числа атак замечен и в торговле. В сравнении с III кварталом количество инцидентов выросло на 56%. К этому причастны и операторы программ-вымогателей, и злоумышленники, устанавливающие веб-скиммеры на сайтах магазинов.
- В конце 2019 года мы делились своими прогнозами о том, как будет меняться ландшафт киберугроз в 2020 году. Мы предполагали, что будут резонансные кибератаки в преддверии выборов президента США. Наши прогнозы сбылись. Хакеры взламывали системы поддержки выборов, похищали денежные средства со счетов партий, а также распространяли огромное количество фишинговых писем на эту тему. Демократическая партия штата Висконсин, к примеру, за время предвыборной кампании зафиксировала более 800 попыток фишинговых атак.
- В четырех из десяти фишинговых кампаний эксплуатировалась тема вакцины от COVID-19. Доля атак с использованием техник социальной инженерии, в которых затрагивается тема пандемии, держится на уровне III квартала и составляет 4,6%. Несмотря на огромное количество публикаций о коронавирусе, злоумышленникам удается найти подход к жертвам и вынудить их ввести учетные данные на поддельных ресурсах, открыть прикрепленные к письму вредоносные вложения или передать данные банковской карты для «зачисления материальной помощи и оплаты вакцины».

Для защиты от атак мы, прежде всего, советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. В свете последних сообщений об атаках, направленных на эксплуатацию уязвимостей IT-инфраструктуры компаний, настоятельно рекомендуем своевременно устанавливать патчи. Для простоты выявления и устранения недостатков необходимо выстроить автоматизированный процесс управления уязвимостями. Помимо этого, следует использовать современные средства защиты, включая web application firewalls, средства анализа сетевого трафика, SIEM-системы. Для предотвращения атак, связанных с доставкой вредоносных программ по электронной почте, необходимо проверять вложения в песочнице — специальной виртуальной среде, предназначенной для поведенческого анализа файлов.

Сводная статистика

Сохраняется заявленная в III квартале тенденция к увеличению доли хакинга в атаках на организации. Доля этого метода выросла на 6 процентных пунктов. Восемь из 10 атак в минувшем квартале носили целенаправленный характер. В атаках на частных лиц замечен резкий всплеск социальной инженерии (доля выросла с 67% до 85%).

Превалирующим мотивом у злоумышленников по-прежнему является получение данных. Неизменным спросом в атаках на организации пользуются персональные данные и коммерческая тайна. Атакуя частных лиц, злоумышленники чаще всего крадут сведения для аутентификации и персональные данные. Количество инцидентов в IV квартале 2020 года в сравнении с предыдущим кварталом увеличилось на 3,1%. По сравнению с аналогичным периодом 2019 года прирост составил 41,2%.

**На 3,1% больше
кибератак, чем
в III квартале**

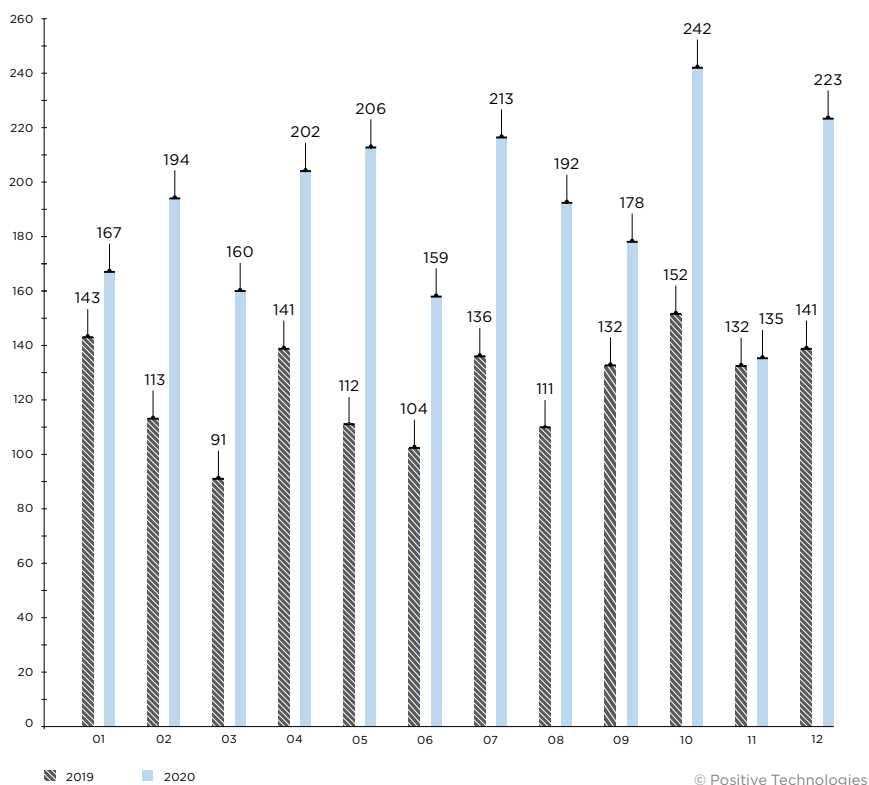


Рисунок 1. Количество инцидентов в 2019 и 2020 годах (по месяцам)

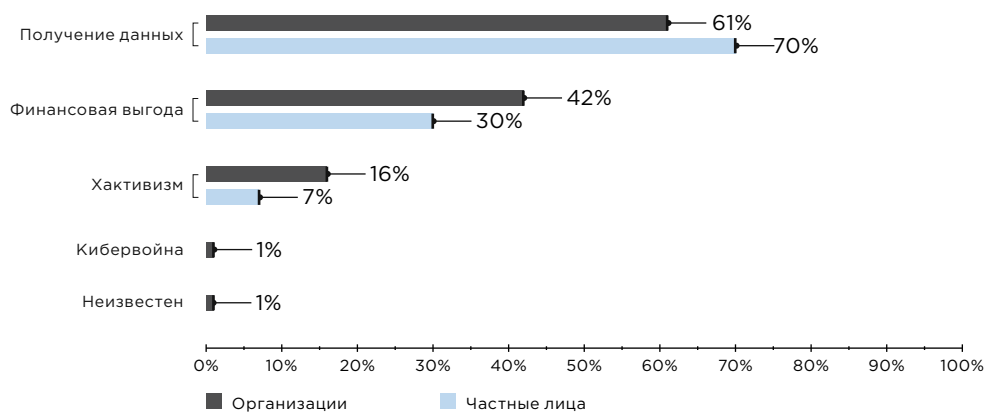


Рисунок 2. Мотивы злоумышленников (доля атак)

