



PT

Актуальные киберугрозы

II квартал 2019 года

ptsecurity.com

Содержание

Тренды и прогнозы	4
Сводная статистика	5
Динамика атак	8
Методы атак	9
Использование вредоносного ПО	9
Социальная инженерия	10
Хакинг	11
Эксплуатация веб-уязвимостей	11
Подбор учетных данных	13
Категории жертв	14
Государственные организации	15
Промышленные компании	16
Медицинские учреждения	17
Финансовые организации	18
IT-компании	20
Как защититься организации	21
Как вендору защитить свои продукты	23
Об исследовании	25

Обозначения

Объекты атак



Компьютеры, серверы
и сетевое оборудование



Веб-ресурсы



Люди



Банкоматы и POS-терминалы



Мобильные устройства



IoT

Методы атак



Использование
вредоносного ПО



Подбор учетных данных



Социальная инженерия



Хакинг



Эксплуатация
веб-уязвимостей

Категории жертв



Финансовая отрасль



Государственные учреждения



Медицинские учреждения



Наука и образование



Оборонные предприятия



Промышленные компании



Онлайн-сервисы



Сфера услуг



Транспорт



IT-компании



Торговля



Частные лица



Телекоммуникационные
компании



Блокчейн-проекты



Другие сферы



Что такое киберугроза

Стремительная информатизация общества оказывает положительное влияние на многие сферы экономики: финансовую отрасль, торговлю, промышленность, здравоохранение, образование, науку. Сегодня информационные технологии — это неотъемлемая часть не только успешного бизнеса, но и государственной политики. Однако преступники научились использовать их в своих целях, что дало начало противостоянию со специалистами по информационной безопасности. Эта борьба способствует постоянному совершенствованию методов и инструментов, которые используют злоумышленники, что неминуемо порождает рост числа киберугроз.

Киберугроза — это совокупность факторов и условий, создающих опасность нарушения информационной безопасности. В нашем исследовании 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 компании, рабочие компьютеры, мобильные устройства, другие технические средства и, наконец, на человека как на элемент киберпространства.

Тренды и прогнозы

Компания Positive Technologies продолжает следить за актуальными угрозами информационной безопасности. Киберпреступники не сдают позиций, быстро реагируют на известия о новых уязвимостях, адаптируются к изменяющемуся курсу криптовалют и продолжают совершенствовать методы атак.

Подводя итоги II квартала 2019 года, мы отмечаем следующие тенденции:

- Количество уникальных киберинцидентов остается высоким и на 3% превзошло показатель I квартала.
- Целенаправленные атаки преобладают над массовыми, их доля составила 59%, что на 12 процентных пунктов больше, чем в I квартале.
- Более половины всех киберпреступлений совершаются с целью кражи информации. Прямая финансовая выгода интересует злоумышленников в 42% атак против частных лиц и в 30% атак на юридические лица.
- Персональные данные — основной тип украденной информации в атаках на юридические лица (29%). Частные лица наиболее часто рискуют учетными записями и данными своих банковских карт (44% и 34% соответственно от всего объема информации, украденной у частных лиц).
- Благодаря уверенному росту курса биткойна объемы скрытого майнинга выходят на прежний уровень.
- Атаки MageCart на онлайн-ресурсы набирают обороты. Специалисты отмечают вредоносные JavaScript-снифферы, в том числе и на сайтах без функции оплаты.
- Растет доля заражений вредоносным ПО среди государственных учреждений (62% против 44% в I квартале 2019 года). Наиболее часто в минувшем квартале государственные учреждения подвергались атакам троянов-шифровальщиков.
- Группировка RTM продолжает активно атаковать промышленный сектор как одну из слабо защищенных отраслей. В то же время, будучи финансово мотивированной, группа RTM не теряет надежды сорвать банк и совершает попытки атак на финансовые организации.
- IT-компании нередко становятся промежуточным звеном в атаках supply chain. Почтовые адреса взломанных поставщиков IT-услуг активно используются хакерами для фишинговых рассылок.

Сводная статистика

Кража информации по-прежнему остается приоритетной целью большинства кибератак. Что касается финансовой выгоды, то ее злоумышленники преследуют в 30% и 42% атак на юридические лица и частных лиц соответственно. Высокая доля финансово мотивированных атак на частных лиц объясняется регулярными массовыми заражениями вредоносным ПО с навязчивой рекламой (в том числе на мобильных устройствах), заражением майнерами и другим ВПО на сомнительных сайтах, а также вымогательскими кампаниями, в ходе которых злоумышленники угрожают распространить компрометирующую информацию о человеке.

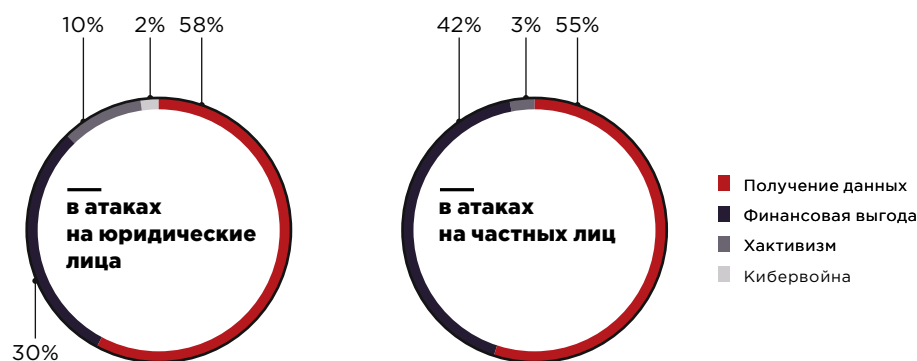


Рисунок 1. Мотивы злоумышленников

Персональные и учетные данные чаще всего интересуют злоумышленников, когда они атакуют юридические лица. Это неудивительно, ведь в компаниях могут храниться большие базы как персональных, так и учетных данных клиентов. Кроме того, злоумышленники могут быть заинтересованы в учетных данных сотрудников компании-жертвы.

Под угрозой и учетные записи в социальных сетях, особенно если аккаунт хорошо «раскручен», то есть имеет большое число подписчиков. Пользователи, в свою очередь, далеко не всегда заботятся о безопасности аккаунтов: используют нестойкие и одинаковые пароли, вводят учетные данные, не удостоверившись в надежности ресурса, выдают информацию о себе, которая может помочь подобрать пароль. Это объясняет высокую долю украденных учетных данных (44%) в атаках на частных лиц. Например, к категории людей, входящих в зону повышенного риска атак со стороны хакеров, относятся любители компьютерных игр. Так, во II квартале злоумышленники заманивали пользователей Steam на веб-ресурсы, где якобы бесплатно можно получить новую игру, введя учетные данные от аккаунта в Steam. Кроме того, попасться на удочку злоумышленников геймеры могут и на специализированных форумах. Так, под видом чит-кодов, упакованных в ZIP-архив, ряд веб-ресурсов распространяли троян для майнинга криптовалюты TurtleCoin.

Данные банковских карт и платежная информация клиентов, как правило, защищены криптографическими методами, поэтому злоумышленникам проще узнать их с помощью методов социальной инженерии напрямую у клиента. Как следствие, 34% украденных в результате атак на частных лиц данных — это данные их банковских карт.

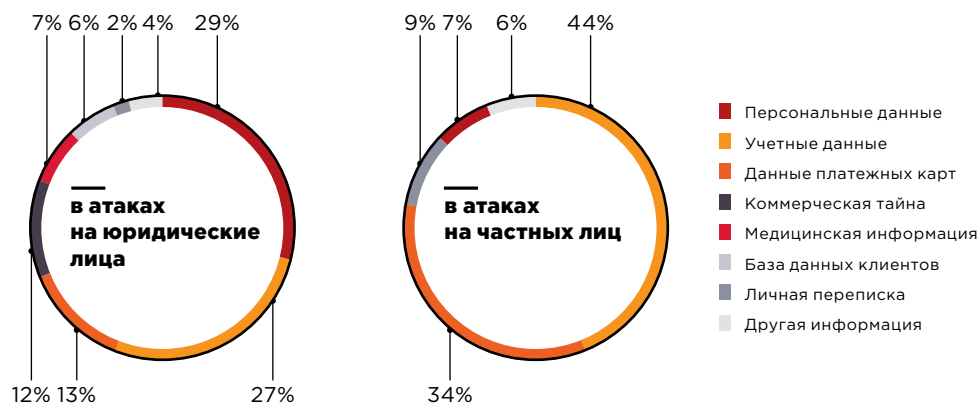


Рисунок 2. Типы украденных данных

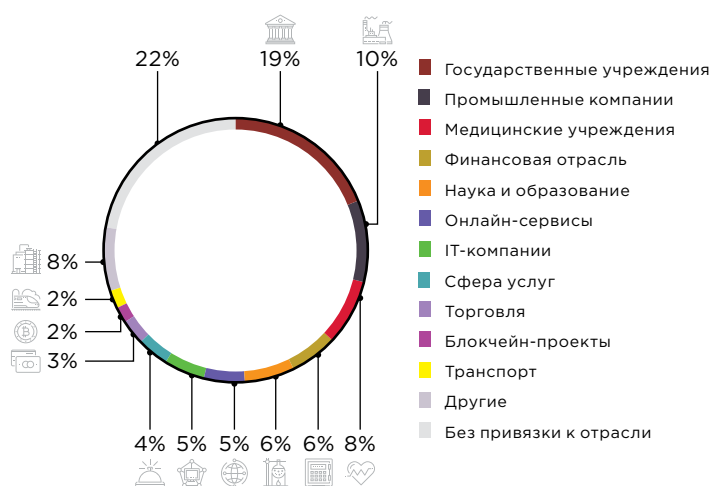


Рисунок 3. Категории жертв среди юридических лиц

Во II квартале 2019 года доля целенаправленных атак существенно выросла по сравнению с I кварталом и составила 59% (в I квартале — 47%). Доля киберинцидентов, в результате которых пострадали частные лица, составила 24%. Среди юридических лиц (см. рисунок 3) наиболее часто злоумышленники атаковали государственные организации, промышленные компании, медицинские организации, банки и другие организации финансовой сферы. Во II квартале мы отмечаем атаки supply chain на крупные IT-компании с большим числом клиентов из различных отраслей, поэтому далее мы рассмотрим некоторые атаки более подробно.

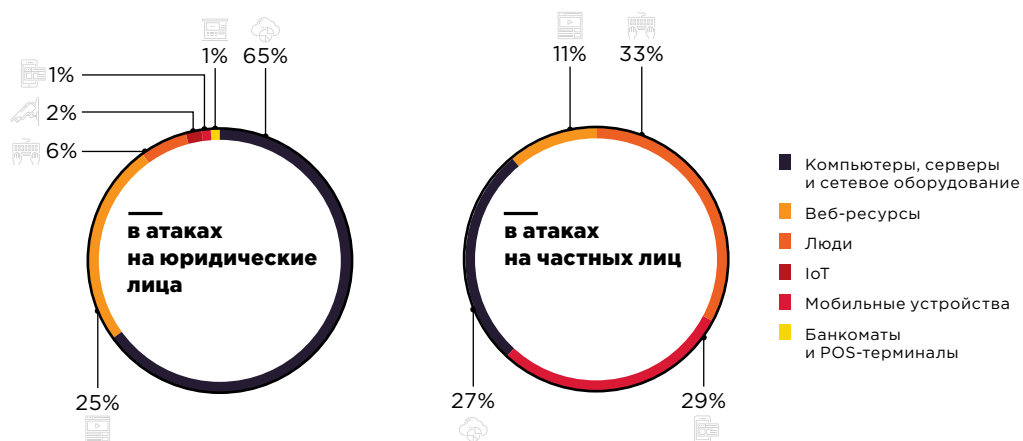


Рисунок 4. Объекты атак

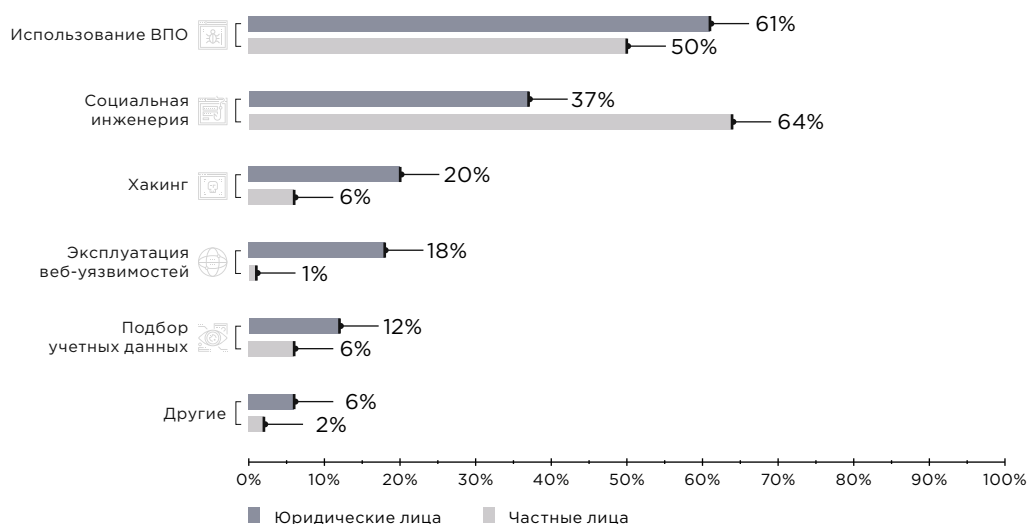


Рисунок 5. Методы атак

		Отрасль												
Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) внутри отраслей		Государственные учреждения	Финансовая отрасль	Промышленные компании	Медицинские учреждения	Онлайн-сервисы	Сфера услуг	IT-компании	Наука и образование	Торговля	Транспорт	Блокчейн-проекты	Другие	Без привязки к отрасли
Всего атак		53	16	27	22	14	10	14	17	9	5	5	21	60
Объект	Компьютеры, серверы и сетевое оборудование	37	14	26	11	5	4	10	8	2	3	4	15	39
	Веб-ресурсы	9	1	1	5	8	5	4	9	7	2		5	13
	Люди	5			6	1						1	1	2
	Мобильные устройства	2												1
	Банкоматы и POS-терминалы		1				1							
	IoT													5
Метод	Использование ВПО	33	14	26	9	2	2	6	7	2	2	1	13	48
	Социальная инженерия	22	11	21	8	1	1		3	2	1	1	9	15
	Подбор учетных данных	6		1	4	2	4	3	3	1			3	7
	Хакинг	6	1	1	1	2	2	5	1		1	4	1	29
	Эксплуатация веб-уязвимостей	6		2	2	8	3	3	5	6	1		4	9
	Другие	7	1			2		1	1			1	1	1
Мотив	Финансовая выгода	19	6	1	6	2	1	5	1	1	1	4	8	28
	Получение данных	25	10	25	16	10	9	9	13	8	2	1	7	24
	Хактивизм	6		1		2			3		2		5	8
	Кибервойна	3											1	

Градации цвета показана доля атак внутри одной отрасли

Динамика атак

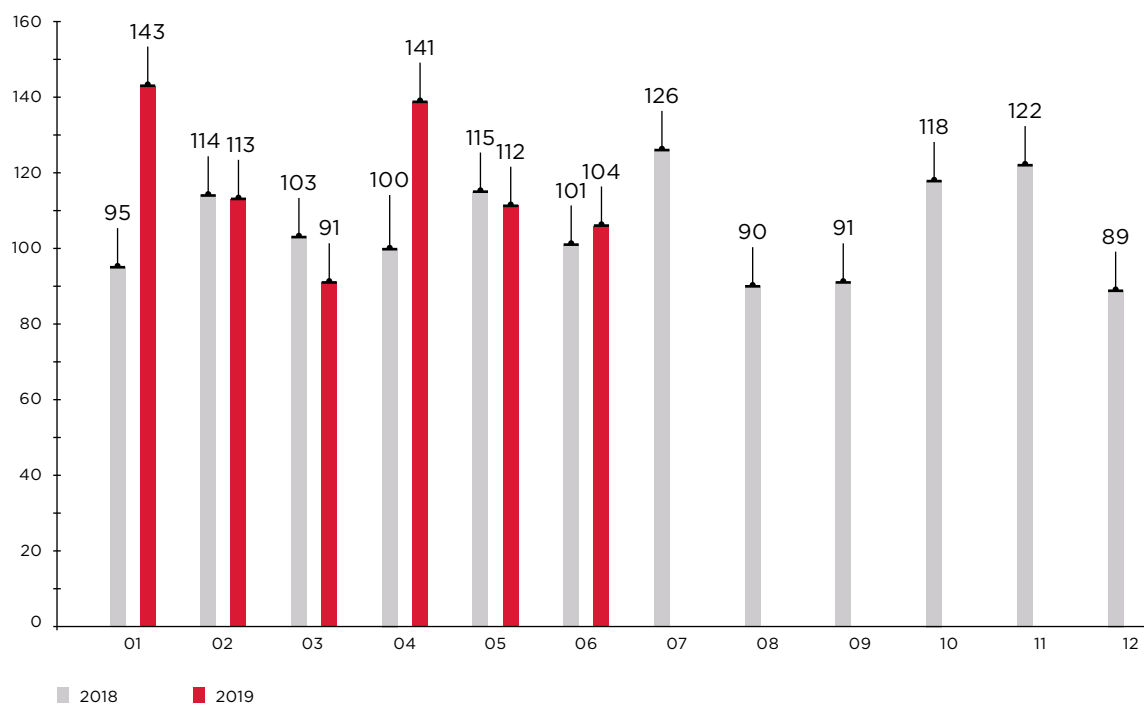


Рисунок 6. Количество инцидентов в 2018 и 2019 годах (по месяцам)