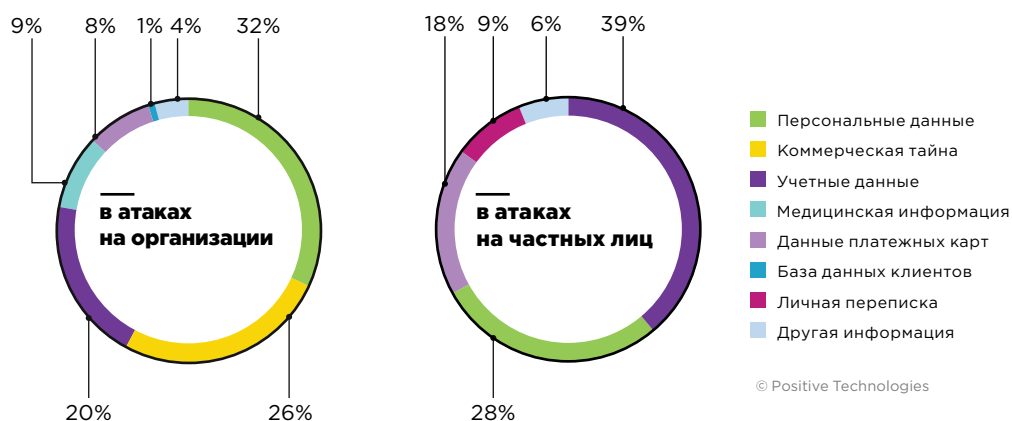


Рисунок 3. Типы украденных данных

80% атак носят целенаправленный характер

12% атак направлены против частных лиц

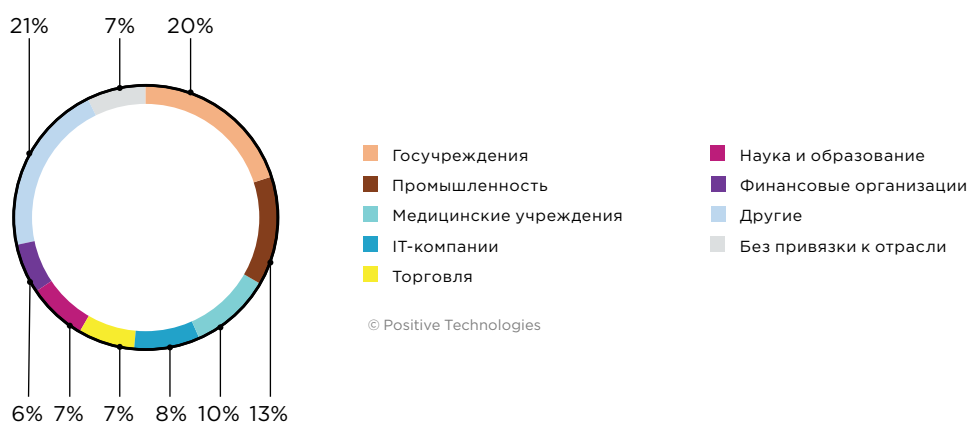


Рисунок 4. Категории организаций, ставших жертвами атак

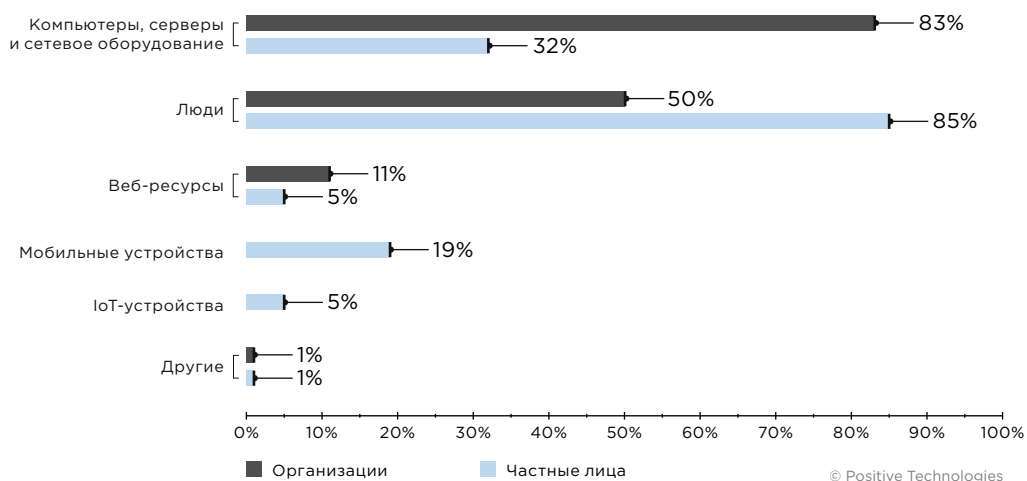


Рисунок 5. Объекты атак (доля атак)

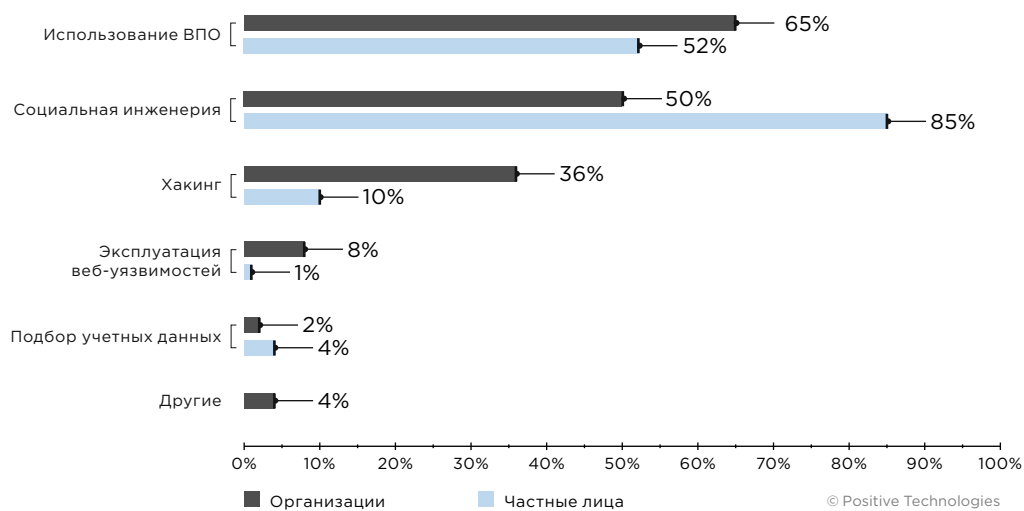


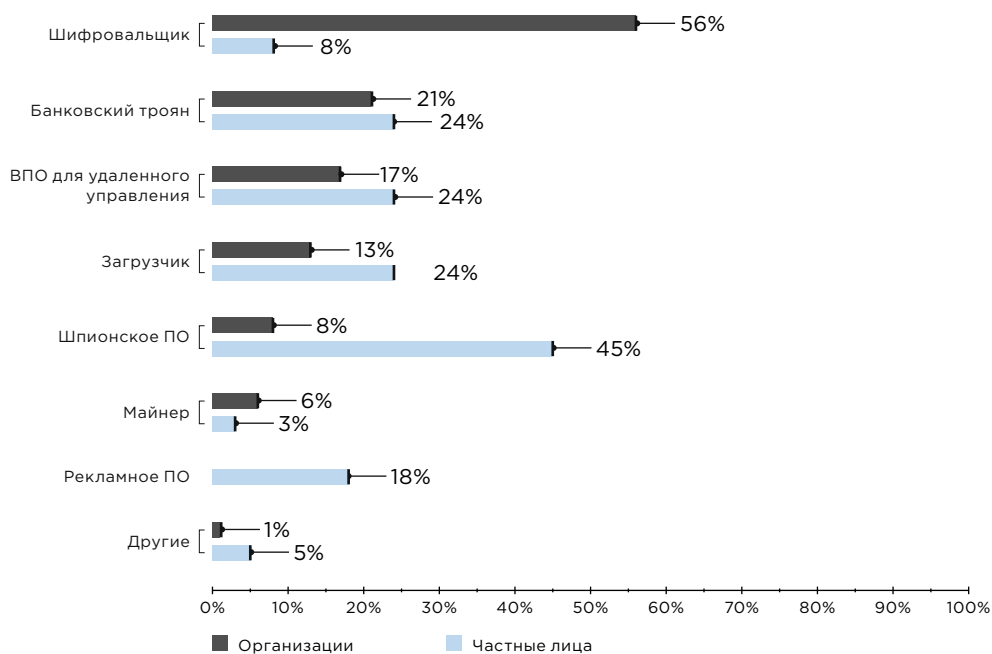
Рисунок 6. Методы атак (доля атак)

Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) внутри отраслей

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

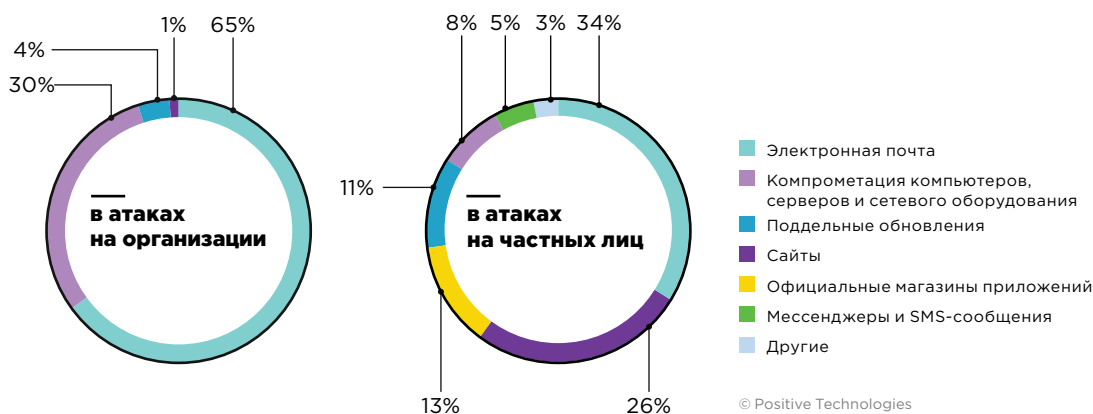
Атаки с использованием вредоносных программ

Весь год мы отмечаем неуклонный рост количества атак с использованием программ-вымогателей. После резкого скачка числа атак шифровальщиков в III квартале в последнем квартале 2020 года мы наблюдали умеренный рост. Доля атак с использованием подобного ВПО увеличилась на 5 п. п. и составляет 56%. В атаках, направленных на частных лиц, трендом на протяжении всего года было использование шпионского ПО.



© Positive Technologies

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



© Positive Technologies

Рисунок 8. Способы распространения вредоносного ПО

При атаках на организации способом распространения вредоносного ПО в 30% случаев была эксплуатация уязвимостей IT-инфраструктуры и недостатков систем защиты. На протяжении IV квартала злоумышленники активно эксплуатировали, к примеру, уязвимость серверов Oracle WebLogic (CVE-2020-14882), позволявшую удаленно выполнить код; патч для нее был выпущен еще в начале октября. Одна из хакерских атак была направлена на получение удаленного доступа на уязвимых узлах посредством внедрения полезной нагрузки Beacon, входящей в состав Cobalt Strike. В дальнейшем этот доступ использовался для сбора информации и развертывания других вредоносных программ. Другая волна атак была связана с распространением вредоносной программы DarkIRC. Этот вредонос обладает большим набором функций — от предоставления удаленного управления и кейлоггинга до запуска DDoS-атак и биткойн-клиппинга — и может распространяться по сети путем подбора учетных данных к Microsoft SQL Server или RDP-каналу, а также через SMB-соединения и USB-устройства. Интересная особенность DarkIRC в том, что перед установкой она проверяет, развернут ли узел на базе средств виртуализации — VMware, VirtualBox, VBox, QEMU или Xen, — и если да, то останавливает процесс заражения, чтобы избежать обнаружения в песочнице.

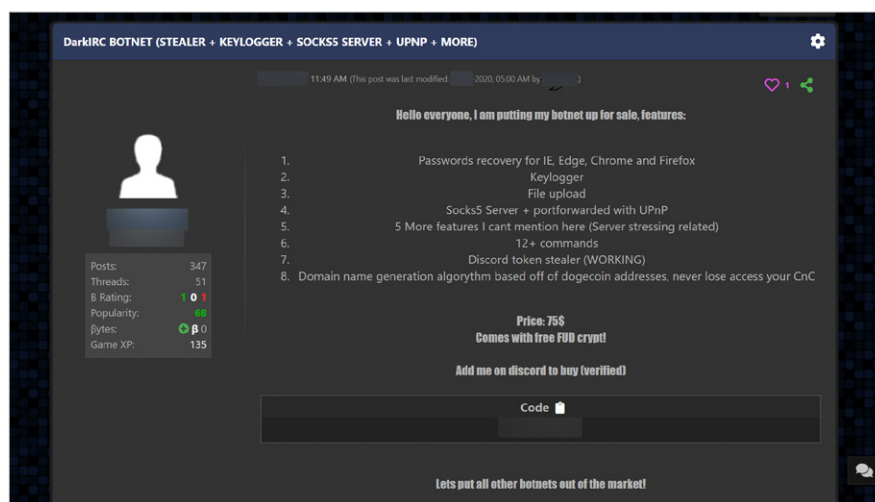


Рисунок 9. Объявление о продаже вредоносной программы DarkIRC в дарквебе

Социальная инженерия также не теряет своей актуальности. В 65% атак на организации злоумышленники использовали человеческий фактор, чтобы начать атаку. В этом контексте следует упомянуть множество атак с использованием трояна Emotet. Пробудившийся в середине года вредонос наделал много шума. В IV квартале злоумышленники, распространяющие его, атаковали несколько муниципалитетов и Национальный центр общественного здоровья Литвы, а также, ориентируясь на более широкую публику, рассылали фишинговые письма, выдавая их за оповещения от центра обновлений Windows и от служб доставки, за письма соискателей кадровикам, отправляли людям «дополнительную» информацию о COVID-19 и даже приглашения на вечеринку по случаю Хэллоуина. Как и прежде, во вложении пользователей ждал файл с расширением .doc, при открытии которого необходимо разрешить запуск макросов. Главное отличие данной кампании: после запуска макросов пользователи получают оповещение о том, что Word обнаружил ошибку при попытке открыть файл. Этот трюк усыпляет бдительность и вредонос может приступить к выполнению скрытой полезной нагрузки.

Другой не менее интересный и опасный троян BazarLoader тоже ярко проявил себя в IV квартале. Он позволяет получить удаленный доступ к компьютеру жертвы и используется для распространения вымогателя Ryuk. В начале октября исследователи компании ProofPoint обнаружили фишинговую атаку, в которой эксплуатировался интерес к состоянию здоровья Дональда Трампа. В тексте фишингового письма предлагалось перейти по предоставленной ссылке и загрузить документ, размещенный на ресурсах Google. При попытке скачать этот документ на компьютер жертвы загружался исполняемый файл — BazarLoader. В середине октября появилась новая волна фишинговых писем, распространяющих этот вредонос, но уже посредством общедоступных ссылок, ведущих на веб-сервис управления проектами Basecamp. Этот ресурс позволяет загружать в проект любые файлы, в том числе исполняемые, что облегчает задачу злоумышленников. Исследователи компании Sujaх отмечают, что ресурсы этой веб-платформы используются не только для распространения ВПО, но и в фишинговых атаках, направленных на сбор учетных данных.