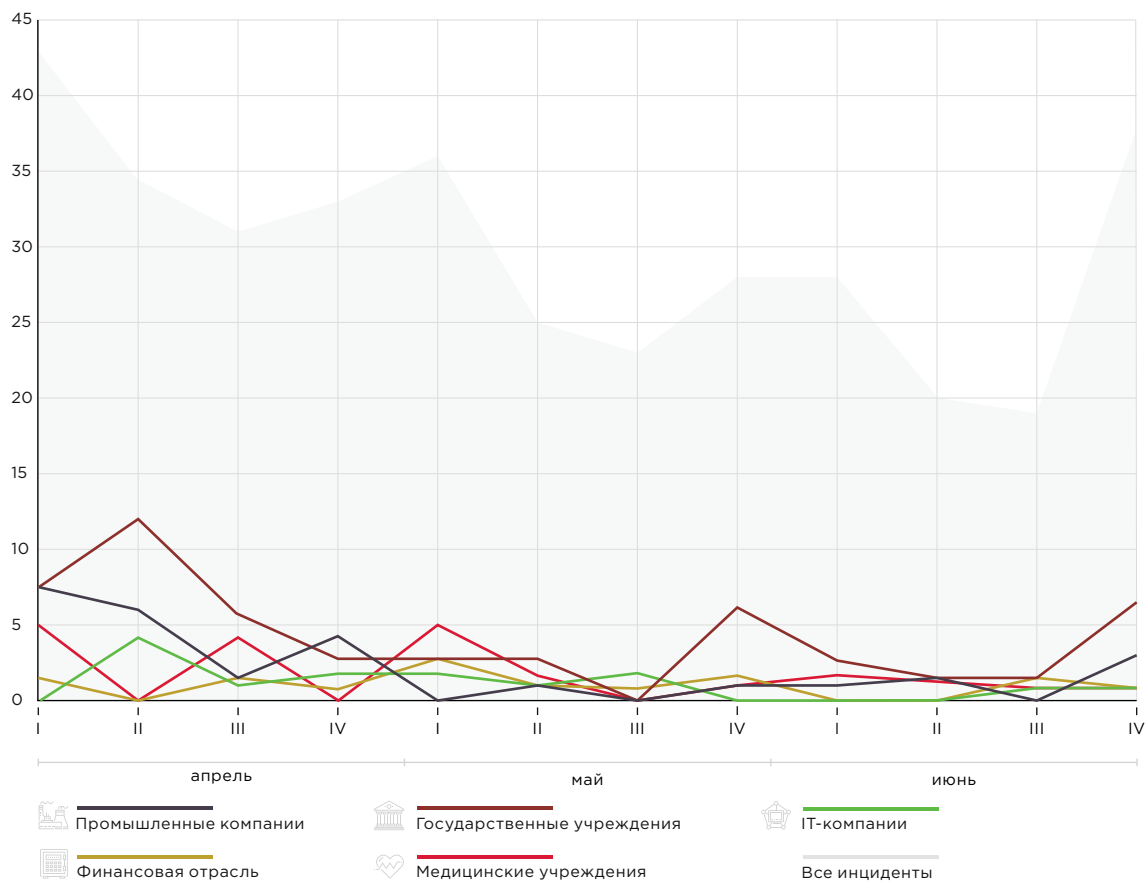


Рисунок 7. Количество инцидентов во II квартале 2019 года (по неделям)

Методы атак

Остановимся подробнее на каждом методе и укажем, какие объекты и отрасли больше других страдали от этих категорий атак.

Использование вредоносного ПО

Доля многофункциональных троянов продолжает расти. Например, модульный троян DanaBot, о котором мы [писали](#) в I квартале, теперь [способен](#) выполнять роль шифровальщика. Активность одного из самых распространенных шифровальщиков GandCrab, напротив, пошла на спад, и его операторы [заявили](#) о завершении вредоносной кампании. Спустя несколько недель после новости о прекращении развития трояна-вымогателя стало известно, что специалисты по кибербезопасности получили [доступ](#) к серверам GandCrab, а вместе с ним и ключи шифрования, благодаря чему была создана программа-дешифровщик для последней версии GandCrab, позволяющая восстанавливать зашифрованные им файлы.

Несмотря на эти события, доля атак троянов-вымогателей остается высокой. Это объясняется тем, что для создания простого шифровальщика не требуется разрабатывать уникальный код. Большинство новых экземпляров вымогателей очень похожи на своих предшественников, поскольку зачастую киберпреступники не разрабатывают шифровальщик с нуля, а приобретают готовый код или подписку (ransomware as a service) в дарквебе. Таким образом, при минимальном стартовом капитале шифровальщики могут приносить владельцам неплохой доход.

С апреля 2019 года периодически появляются [сообщения](#) об атаках нового криптовымогателя Sodinokibi. Жертвами стали уже как минимум три провайдера IT-услуг. Киберпреступники использовали инструменты удаленного администрирования (Webroot и Kaseya) для заражения шифровальщиком компаний — клиентов скомпрометированных поставщиков IT-услуг. Однако атаки supply chain — не единственный вектор распространения Sodinokibi. Троян распространяется также через уязвимости в [Oracle WebLogic Server](#) и фишинговые [письма](#).

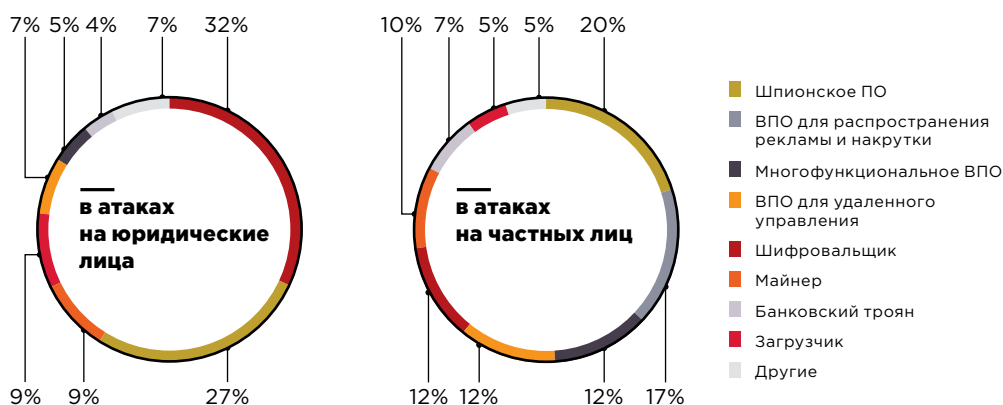


Рисунок 8. Типы вредоносного ПО

Наиболее популярным способом доставки вредоносного ПО остается электронная почта. Во II квартале специалисты отмечают участвовавшие случаи распространения троянов посредством файлов в формате ISO (цифровых образов компакт-дисков). Например, так распространяются [AgentTesla](#), [LokiBot](#), [NanoCore](#). ISO-образы зачастую не детектируются антивирусными решениями, поскольку могут быть включены в белые списки. Заподозрить неладное можно по размеру файла — вредоносное вложение имеет размер не более 2 МБ, в то время как легитимный ISO-образ, как правило, значительно больше.

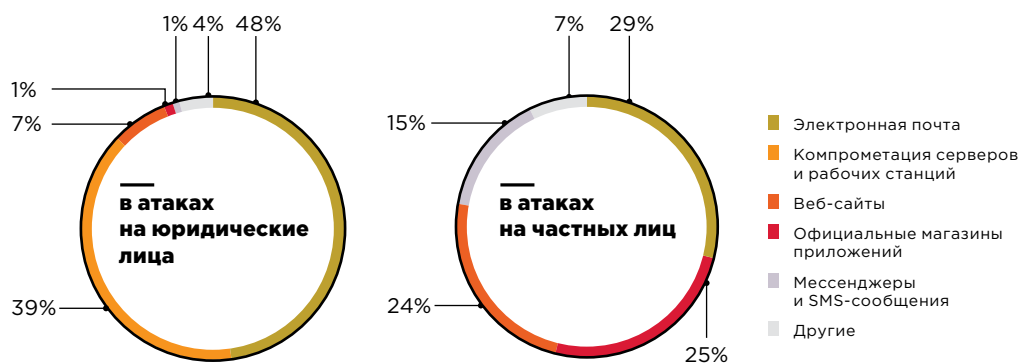


Рисунок 9. Способы распространения ВПО

Во втором квартале 2019 года мы отмечаем вернувшийся интерес злоумышленников к криптоджекингу. Курс биткойна уверенно растет, и злоумышленники продолжают развивать ПО для скрытого майнинга. Так, специалисты Sucuri обнаружили образец майнера с улучшенными механизмами для закрепления в инфраструктуре: специальный cron-скрипт (сценарий для выполнения определенных действий по расписанию) позволяет восстановить процесс майнинга даже в случае, если основной модуль ВПО был обнаружен и удален из зараженной системы.

Во II квартале злоумышленники активно распространяли инфостилер AZORult. Например, в апреле эксперты Positive Technologies Expert Security Center (PT ESC) отмечали, что группировка RTM стала использовать AZORult вместо Pony. Кроме того, троян AZORult распространяется через веб-сайты под видом различных утилит (например, под видом утилиты для очистки и оптимизации работы ОС G-Cleaner или VPN-клиента Pirate Chick).

Социальная инженерия

Во II квартале киберпреступники активно использовали набор сервисов Azure App Service для различного рода мошенничества с применением методов социальной инженерии. Например, сервис Azure задействуется для быстрого развертывания фишинговых страниц с поддельными формами аутентификации и для создания поддельных страниц службы технической поддержки Microsoft со всплывающими сообщениями о том, что компьютер посетителя сайта якобы заражен вирусом. Кроме того, злоумышленники рассылают письма, в которых предлагают скачать файл, авторизовавшись через поддельную форму, предварительно размещенную на платформе Azure Blob Storage. Масштабу и успеху подобного рода мошеннических операций способствует домен windows.net в адресной строке и действующий SSL-сертификат Microsoft. Однако схема кражи учетных данных не является новой, и существуют специальные инструкции для пользователей, которые помогают настроить автоматическое блокирование подобных фишинговых писем.