Новый пик шифровальщиков

Чаще всего под прицелом операторов программ-вымогателей оказывались медицинские и государственные учреждения, а также промышленные предприятия.



Рисунок 10. Распределение атак программ-вымогателей по отраслям

Активность злоумышленников выражалась не только в атаках, но и в создании новых сайтов для публикации украденных данных, к примеру веб-ресурса News & Leaks группировки Mount Locker, и в коллаборации (пример — объединение шифровальщиков Ako и ThunderX под единым брендом Ranzy Locker).

Топ-5 шифровальщиков

1. Ryuk (он же Conti)
2. REvil
3. Clap
4. Egregor
5. DoppelPaymer

Чаще всего злоумышленники, стоящие за шифровальщиком Ryuk, в IV квартале 2020 года атаковали медицинские учреждения. В список пострадавших попали медицинский центр Университета Вермонта, клиники Wyckoff Heights и Sky Lakes, больницы округа Сент-Лоренс в штате Нью-Йорк, гастроэнтерологическая клиника в Неваде, а также диагностический центр Taylor Made Diagnostics. Атаки на медицинские учреждения не проходят бесследно, к примеру систему электронных медицинских карт пациентов с онкологическими заболеваниями в медицинском центре университета Вермонт удалось восстановить только через месяц после атаки, а все время, пока они были недоступны, врачи пытались восстанавливать протоколы химиотерапии по памяти.

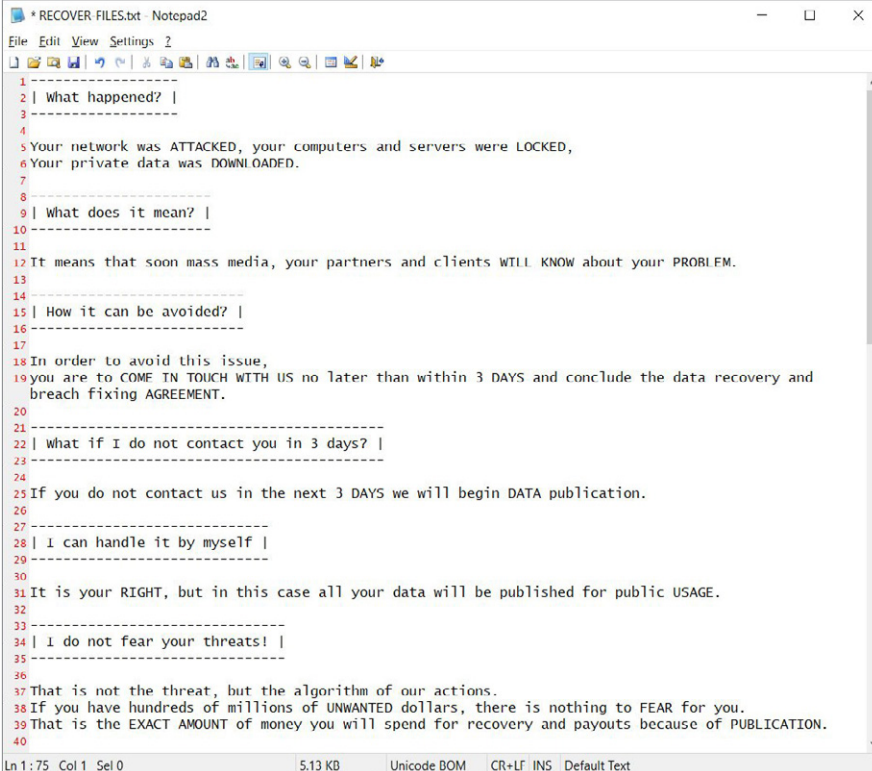
Однако в списке целей у Ryuk не только медицинские клиники. В отчете FS-ISAC Ryuk обозначен как самый распространенный шифровальщик, нацеленный на компании, оказывающие финансовые услуги. Данные отчета подтверждает инцидент, произошедший с платежной системой компании Total System Services. Третья по величине платежная система для финансовых учреждений в Северной Америке в начале декабря подверглась атаке Ryuk. В результате этой атаки было опубликовано более 10 ГБ внутренних данных компании.

Исследователи DFIR проанализировали один инцидент, связанный с деятельностью операторов программы-вымогателя Ryuk, и установили, что злоумышленникам удалось за два часа распространить свое ВПО по всей сети предприятия. Для повышения привилегий в домене хакеры воспользовались уязвимостью CVE-2020-1472. В среднем для реализации атаки оператору программы-вымогателя Ryuk требуется от двух до пяти дней.

В начале декабря дебютировал новый оператор программ-вымогателей — Hades. Первый инцидент, преданный огласке, произошел 15 декабря с транспортно-логистической компанией Forward Air. Атака повлияла на операционные процессы компании и вызвала задержки в обслуживании клиентов, поскольку документы, необходимые для выдачи груза, хранились в электронных системах. Спустя девять дней после инцидента с Forward Air в СМИ появились новости об атаке на другую логистическую компанию — OmniTRAX. На этот раз ответственность за атаку возложена на операторов шифровальщика Conti. В ходе инцидента было похищено более 70 ГБ внутренних документов компании. Известно, что OmniTRAX отказалась платить выкуп.

В случае атаки операторов программ-вымогателей специалисты по ИБ советуют не платить злоумышленникам выкуп, так как это поощряет их преступную деятельность и подтверждает, что они тратят время и силы не зря. Однако не все компании придерживаются этих общих рекомендаций, некоторые идут на поводу у хакеров. Только в последнем квартале минувшего года заплатили выкуп атакованная в середине ноября Ryuk онлайн-школа K12, конгломерат Ansa на Барбадосе, подвергшийся в октябре атаке REvil, школьный округ в штате Миссисипи и округ Делавэр штата Пенсильвания, пораженный DoppelPaymer. Последние две жертвы выплатили злоумышленникам 300 000 и 500 000 долл. США соответственно.

Появившийся в сентябре 2020 года шифровальщик Egregor особенно отличился в конце года. Среди известных жертв этого шифровальщика можно отметить транспортное агентство TransLink, чилийскую международную торговую компанию Cencosud, универмаг Kmart в США, разработчиков игр Ubisoft и Crytek, крупнейший в США книжный магазин Barnes & Noble и крупное кадровое агентство Randstad. В ходе атаки, направленной на Barnes & Noble, были похищены финансовая, аудиторская отчетность и клиентские данные, включающие адреса доставки, адреса электронной почты и историю покупок. Во время инцидента в Cencosud клиенты в течение какого-то времени не могли пользоваться кредитными картами компании, совершить возврат и забрать заказы, оформленные в интернет-магазине.



```

1 -----
2 | What happened? |
3 -----
4
5 Your network was ATTACKED, your computers and servers were LOCKED,
6 Your private data was DOWNLOADED.
7
8 -----
9 | What does it mean? |
10 -----
11
12 It means that soon mass media, your partners and clients WILL KNOW about your PROBLEM.
13
14 -----
15 | How it can be avoided? |
16 -----
17
18 In order to avoid this issue,
19 you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the data recovery and
20 breach fixing AGREEMENT.
21
22 -----
23 | What if I do not contact you in 3 days? |
24 -----
25
26 If you do not contact us in the next 3 DAYS we will begin DATA publication.
27
28 -----
29 | I can handle it by myself |
30 -----
31
32 It is your RIGHT, but in this case all your data will be published for public USAGE.
33
34 -----
35 | I do not fear your threats! |
36 -----
37
38 That is not the threat, but the algorithm of our actions.
39 If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
40 That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.
41

```

Рисунок 11. Записка с требованием выкупа от операторов шифровальщика Egregor

Не пощадили шифровальщики и курорты. В конце октября из-за атаки программы-вымогателя WastedLocker на ресурсы американского оператора горнолыжных и гольф-курортов Boyne Resorts клиенты компании в течение нескольких дней не могли забронировать жилье.

В ноябре была атака шифровальщика REvil на сервис веб-хостинга Managed.com. Системы хостинга были недоступны по меньшей мере четыре дня. Атака затронула сайты клиентов, и по заявлению компании, пострадала вся ее инфраструктура, которая включает в себя управляемые хостинговые решения WordPress и DotNetNuke, почтовые серверы, DNS-серверы, точки доступа RDP, FTP-серверы и сетевые базы данных. Злоумышленники запросили выкуп в размере 500 000 долл. США.

Атаки на промышленные объекты

Промышленность почти на протяжении двух лет держится на втором месте в списке наиболее часто атакуемых отраслей. В четвертом квартале треть всех инцидентов в этой отрасли были совершены с помощью хакинга, в 84% атак применялось вредоносное ПО.

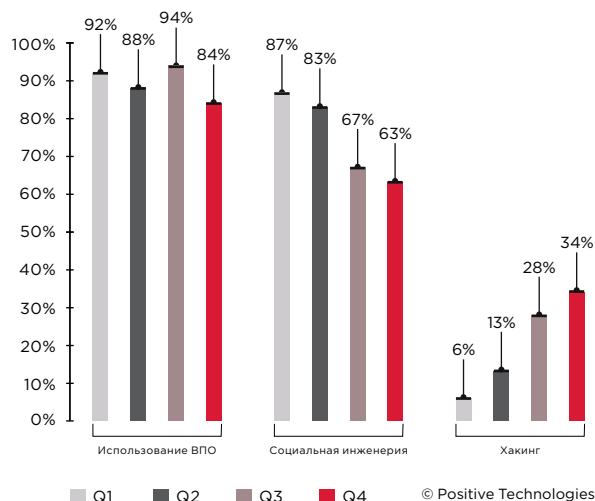


Рисунок 12. Основные методы атак в 2020 году (доля атак на промышленность)

Был зафиксирован всплеск активности группировки RTM: специалисты РТ Expert Security Center обнаружили 61 фишинговую рассылку, которая затрагивала, в числе прочего, и промышленный сектор. Доля атак на промышленные предприятия, в которых использовались банковские трояны, выросла на 26 п. п. — до 59% от общего числа атак с использованием вредоносного ПО.

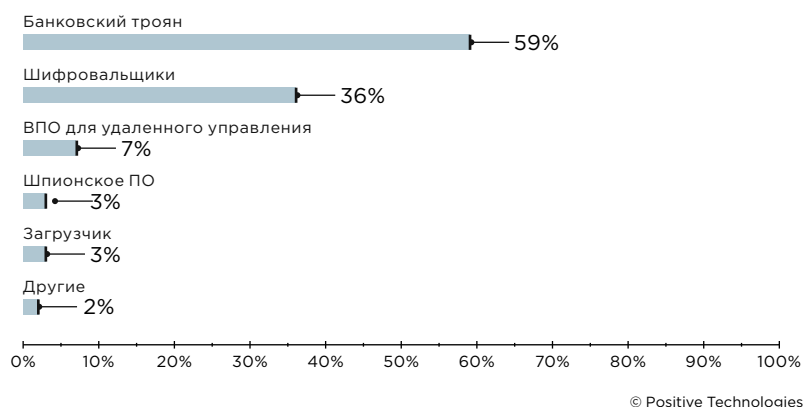


Рисунок 13. Типы вредоносного ПО в атаках на промышленность (доля атак с использованием ВПО)

В последнем квартале 2020 года под шквал атак шифровальщиков попали две авиастроительные компании. Сначала RansomExx атаковал компанию Embraer. В ходе этого инцидента были похищены и впоследствии преданы огласке сведения о сотрудниках, контрактах, данные, полученные в результате имитации полетов, и другая конфиденциальная информация. Затем операторы программы-вымогателя Ragnar Locker, воспользовавшись уязвимостью CVE-2019-19781 в линейке Citrix Application Delivery Controller, проникли в сеть Dassault Falcon Jet и запустили процедуру шифрования. Злоумышленники похитили сведения, относящиеся к коммерческой тайне, в том числе документацию по разработке нового самолета Falcon 6X. Они находились в сети компании больше полугода, изучили инфраструктуру компании и нанесли удар по самым важным ее объектам.

Dassault Falcon Jet — не единственная крупная жертва шифровальщика Ragnar Locker. Первого ноября 2020 года производитель алкогольной продукции Campari Group присоединился к списку его жертв. В ходе атаки было похищено 2 ТБ данных — банковские выписки, электронные письма, коммерческая тайна. Злоумышленники запросили выкуп в размере 15 млн долл. США. За эту сумму они обещали предоставить дешифратор, не распространять украденные сведения, предоставить отчет по проникновению и дать рекомендации по защите.

Еще больший выкуп (34 млн долларов) потребовали операторы программы-вымогателя DoppelPaymer за дешифровку и «молчание» после атаки на производителя электронной техники Foxconn. В ходе атаки они выкрали более 100 ГБ данных. Примечательно, что операторы программы-вымогателя, прокомментировав атаку, подчеркнули, что они специально ограничили атаками на серверы компании, но не атаковали рабочие станции сотрудников.

Энергетическая промышленность также не осталась в стороне. Кибератака, которую хакеры провели 13 октября в городе Мумбаи, привела к отключению электроэнергии на два часа. Объектом атаки стала городская электроподстанция. Перебои электроснабжения сказались на работе фондовой биржи и коммерческих предприятий в районах Мумбаи, Тханы и Нави-Мумбаи, а также привели к отмене движения поездов. В медицинских учреждениях Мумбаи могли продолжать работу только отделения интенсивной терапии, остальным пришлось приостановить работу. В середине ноября операторы программы-вымогателя Clor атаковали промышленную компанию Parkland в городе Калгари. В результате была похищена конфиденциальная информация, в том числе документы, касающиеся работы нефтеперерабатывающего завода, и персональные данные сотрудников, к примеру скан паспорта одного из директоров. Стоит отметить, что на киберполигоне The Standoff в ноябре 2020 года риск утечки конфиденциальных документов предприятия, связанного с добычей нефти, был одним из самых часто реализуемых.

В ноябре 2020 года в Израиле была взломана SCADA-система для управления одним из резервуаров системы водоснабжения. Получение подобного доступа позволяет злоумышленникам вносить любые коррективы в параметры объекта критически значимой инфраструктуры, например увеличить давление в резервуаре, приведя его к разрыву или увеличить температуру до критических значений. Изначальный доступ был получен из-за подключения элементов АСУ ТП к интернету и отсутствия аутентификации. После публикации злоумышленником видео взлома была включена аутентификация, однако компоненты технологической сети все еще доступны из интернета, а значит хакеры могут атаковать снова.