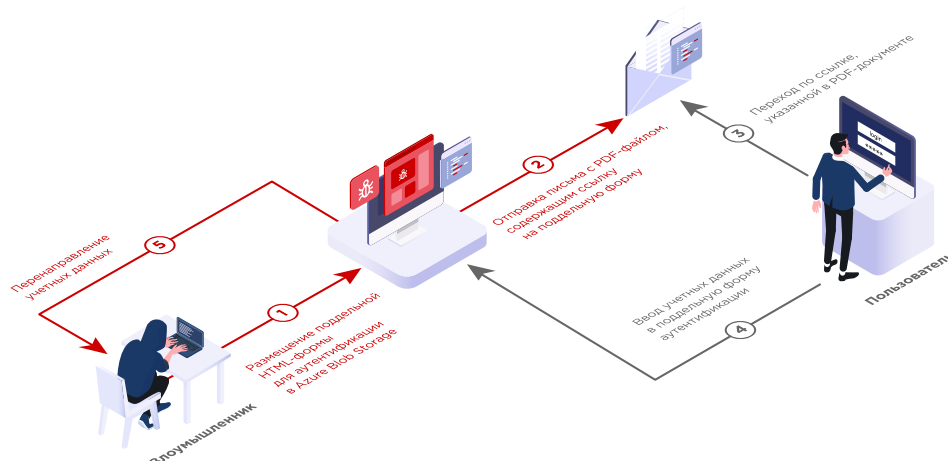


Рисунок 10. Схема кражи учетных данных аккаунтов в Office 365 с использованием Azure Blob Storage

Как уже отмечалось, стремительный рост курса биткойна во II квартале привел к росту интереса к криптовалюте, на чем и пытаются заработать некоторые злоумышленники. Например, мошенники в очередной раз обратились к старой схеме, когда якобы от имени известных людей или организаций раздаются денежные призы с единственным условием: для получения вознаграждения необходимо совершить предварительный перевод небольшой суммы денег под предлогом верификации адреса получателя награды. На этот раз «призы» в криптовалюте раздавались якобы от лица Джона Макафи и Илона Маска.

У пользователей интернета большой популярностью пользуется платформа YouTube, в связи с чем видеоканалы становятся привлекательной площадкой для размещения вредоносных ссылок. В ходе одной из таких мошеннических кампаний зрителям предлагались к просмотру видеоролики, якобы обучающие работе с бесплатным генератором биткойнов, ссылка на который размещалась в описании под видео. В действительности же клик по ссылке инициировал загрузку инфостилера Qulab. В результате другой аналогичной кампании через YouTube распространялось ВПО для удаленного управления nJRaT.

Хакинг



Во II квартале злоумышленники нацелены на эксплуатацию:

- CVE-2017-11882
- CVE-2019-0708
- CVE-2019-0604
- CVE-2019-2725
- CVE-2019-10149
- CVE-2019-3396



Самой обсуждаемой проблемой безопасности во II квартале стала критически опасная RCE-уязвимость BlueKeep (CVE-2019-0708) в службе RDS некоторых старых версий Windows. Несмотря на то, что 14 мая компания Microsoft выпустила патч, множество компьютеров по всему миру остаются под угрозой, в то время как злоумышленники продолжают активно искать уязвимые узлы и разрабатывать эксплойты.

Распространение вредоносного ПО посредством эксплуатации BlueKeep может достичь масштаба WannaCry, поэтому настоятельно рекомендуется установить обновления.

Хакеры активно эксплуатируют уязвимость в почтовом сервере Exim (CVE-2019-10149), которая позволяет удаленно выполнять команды ОС с правами администратора. Одна из хакерских группировок использует уязвимость для внедрения бэкдора, загружая на почтовые серверы shell-скрипты и добавляя SSH-ключ к учетной записи root. Кроме того, злоумышленники незаконно загружают на уязвимые серверы ПО для майнинга криптовалюты. Уязвимость была устранена разработчиками Exim в феврале 2019 года. Однако выпуск обновления производителем далеко не всегда нейтрализует угрозу, и, как показывает практика, из-за несвоевременного обновления ПО хакеры успешно эксплуатируют уязвимости даже пятилетней давности.

На протяжении II квартала злоумышленники искали публично доступные Docker API, сканируя интернет в поисках узлов с открытым портом 2375. Неверно сконфигурированные контейнеры Docker используются в самых разных целях. Например, обнаружив работающий контейнер, хакеры устанавливают в него троян Dofloo. Этот же троян злоумышленники доставляют на узлы с установленным ПО Atlassian Confluence, эксплуатируя уязвимость CVE-2019-3396. Зловред Dofloo использует вычислительные мощности жертв для DDoS-атак и скрытого майнинга криптовалюты.

Эксплуатация веб-уязвимостей

Во II квартале злоумышленники эксплуатировали веб-уязвимости в 18% атак на юридические лица. Волна атак на веб-ресурсы с возможностью онлайн-платежей, начавшаяся в I квартале, набирает обороты. Так, атакам с использованием JavaScript-снифферов MageCart (вредоносных скриптов, направленных на кражу данных платежных карт) на этот раз подверглись Forbes, Puma и множество интернет-магазинов. Киберпреступники, стоящие за атаками MageCart, регулярно обновляют вредоносные скрипты.

Опасность JavaScript-снифферов заключается в том, что посетители зараженных сайтов не могут распознать угрозу, поскольку действие вредоносных скриптов незаметно для пользователей. Однако один из новых способов кражи данных MageCart содержит признаки, по которым внимательный человек сможет распознать угрозу. Злоумышленники внедряют форму для ввода данных карты на страницы сайтов, в то время как этот интерфейс должен быть доступен только после перенаправления на защищенную страницу провайдера платежных систем. Необходимость дважды вводить реквизиты карты (непосредственно на сайте и на странице платежного провайдера) должна насторожить покупателя.

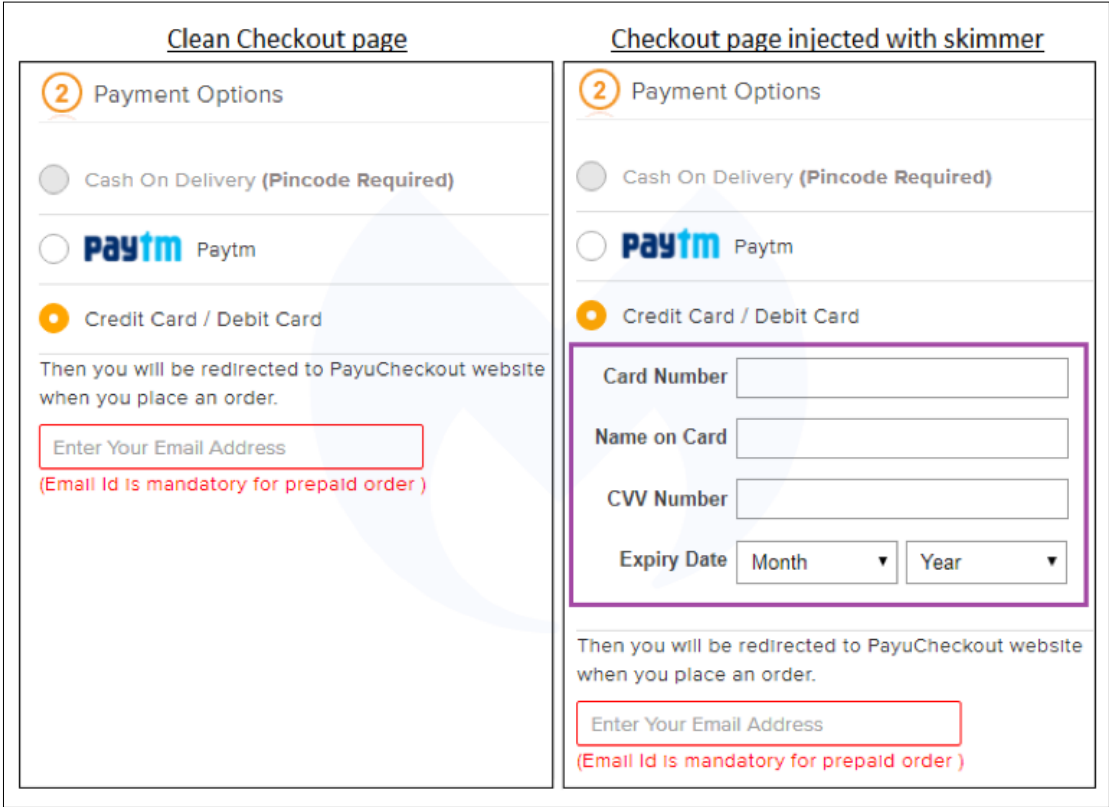


Рисунок 11. Форма MageCart для кражи данных платежных карт

Во втором квартале специалисты Malwarebytes Labs обнаружили JavaScript-снифферы MageCart в библиотеках, которые разработчики сайтов размещали в закрытых репозиториях CDN на базе Amazon CloudFront. Кроме того, с начала апреля злоумышленники внедряют JavaScript-снифферы MageCart в файлы, хранящиеся в Amazon S3, что уже привело к компрометации 17 тысяч сайтов. Интересно, что не все скомпрометированные ресурсы содержат форму для ввода платежной информации, из чего эксперты делают вывод, что хакеры внедряют JavaScript-снифферы в ходе массовых атак в технике spray and pray.

Очевидно, что злоумышленников привлекают не только те сайты, на которых есть возможность совершать онлайн-платежи. В июне был взломан форум Social Engineered, разработанный на базе ПО MyBB. Хакеры воспользовались XSS-уязвимостью в MyBB, о которой стало известно за несколько дней до инцидента. В результате атаки в руки хакеров попали 55 тысяч учетных записей пользователей форума и их личные сообщения.

Подбор учетных данных

Слабые пароли остаются одной из основных проблем безопасности. Пароли 300 сотрудников агентства [Information Network Security Agency](#) в Эфиопии, основной целью которого является обеспечение безопасности информации, имели слабую стойкость, из-за чего попали в руки злоумышленников и оказались в открытом доступе. Примечательно, что 142 пароля из 300 — это сочетание символов p@\$wOrd, еще 60 — сочетание цифр 123.