Атаки по цепочке

Атаки на поставщиков программного обеспечения стали одним из трендов IV квартала. Самое нашумевшее событие — [атака на клиентов компании SolarWinds](#), в числе которых Государственный департамент США, компании Microsoft, Cisco и FireEye. Это была так называемая атака на цепочку поставок (supply chain attack). Проникнув в сеть SolarWinds, злоумышленники добавили в обновление для платформы Orion вредоносный бэкдор-модуль, а 18 000 клиентов, ничего не подозревая, установили эту версию. Отдельно отметим, что в ходе атаки на компанию FireEye были похищены принадлежащие ей инструменты для проведения тестов на проникновение. Украденное ПО содержит эксплойты для множества уязвимостей, поэтому злоумышленники с большой вероятностью будут использовать его в будущих кампаниях.

В ноябре злоумышленники провели [фишинговую атаку на регистратор доменных имен GoDaddy](#). В ходе атаки преступникам удалось убедить сотрудников компании в том, что необходимо внести изменения в регистрационные записи нескольких организаций-клиентов. В этот список попали две криптовалютные биржи — [NiceHash](#) и [Liquid](#). Внесенные в их записи изменения позволили организовать перенаправление пользовательского трафика бирж на подконтрольные злоумышленникам серверы.

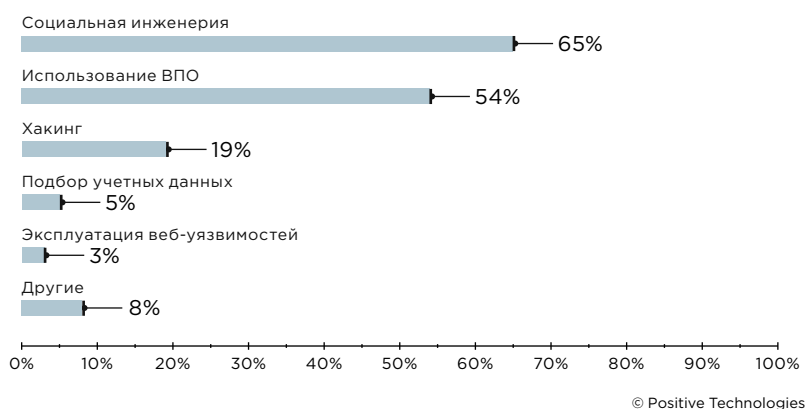


Рисунок 14. Методы атак (доля атак на IT-компании)

Техники социальной инженерии в этом квартале пользовались особой популярностью, их доля составила 65% в атаках, направленных на IT-сферу. К примеру, с помощью фишингового письма, адресованного сотруднику японской IT-компании Коеи Тесто, [хакер взломал сайт компании](#) и украл данные 65 000 пользователей. После атаки хакер попытался продать доступ (бэкдор) и украденную базу данных пользователей форума за 7800 долл. США. Однако спустя пять дней база данных была выложена в сеть абсолютно бесплатно.

Еще один крупный японский разработчик игр Capcom в начале ноября [был атакован оператором программы-вымогателя Ragnar Locker](#). Компания до последнего отрицала факт получения злоумышленниками доступа к клиентским данным, однако операторы шифровальщика выложили на своем сайте подтверждение. В итоге стало известно, что украдены персональные данные сотрудников компании (в том числе — бывших), включая их паспортные данные, данные клиентов и деловых партнеров, отчеты о продажах, документы,

касающиеся новых разработок, и прочая конфиденциальная информация. На этом атаки шифровальщиков на IT-компании не закончились. В конце декабря группировка Pay2Key атаковала израильскую компанию Portnox, которая занимается информационной безопасностью. Перед тем как зашифровать IT-инфраструктуру, хакеры похитили конфиденциальные сведения, в том числе касающиеся клиентов компании; к примеру, злоумышленники опубликовали отчет об аудите безопасности крупной израильской оборонной компании Elbit. В общей сложности был похищен 1 ТБ информации.

Нельзя не упомянуть атаку операторов программы-вымогателя Clop, направленную на второго по величине поставщика программного обеспечения в Германии — Software AG. В ходе этой атаки были скомпрометированы файлы компании и информация о сотрудниках. За неразглашение данных операторы Clop потребовали выкуп в 23 млн долларов.

Опасный шоппинг

В IV квартале количество атак на компании из сферы торговли выросло на 56% в сравнении с прошлым кварталом и является абсолютным максимумом за последние два года.

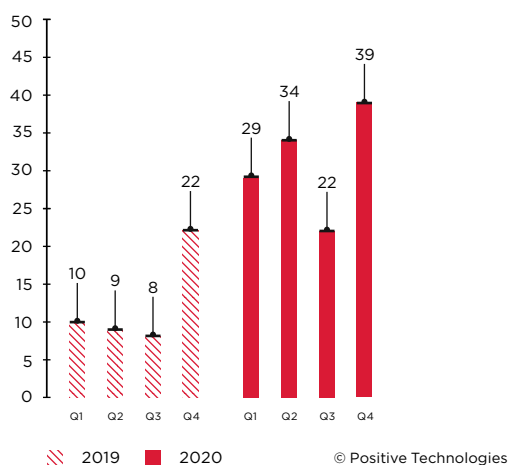


Рисунок 15. Количество атак на торговые предприятия

Чаще всего в ходе атак на эту отрасль злоумышленники похищают данные платежных карт. К примеру, с октября по декабрь 2020 года их доля среди всей украденной информации составила 33%. На втором месте по популярности персональные данные (27%), а на третьем — учетные данные (20%).

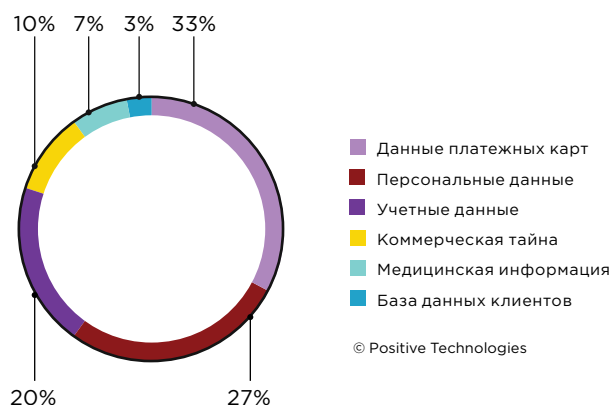


Рисунок 16. Данные, украденные в ходе атак на торговые компании

В 31% инцидентов в этой сфере были задействованы программы-вымогатели. Яркий пример — атака на южнокорейского ретейлера E-Land, которая имела место 22 ноября. В ходе расследования оказалось, что киберпреступники находились в сети компании больше года и все это время извлекали данные кредитных карт клиентов с помощью вредоносного ПО, внедренного в POS-терминалы. Узнать об этом инциденте удалось только после того, как операторы Clor запустили свою программу-вымогателя. В результате компания E-Land закрыла 23 магазина. Злоумышленники не получили доступа к CVC/CVV-кодам, однако текущий объем похищенных данных позволяет создавать поддельные карты.