По-прежнему актуальны атаки типа credential stuffing (попытки доступа к системе с использованием украденной базы учетных данных). Так, во II квартале от этих атак [пострадали](#) около полумиллиона пользователей двух интернет-магазинов (брендов Uniqlo и GU).

В течение II квартала специалисты [фиксируют](#) атаки нового ботнета GoldBrute, направленные на подбор паролей для доступа по RDP. Атакам подверглись уже более 1,5 млн устройств под управлением Windows. Цели злоумышленников пока неясны, но с большой вероятностью они планируют продавать украденные учетные записи в дарквебе. Нередко подобным массовым атакам, направленным на подбор учетных данных, подвергаются и IoT-устройства. В июне стало [известно](#) о вредоносном ПО Silex, которое нацелено на подбор стандартных паролей на устройствах IoT. После успешного подбора паролей Silex выводит устройства из строя; насчитывается более двух тысяч устройств, пострадавших от деструктивного воздействия Silex.

Категории жертв

Г Далее мы подробнее остановимся на анализе атак на отдельные отрасли, которые нам показались наиболее интересными во **II квартале 2019 года**.

Государственные организации

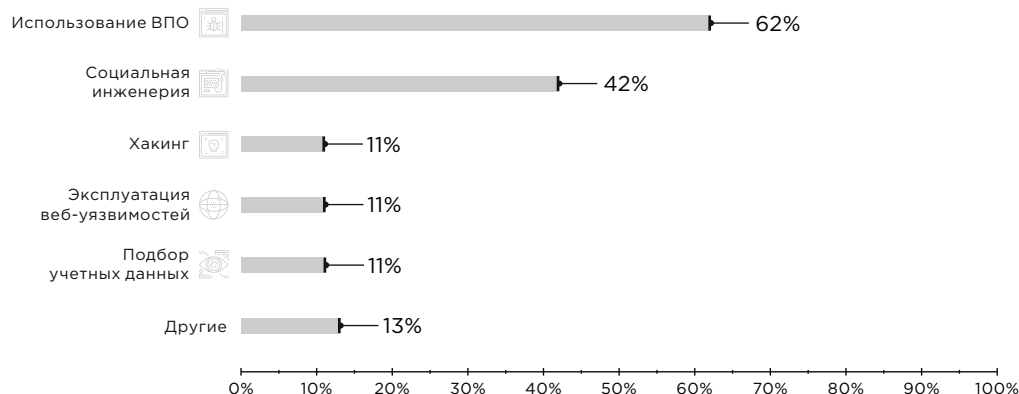


Рисунок 12. Методы атак на государственные организации в Q2 2019

Во II квартале 2019 года мы наблюдаем значительный рост доли заражений вредоносным ПО среди государственных организаций (62% против 44% в I квартале).

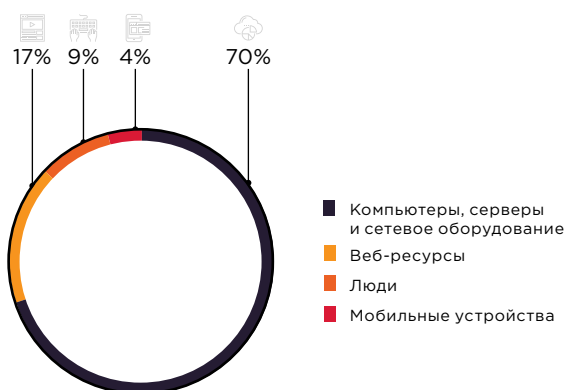


Рисунок 13. Объекты атак

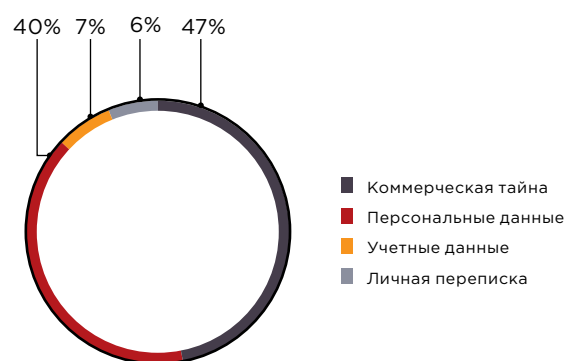


Рисунок 14. Украденные данные

Наиболее часто государственные учреждения подвергаются атакам шифровальщиков. В начале мая вся IT-инфраструктура города Балтимор (США) оказалась заблокирована на несколько недель из-за атаки шифровальщика RobinHood. Власти города оценили ущерб от атаки более чем в 18 млн долл. США. Балтимор стал не первой жертвой трояна RobinHood: в апреле шифровальщиком были заражены информационные системы города Гринвилл (США).

Нарушение работоспособности информационных систем нередко вынуждает администрации пострадавших населенных пунктов идти на сделку с вымогателями и платить выкуп. Острую актуальность эта проблема приобретает в небольших городах со слабо развитой IT-инфраструктурой. Так, в правительстве города Ривьера-Бич в штате Флорида единогласно приняли решение заплатить выкуп в 65 биткойнов (600 тыс. долл. США), поскольку у IT-специалистов не оказалось резервных копий, необходимых для восстановления пораженных систем.

В начале июня атаке трояна-шифровальщика подвергся и другой город Флориды — Лейк-Сити. Городские информационные системы были заражены в ходе масштабной вредоносной кампании Triple Threat, о которой в апреле впервые рассказали специалисты Cybereason. Кампания получила название из-за тройной «полезной нагрузки»: посредством фишинговых писем на компьютеры жертв доставляются три трояна — Emotet, TrickBot и Ryuk. Несмотря на то что зараженные устройства были максимально быстро отключены от сети города, заражены оказались большинство телефонных и почтовых систем. Правительство также приняло решение заплатить выкуп вымогателям в размере 42 биткойна (530 тыс. долл. США), после чего IT-директор был уволен.

Однако на этом атаки троянов-вымогателей на населенные пункты Флориды не закончились, и в конце июня очередной жертвой стал Ки-Бискейн, но на этот раз власти города отказались платить выкуп.

Не обошли атаки троянов-шифровальщиков и Россию. На Южном Урале во II квартале зафиксированы попытки заражений, в Увельском районе Челябинской области они оказались успешны.

Крупные финансовые потери государственные учреждения могут понести и в результате фишинговой атаки. В результате одной из таких атак чиновники канадского города Берлингтон перевели на счет злоумышленников 503 тыс. долл.

Кроме того, продолжаются атаки на правительственные веб-ресурсы. Хакеры взломали три веб-сайта Национальной академии ФБР и выложили в открытый доступ персональные данные четырех тысяч федеральных агентов и сотрудников правоохранительных органов.

Промышленные компании

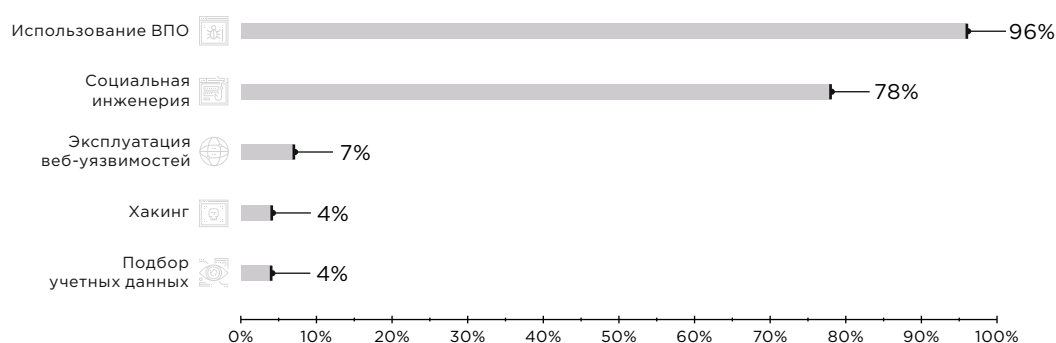


Рисунок 15. Методы атак на промышленные компании в Q2 2019

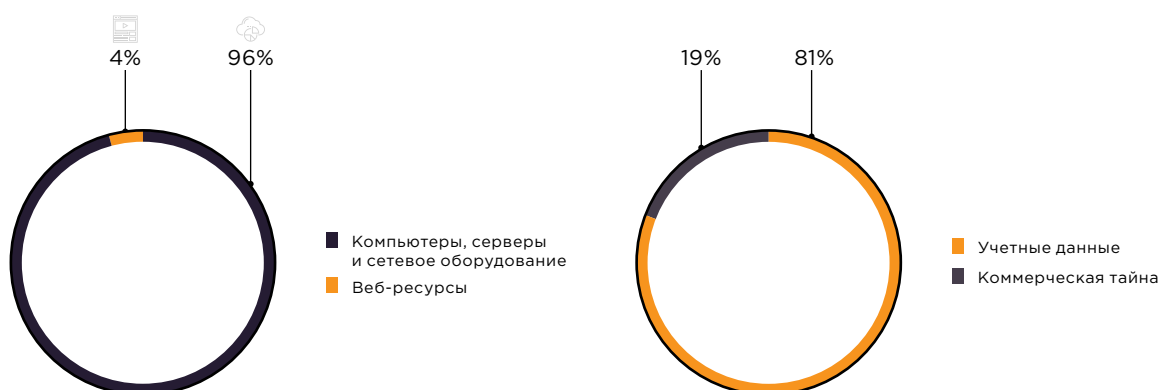


Рисунок 16. Объекты атак

Рисунок 17. Украденные данные

Почти все атаки на промышленные предприятия (96%) во II квартале 2019 года совершались с использованием вредоносного ПО. Активные попытки проникновения во внутреннюю ИТ-инфраструктуру промышленных компаний предпринимает группировка RTM. В течение второго квартала специалисты РТ ESC зафиксировали 26 вредоносных рассылок этой группы. В списке адресатов, кроме финансовых учреждений, более десятка промышленных организаций в России и СНГ. Все письма составлены на русском языке и имеют схожую тематику: как правило, они содержат якобы финансовые документы (акты, счета и др.) с просьбами проверить, подписать документы или осуществить оплату.

Троян RTM относится к категории шпионских: ворует учетные записи, записывает видео, делает снимки экрана и передает их на сервер злоумышленников. Примечательно, что в июне группа изменила способ получения IP-адреса контрольного сервера. Теперь адрес получается с помощью логических операций (AND и циклический сдвиг вправо) над суммой транзакции, полученной на определенный кошелек Bitcoin.

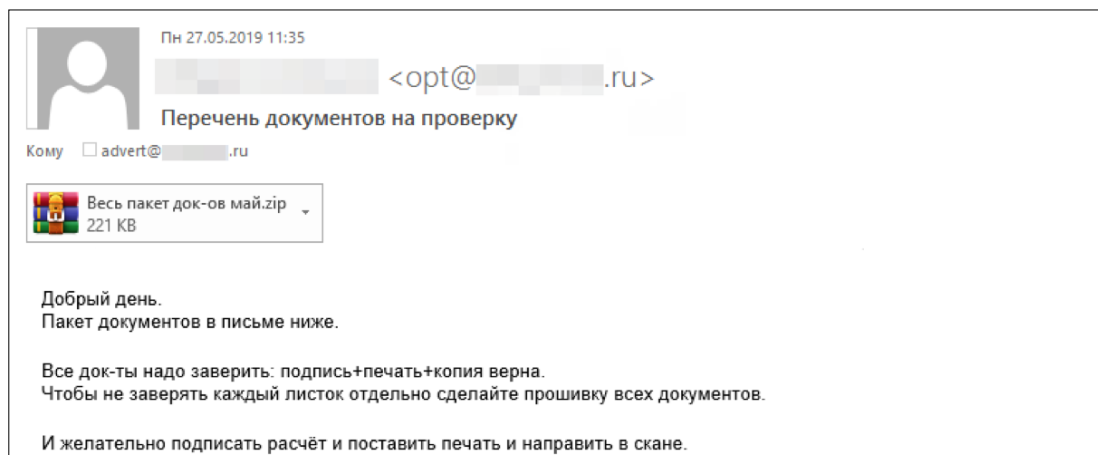


Рисунок 18. Фишинговая рассылка группы RTM

Во II квартале специалисты PT ESC зафиксировали атаки группы TaskMasters, направленные на промышленные предприятия России. Интересно, что в этих атаках группа использовала VMProtect для защиты трояна от детектирования антивирусным ПО. После публикации нашего исследования о группе TaskMasters, а также доклада на конференции PHDays 9, посвященного деятельности группы, злоумышленники перевели большинство доменов на IP-адрес 127.0.0.1, предотвращая тем самым передачу трафика за пределы компьютера жертвы. Это свидетельствует о том, что группа знает об обнаружении и, вероятно, приостановила свои действия.

Продолжаются атаки на промышленность со стороны шифровальщиков. Во II квартале жертвами троянов-вымогателей стали, например, производитель спецоборудования для содержания аэропортов Aebi Schmidt и один из крупнейших производителей запчастей для авиационной техники ASCO.

Нередко хакеры атакуют и веб-ресурсы промышленных компаний. Так, злоумышленники взло-мали сайт компании Uniden для размещения на нем трояна Emotet. Сайт нефтегазовой компании Petrobangla был дважды взломан в течение суток. Хакер, атаковавший сайт Petrobangla, пытался таким образом продемонстрировать владельцам веб-ресурса имеющиеся проблемы с безопасностью.

Медицинские учреждения

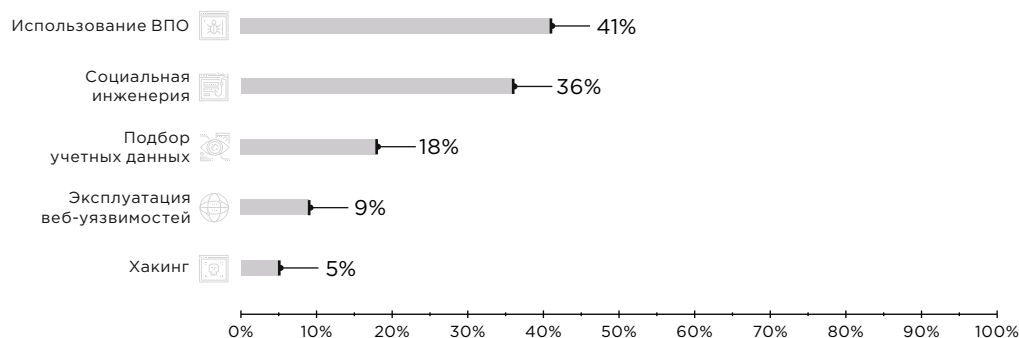


Рисунок 19. Методы атак на медицинские учреждения в Q2 2019

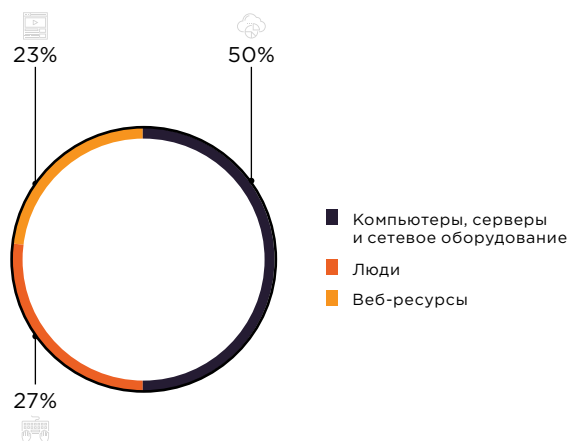


Рисунок 20. Объекты атак

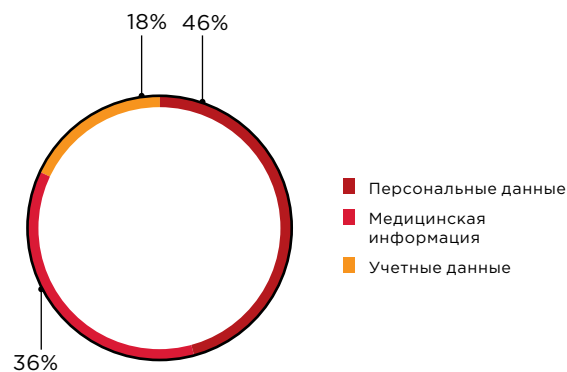


Рисунок 21. Украденные данные

Вредоносное ПО, нарушающее работоспособность систем организации, представляет особую угрозу для учреждений здравоохранения, где подобного рода инциденты могут дорого обойтись как самой компании, так и ее клиентам. В апреле 2019 года жертвой атаки шифровальщика стала офтальмологическая клиника JFJ Eyescare, в результате инцидента зашифрованными оказались персональные данные пациентов.

Сотрудники медицинских организаций нередко подвергаются фишинговым атакам. Работник организации здравоохранения в Новой Шотландии (Канада) получил письмо якобы от сотрудника IT-департамента с просьбой ввести данные своей учетной записи, чтобы предотвратить ее блокирование. В результате успешной атаки в руки злоумышленников попали логин и пароль сотрудника, а данные около трех тысяч пациентов оказались под угрозой.

Однако злоумышленники могут атаковать медицинские организации с целью получения сведений не только о пациентах, но и о сотрудниках. Например, за 500 долл. США в дарквебе продавались пакеты документов врачей: дипломы о медицинском образовании, рекомендации, лицензии на медицинскую деятельность.

Финансовые организации

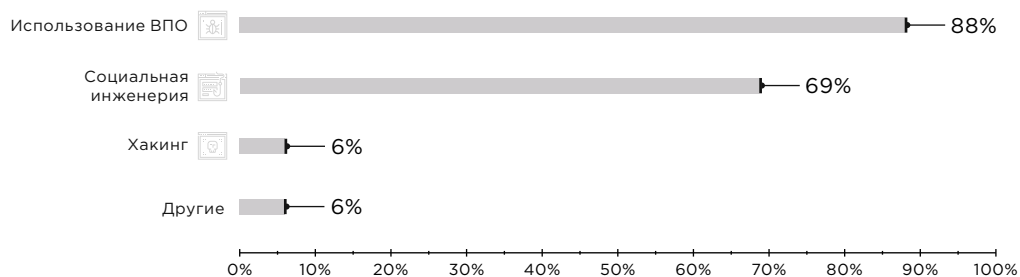


Рисунок 22. Методы атак на финансовые организации в Q2 2019

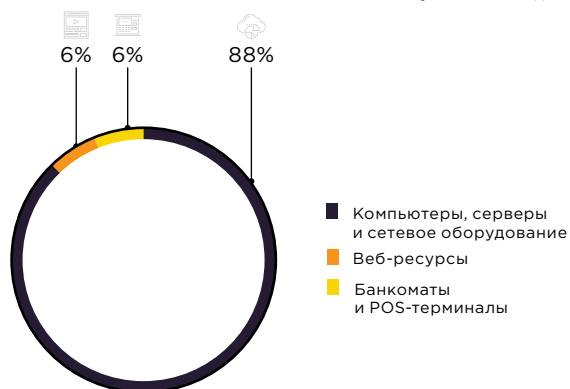


Рисунок 23. Объекты атак

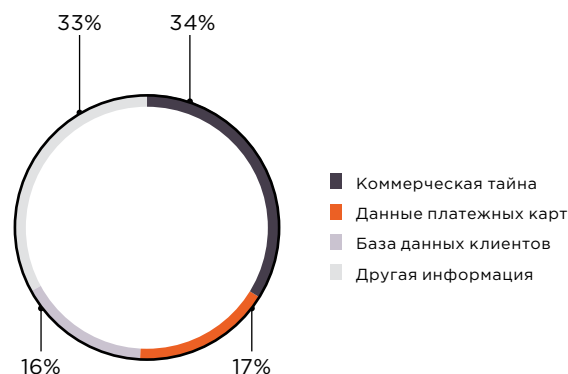


Рисунок 24. Украденные данные

Во II квартале фишинговые рассылки проводили сразу несколько групп, ориентированных на финансовую отрасль. Группировка Cobalt продолжает атаковать: в течение II квартала эксперты PT ESC отметили две атаки. Во время второй атаки группа перешла от традиционных COM-DLL-Dropper и JavaScript-бэкдора, которые использовались злоумышленниками с конца прошлого года, к использованию модифицированного CobInt, который отмечался в их арсенале с августа по ноябрь 2018 года.