Каждый пятый инцидент (23%) составили атаки типа Magecart. В этих атаках интересней всего рассмотреть способы их сокрытия. Например, исследователи компании Sansec обнаружили веб-скиммеры, размещенные в CSS-коде на сайтах трех интернет-магазинов. Подобный способ размещения вредоносного ПО позволяет избежать обнаружения, так как этот код не проверяется сканерами безопасности, а при ручной проверке скрипта на него мало кто обратит внимание. Запуск скрипта происходил только с того момента, как клиенты взломанного ресурса начинали вводить данные платежных карт или другую личную информацию.

Другой не менее изощренный способ сокрытия скиммера был также обнаружен сотрудниками компании Sansec и заключался в размещении вредоносной полезной нагрузки в виде SVG-кнопок социальных сетей. Таким образом, код скрипта веб-скиммера расположен в HTML-разметке, а декодер злоумышленники могут намерено разместить в другом месте, так как в случае обнаружения только одного из компонентов вредоноса специалист по безопасности может сделать вывод о неактивности ВПО.

Злоумышленники не прошли мимо «черной пятницы», более чем на 50 сайтах интернет-магазинов был обнаружен самовосстанавливающийся скиммер. Скрипт скиммера запускал для пользователя поддельные формы оплаты в скомпрометированных интернет-магазинах, а собранные данные из этих форм отправлял на настоящую страницу оплаты. Такой механизм с высокой точностью копирует нормальный поток транзакции, как если бы он проходил без вмешательства злоумышленников, из-за чего системы безопасности не выдают оповещений об аномальном поведении.

Для обеспечения бесперебойной работы злоумышленники размещали на взломанных веб-ресурсах четыре полезные нагрузки:

- 1) бэкдор-загрузчик, устанавливающий скиммер;
- 2) сторожевой бэкдор, восстанавливающий бэкдор-загрузчик в случае его обнаружения и удаления;
- 3) сам веб-скиммер;
- 4) инфостилер для кражи учетных данных администратора.

Таким образом, даже в случае раскрытия всей цепочки заражения и способов восстановления инфостилер обеспечивал хакеров постоянным доступом к серверам и позволял заново развернуть все нагрузки. Само по себе это заражение стало возможным из-за использования магазинами платформы Magento версий 2.2.3—2.2.7, несмотря на то, что всем магазинам, работающим на этой платформе, были направлены уведомления о необходимости перехода на новую версию.

Даже если сайт онлайн-магазина не был взломан злоумышленниками, клиенты все равно могут не получить желаемый товар, например из-за атаки на другое звено цепочки поставок — службу доставки. Подобный инцидент произошел с российским сервисом доставки PickPoint. Четвертого декабря хакер взломал сеть постаматов компании и дистанционно открыл 2732 ячеек в Москве и Санкт-Петербурге. На восстановление системы доставки ушло несколько дней.

Предвыборная суэта

В конце 2019 года сотрудники Positive Technologies делились своими прогнозами о ситуации в киберпространстве в 2020 году. Они опасались, что будет много кибератак на фоне подготовки к президентским выборам в США, в том числе направленных на сайты политических партий и кандидатов. Так и случилось.

В конце октября хакеры украли 2,3 млн долларов со счета Республиканской партии штата Висконсин. Злоумышленники провернули эту атаку, манипулируя счетами от четырех поставщиков, обеспечивающих партию маркетинговыми материалами и осуществляющих доставку корреспонденции. Пресс-секретарь Демократической партии в штате Висконсин заявила, что было предпринято более 800 попыток фишинговых атак за всю предвыборную кампанию, но стоит отметить, что, по ее словам, ни одна из них не увенчалась успехом.

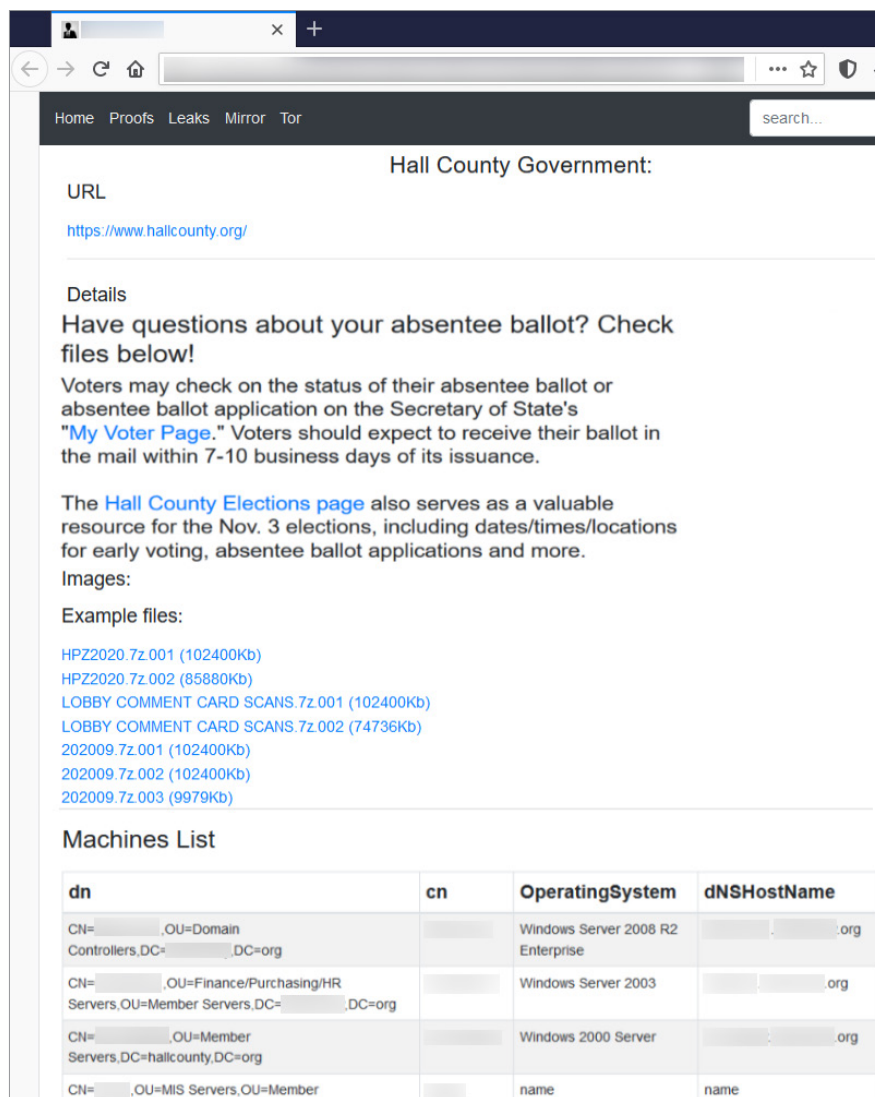


Рисунок 17. Объявление о данных жителей округа Холл, украденных вымогателем DoppelPaymer

Кибератаки затронули не только представителей власти, но и обычных людей. Седьмого октября 2020 года злоумышленники-вымогатели из группировки DoppelPaymer похитили данные избирателей штата Джорджия в ходе атаки на сеть и телефонные системы округа Холл. В начале ноября была замечена фишинговая атака, в ходе которой злоумышленники под видом документа, раскрывающего факт вмешательства в выборы, распространяли вредонос Qbot. Попав на компьютер жертвы, это ВПО начинает собирать пользовательские данные и личную переписку для последующего использования в новых атаках.