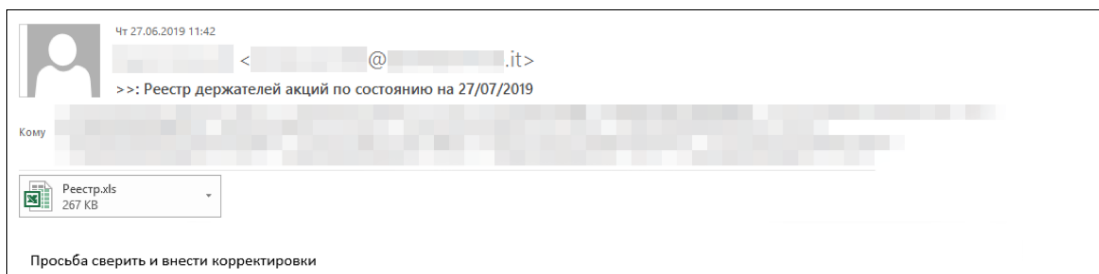


Рисунок 25. Фишинговое письмо группировки Cobalt

В июне специалисты PT ESC обнаружили фишинговую рассылку группировки Silence якобы от лица клиента банка.

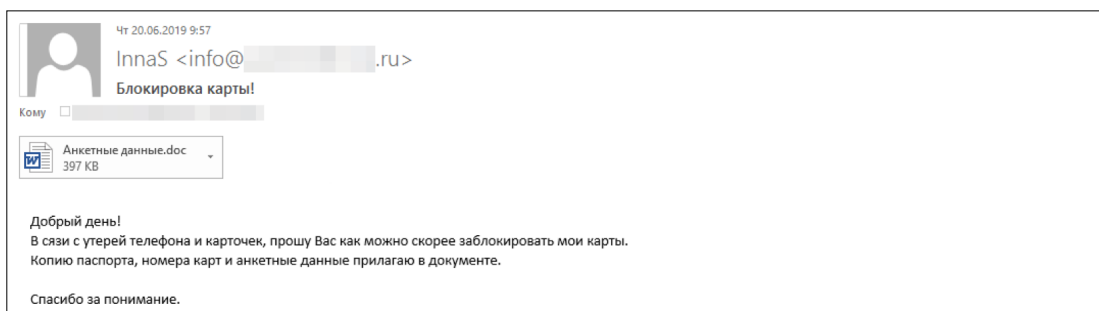


Рисунок 26. Фишинговое письмо Silence

В мае специалистами PT ESC были выявлены фишинговые письма с зашифрованными архивами, в которых находился файл в формате LNK. При запуске этого файла на компьютер жертвы загружался скрипт PowerShell, собирающий системную информацию и отправляющий ее злоумышленникам. По этой информации злоумышленники определяли, какой зловред установить в скомпрометированную систему. Сетевая инфраструктура позволяет нам идентифицировать эту преступную группу как FinTeam.

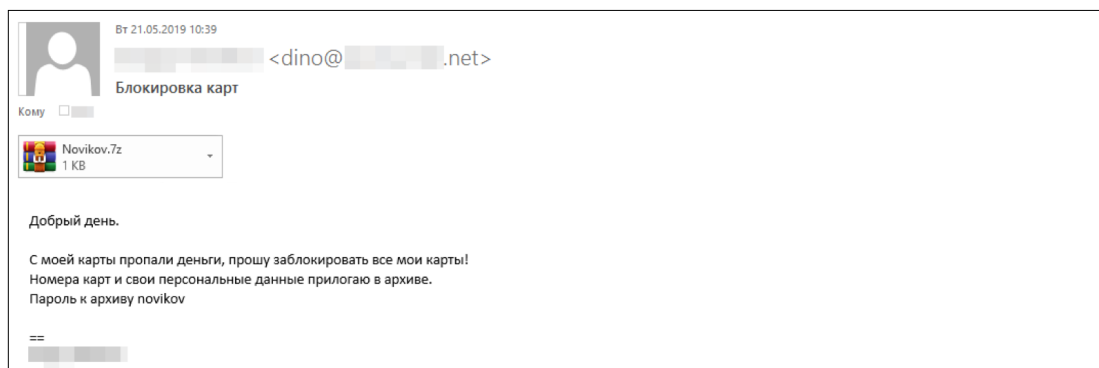


Рисунок 27. Фишинговая рассылка неизвестной группы (предположительно FinTeam)

Кроме того, во II квартале 2019 года жертвами хакеров стали по меньшей мере три банка в Бангладеш — Dutch Bangla Bank Limited (DBBL), NCC Bank и Prime Bank. Известно, что в результате кибератаки банк DBBL потерял 3 млн долл. США. По словам представителей двух других банков, они не понесли финансовых потерь.

IT-компании

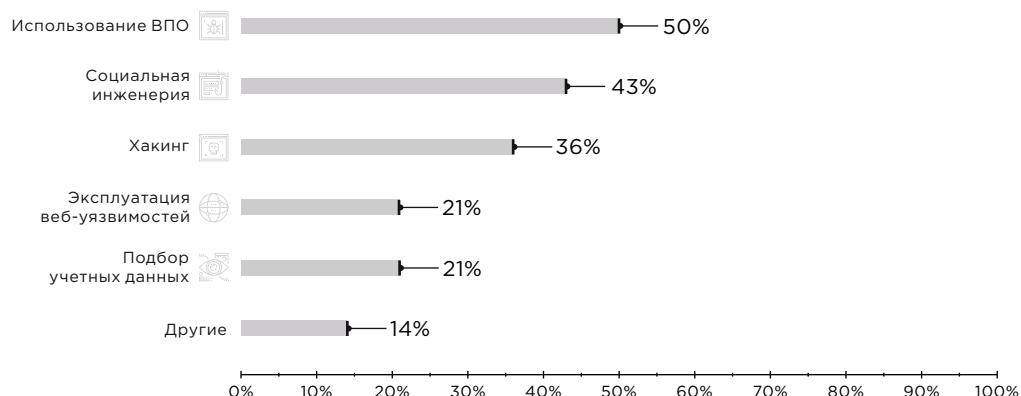


Рисунок 28. Методы атак на IT-компании в Q2 2019

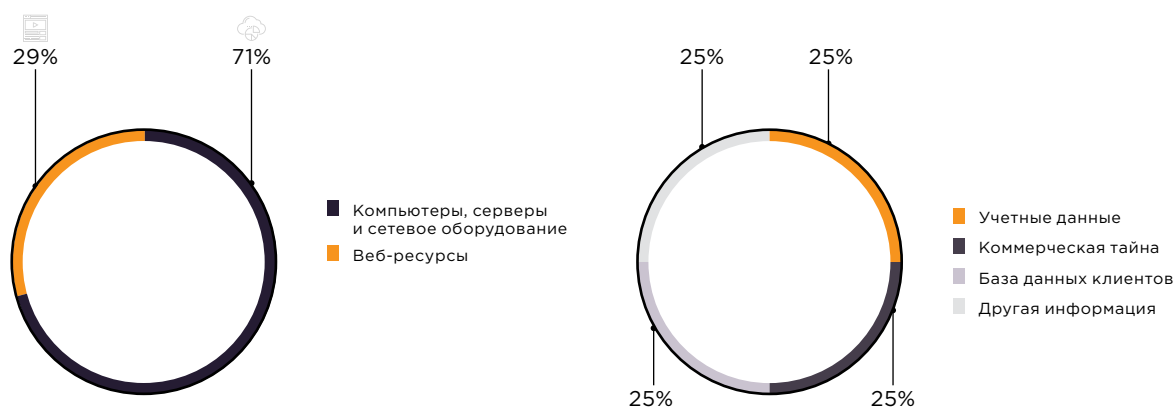


Рисунок 29. Объекты атак

Рисунок 30. Украденные данные

В первой половине апреля хакеры получили доступ к инфраструктуре компании [Matrix](#), разработчика децентрализованной платформы обмена сообщениями, воспользовавшись уязвимостями в устаревшей версии Jenkins. В результате вторжения в руки злоумышленников попали незашифрованные сообщения, хеши паролей пользователей и токены доступа.

IT-компании нередко становятся жертвами атак supply chain. Хакеры взломали одного из крупнейших индийских поставщиков IT-услуг — компанию Wipro, клиентами которой являются организации сферы здравоохранения, телекоммуникаций и финансовой отрасли. В результате взлома инфраструктуры Wipro от фишинговых атак пострадали не менее десятка компаний-клиентов, получивших электронные письма с вредоносными вложениями якобы от сотрудников Wipro. По [мнению](#) экспертов Flashpoint, проводивших расследование инцидента, одной из целей злоумышленников стала мошенническая операция с подарочными картами (gift card fraud).

В середине мая от атаки supply chain [пострадал](#) и поставщик облачных решений РСМ. Злоумышленники получили доступ к учетной записи администратора, которая использовалась в РСМ для управления учетными записями клиентов в Office 365. И вновь целью злоумышленников стала кража информации с целью ее использования для незаконного получения подарочных карт.

Как защититься организации

Г Используйте эффективные технические средства защиты

- Системы централизованного управления обновлениями и патчами для используемого ПО. Для правильной приоритизации планов по обновлениям необходимо учитывать сведения об актуальных угрозах безопасности.
- Системы антивирусной защиты со встроенной изолированной средой («песочницей») для динамической проверки файлов, способные выявлять и блокировать вредоносные файлы в корпоративной электронной почте до момента их открытия сотрудниками и другие вирусные угрозы. Наиболее эффективным будет использование антивирусного ПО, построенного на решениях одновременно нескольких производителей, способного обнаруживать скрытое присутствие вредоносных программ и позволяющего выявлять и блокировать вредоносную активность в различных потоках данных — в почтовом, сетевом и веб-трафике, в файловых хранилищах, на веб-порталах. Важно, чтобы выбранное решение позволяло проверять файлы не только в реальном времени, но и автоматически анализировало уже проверенные ранее, это позволит выявить не обнаруженные ранее угрозы при обновлении баз сигнатур.
- SIEM-решения — для своевременного выявления и эффективного реагирования на инциденты информационной безопасности. Это позволит своевременно выявлять злонамеренную активность, попытки взлома инфраструктуры, присутствие злоумышленника и принимать оперативные меры по нейтрализации угроз.
- Автоматизированные средства анализа защищенности и выявления уязвимостей в ПО.
- Межсетевые экраны уровня приложений (web application firewalls) — в качестве превентивной меры защиты веб-ресурсов.
- Системы глубокого анализа сетевого трафика — для обнаружения сложных целевых атак как в реальном времени, так и в сохраненных копиях трафика. Применение такого решения позволит не только увидеть не обнаруженные ранее факты взлома, но и в режиме реального времени отслеживать сетевые атаки, в том числе запуск вредоносного ПО и хакерских инструментов, эксплуатацию уязвимостей ПО и атаки на контроллер домена. Такой подход позволит существенно снизить время скрытного присутствия нарушителя в инфраструктуре, и тем самым минимизировать риски утечки важных данных и нарушения работы бизнес-систем, снизить возможные финансовые потери от присутствия злоумышленников.
- Специализированные сервисы анти-DDoS.

Г Защищайте данные

- не храните чувствительную информацию в открытом виде или в открытом доступе;
- регулярно создавайте резервные копии систем и храните их на выделенных серверах отдельно от сетевых сегментов рабочих систем;
- минимизируйте, насколько это возможно, привилегии пользователей и служб;
- используйте разные учетные записи и пароли для доступа к различным ресурсам;
- применяйте двухфакторную аутентификацию там, где это возможно, например для защиты привилегированных учетных записей.

Г Не допускайте использования простых паролей

- применяйте парольную политику, предусматривающую строгие требования к минимальной длине и сложности паролей;
- ограничьте срок использования паролей (не более 90 дней);
- смените стандартные пароли на новые, удовлетворяющие строгой парольной политике.

Г Контролируйте безопасность систем

- своевременно обновляйте используемое ПО по мере выхода патчей;
- проверяйте и повышайте осведомленность сотрудников в вопросах информационной безопасности;
- контролируйте появление небезопасных ресурсов на периметре сети; регулярно проводите инвентаризацию ресурсов, доступных для подключения из интернета; анализируйте защищенность таких ресурсов и устраняйте уязвимости в используемом ПО; хорошей практикой является постоянный мониторинг публикаций о новых уязвимостях: это позволяет оперативно выявлять такие уязвимости в ресурсах компании и своевременно их устранять;
- эффективно фильтруйте трафик для минимизации доступных внешнему злоумышленнику интерфейсов сетевых служб; особое внимание стоит уделять интерфейсам удаленного управления серверами и сетевым оборудованием;
- регулярно проводите тестирование на проникновение для своевременного выявления новых векторов атак на внутреннюю инфраструктуру и оценки эффективности принятых мер по защите;
- регулярно проводите анализ защищенности веб-приложений, включая анализ исходного кода, с целью выявления и устранения уязвимостей, позволяющих проводить атаки, в том числе на клиентов приложения;
- отслеживайте количество запросов к ресурсам в секунду, настройте конфигурацию серверов и сетевых устройств таким образом, чтобы нейтрализовать типичные сценарии атаки (например, TCP- и UDP-флуд или множественные запросы к БД).

Г Позаботьтесь о безопасности клиентов

- повышайте осведомленность клиентов в вопросах ИБ;
 - регулярно напоминайте клиентам о правилах безопасной работы в интернете, разъясняйте методы атак и способы защиты;
 - предостерегайте клиентов от ввода учетных данных на подозрительных веб-ресурсах и тем более от сообщения такой информации кому бы то ни было по электронной почте или во время телефонного разговора;
 - разъясняйте клиентам порядок действий в случае подозрений о мошенничестве;
 - уведомляйте клиентов о событиях, связанных с информационной безопасностью.
-

Как вендору защитить свои продукты

- применяйте все те же меры защиты, что рекомендованы для обеспечения безопасности организации;
 - внедрите процессы обеспечения безопасности на протяжении всего цикла разработки ПО;
 - проводите регулярный анализ защищенности ПО и веб-приложений, включая анализ исходного кода;
 - используйте актуальные версии веб-серверов и СУБД;
 - откажитесь от использования библиотек и фреймворков, имеющих известные уязвимости.
-

Как защититься обычному пользователю

Г Не экономьте на безопасности

- используйте только лицензионное ПО;
- используйте эффективные средства антивирусной защиты на всех устройствах;
- своевременно обновляйте используемое ПО по мере выхода патчей.

Г Защищайте ваши данные

- наиболее важные файлы храните не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище;
- для повседневной работы в ОС используйте учетную запись без привилегий администратора;
- используйте двухфакторную аутентификацию там, где это возможно, например для защиты электронной почты.

Г Не используйте простые пароли

- используйте сложные пароли, состоящие из незначущих комбинаций букв, цифр и знаков, длиной не менее 8 символов. Для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей);
- не используйте один и тот же пароль для разных систем (для сайтов, электронной почты и др.);
- меняйте все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.

Г Будьте бдительны

- проверяйте все вложения, полученные по электронной почте, с помощью антивирусного ПО;
- с осторожностью относитесь к сайтам с некорректными сертификатами и учитывайте, что введенные на них данные могут быть перехвачены злоумышленниками;
- будьте предельно внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами;
- не переходите по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности;
- не переходите по ссылкам из всплывающих окон, даже если рекламируемые компания или продукт вам знакомы;
- не загружайте файлы с подозрительных веб-ресурсов или из других неизвестных источников.

Г 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.

В рамках аналитического исследования массовые инциденты (например, вирусные атаки, в ходе которых злоумышленники проводят многоадресные фишинговые рассылки) рассматриваются как одна уникальная угроза информационной безопасности. Каждое событие характеризуется следующими признаками:

Объект атаки — объект деструктивного воздействия со стороны киберпреступников. Если методы социальной инженерии направлены на получение информации непосредственно от частного лица, клиента или сотрудника компании, то объектом атаки является категория «Люди». Если же методы социальной инженерии применяются с целью доставки ВПО в инфраструктуру компании или на компьютер частного лица, то в качестве объекта атаки выбирается категория «Компьютеры, серверы и сетевое оборудование».

Мотив атаки — первостепенная цель киберпреступников. Например, если в результате атаки похищены данные платежных карт, мотивом в этом случае является получение данных.

Методы атаки — совокупность приемов, которые использовались для достижения цели. Например, злоумышленник может провести разведку, выявить доступные для подключения уязвимые сетевые службы, проэксплуатировать уязвимости и получить доступ к ресурсам или информацию; такой процесс мы называем хакингом. При этом подбор учетных данных и использование уязвимостей веб-приложений мы выделили в отдельные категории для большей детализации.

Категория жертв — сфера деятельности атакованной организации (или частные лица, если в результате атаки пострадали люди независимо от места их работы). Так, к сфере услуг мы относим организации, которые предоставляют услуги на коммерческой основе (например, консалтинговые организации или гостиницы, рестораны и др.). Категория «Онлайн-сервисы» включает интернет-площадки, позволяющие пользователям решать их задачи онлайн (например, сайты-агрегаторы для покупки билетов, бронирования номеров в гостиницах, блоги, соцсети, мессенджеры и иные социальные медиаресурсы, видеохостинги, онлайн-игры). Масштабные кибератаки, преимущественно вредоносные эпидемии, которые не ограничиваются воздействием на какую-то одну отрасль, мы отнесли к категории «Без привязки к отрасли».

По нашей оценке, большинство кибератак не передается огласке из-за репутационных рисков, поэтому оценить точное число угроз не могут даже организации, занимающиеся расследованием инцидентов и анализом действий хакерских групп. Данное 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.

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.