Не устояли и системы поддержки выборов: хакеры смогли получить к ним доступ, проэксплуатировав уязвимость CVE-2018-1337 в FortiOS SSL VPN и уязвимость Windows CVE-2020-1472.

Злоумышленники, стоящие за трояном Emotet, и в этой ситуации не остались в стороне. В одной из октябрьских фишинговых атак они выдавали себя за Демократическую партию США. Основная тематика писем — поиск волонтеров, а во вложении заботливо прикреплен файл с инициативами партии.

Открытие файла сопровождалось появлением оповещения, что он был создан на устройстве с операционной системой iOS и для дальнейшего просмотра необходимо «включить контент». Разблокирование контента приводило в действие механизм заражения.

Тысяча и один способ эксплуатировать COVID-19

Доля атак с использованием техник социальной инженерии, в которых затронута тема пандемии, держалась на уровне третьего квартала и составила 4,6%. Несмотря на обилие информации по теме коронавирусной инфекции в интернете, злоумышленникам по-прежнему удается завлечь жертв фишинговыми письмами, в которых они обещают рассказать особо ценную информацию. К примеру, в одной из фишинговых атак письмо имитировало автоматическое сообщение от SharePoint, оповещающее об отправленном пользователю документе с требованиями в связи с пандемией. Для просмотра этого файла пользователям предлагалось перейти по ссылке, которая вела на мошеннический сайт.

Еще одна популярная уловка — использовать тему полагающейся пользователю компенсации. В конце октября мошенники с целью сбора информации отправляли оповещения от лица Международного валютного фонда о том, что жертва включена в список 125 «счастливчиков», которым будет выплачена компенсация из-за пандемии. Все, что нужно для ее получения, — это дать ответ, указав свою личную почту, и предоставить дополнительные сведения по запросу. Цель атаки — собрать как можно больше пользовательских данных. Отдельного внимания заслуживает защита этой атаки от обнаружения: во-первых, письмо не содержало никаких ссылок; во-вторых, адрес для ответа отличался от адреса отправителя; в-третьих, письмо выглядело как часть цепочки писем.

В декабре мошенники представлялись сотрудниками департамента труда штата Нью-Йорк и гарантировали выплаты материальной помощи в размере 600 долларов в связи с трудной ситуацией, вызванной пандемией. Однако для этого в срочном порядке нужно было предоставить персональные данные, указав их в специальной форме на сайте.

Другая фишинговая атака эксплуатировала интерес жертв-получателей к результатам теста на COVID-19. Письмо содержало защищенный паролем RAR-архив с вредоносным содержимым. Кстати, это еще одна проверенная техника сокрытия атаки: не все средства защиты могут проверить подобный архив.

Фишинг с упоминанием вакцины от COVID-19 составил около 40% от числа всех фишинговых атак на тему пандемии в IV квартале 2020 года. Яркой иллюстрацией статистики является декабрьская фишинговая кампания, обнаруженная исследователями компании KnowBe4. Толчком для ее начала послужило сообщение в СМИ о том, что один из производителей вакцины не сможет поставлять дополнительные дозы в США. Злоумышленники, воспользовавшись паникой, разослали письма, содержащие ссылку на форму, заполнив которую жертва якобы точно попала бы в список на вакцинацию. Для просмотра формы пользователям необходимо было пройти процедуру аутентификации на веб-ресурсе, имитирующем легальный облачный сервис.

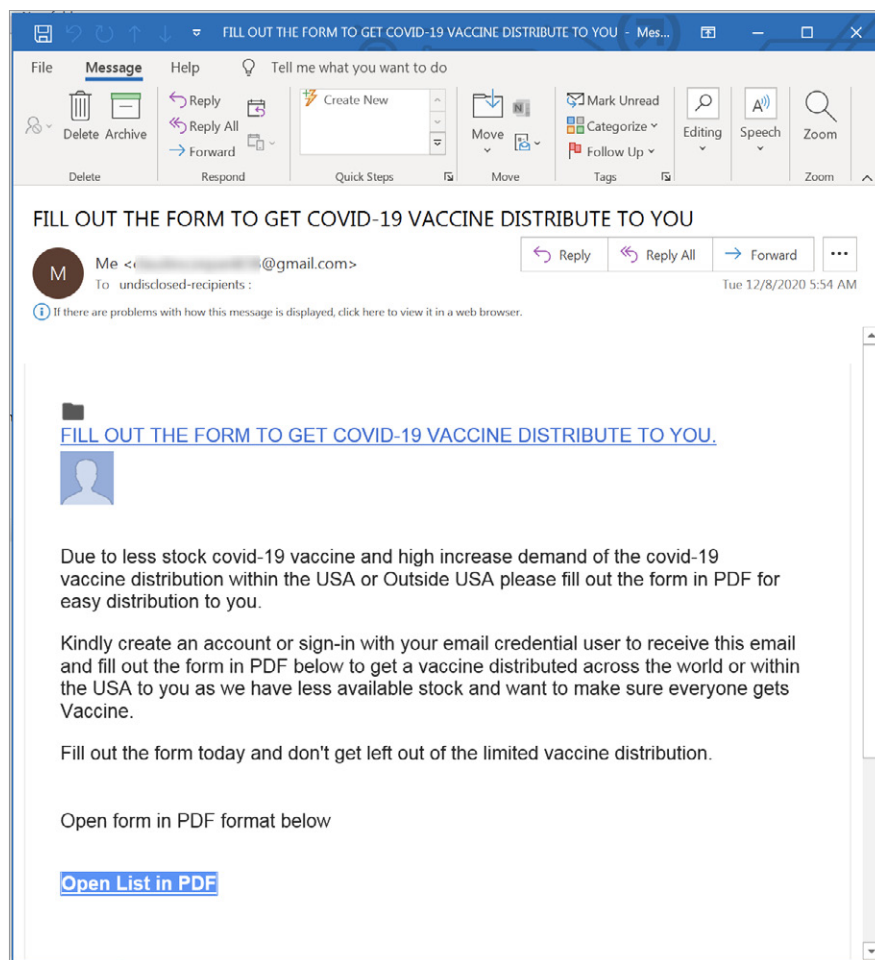


Рисунок 18. Образец фишингового письма, эксплуатирующего интерес к теме вакцины

Интерес к вакцине питают не только обычные интернет-пользователи, но и киберпреступники. На протяжении всего квартала мы наблюдали атаки на цепочку производства и поставки вакцины. Под шквал атак попали фармацевтические компании Fareva, Dr. Reddy's, Johnson & Johnson, Novavax, Genexine, Shin Poong Pharmaceutical, Celltrion и AstraZeneca. Досталось и американской логистической компании Americold, мощности которой планируют использовать для хранения готовых партий вакцин: предположительно, она была атакована операторами программы-вымогателя. Кибератаки нацелены и на государственные учреждения, которые участвуют в принятии решений о вакцинах. В начале декабря, например, жертвой атаки стало Европейское агентство лекарственных средств, в ходе инцидента были похищены документы зарегистрированных производителей вакцин Pfizer и BioNTech.

Об исследовании

Данный отчет содержит информацию об общемировых актуальных угрозах информационной безопасности. Он основан на собственной экспертизе компании Positive Technologies, результатах многочисленных 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 привлечь 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
pt@ptsecurity.com
[facebook.com/](https://facebook.com/PositiveTechnologies)
[PositiveTechnologies](https://facebook.com/PHDays)
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.