









# АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ IV КВАРТАЛ 2017 ГОДА

## СОДЕРЖАНИЕ







Условные обозначения .....	3
Резюме .....	4
Динамика количества инцидентов.....	6
Методы атак.....	7
Использование вредоносного ПО .....	7
Социальная инженерия.....	9
Эксплуатация уязвимостей ПО .....	10
Эксплуатация веб-уязвимостей.....	12
Компрометация учетных данных .....	14
DDoS.....	15
Объекты атак.....	17
Инфраструктура.....	17
Веб-ресурсы .....	19
Пользователи .....	20
Мобильные устройства.....	22
Банкоматы и POS-терминалы .....	23
IoT .....	24
Выводы .....	26

## УСЛОВНЫЕ ОБОЗНАЧЕНИЯ















### Объекты атак

-  Инфраструктура
-  Веб-ресурсы
-  Пользователи
-  Банкоматы и POS-терминалы
-  Мобильные устройства
-  IoT

### Методы атак

-  Использование вредоносного ПО
-  Компрометация учетных данных
-  Социальная инженерия
-  Эксплуатация уязвимостей в ПО
-  Эксплуатация веб-уязвимостей
-  DDoS

### Категории жертв

-  Финансовая отрасль
-  Государственные учреждения
-  Медицинские учреждения
-  Сфера образования
-  Оборонные предприятия
-  Промышленные компании
-  Онлайн-сервисы
-  Сфера услуг
-  Транспорт
-  IT-компании
-  Розничная торговля
-  Частные лица
-  Телеком-операторы
-  Другие сферы

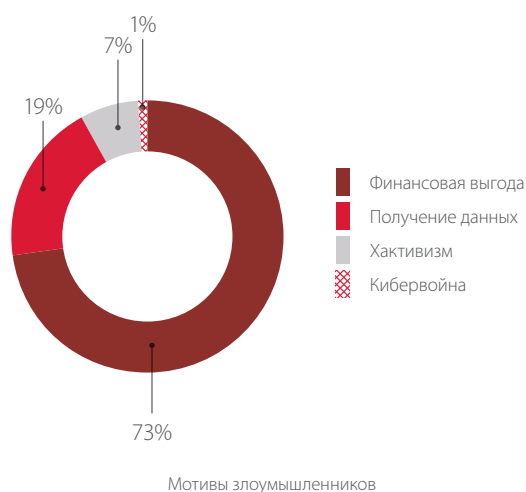
На протяжении всего 2017 года компания Positive Technologies делилась с вами информацией об актуальных угрозах информационной безопасности, основанной на собственной экспертизе, результатах многочисленных расследований, а также данных авторитетных источников. И сегодня мы расскажем о киберинцидентах заключительного квартала 2017 года.

## РЕЗЮМЕ

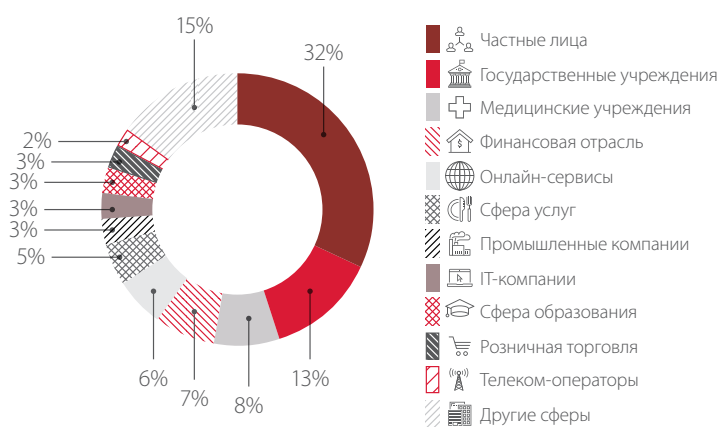
73% атак были совершены с целью получения прямой финансовой выгоды. Кроме того, в IV квартале мы отметили увеличение доли атак (стало 7% — вместо 3% в III квартале), совершенных хактивистами (например, протестующими против действий правительства). При этом снизилось число атак, нацеленных на получение данных, их доля в IV квартале составила 19% (вместо 25% в III квартале).

В IV квартале вновь большинство (58%) составили массовые кибератаки.

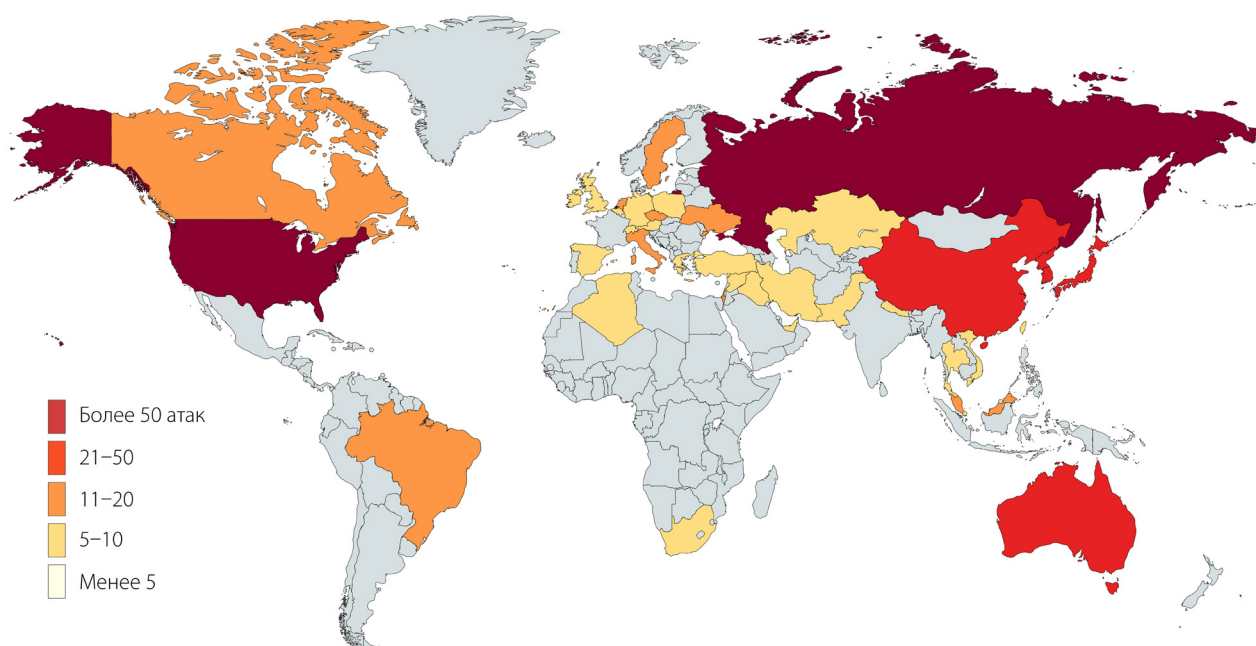
В конце 2017 года злоумышленники продолжили атаки на государственные, медицинские и финансовые учреждения (доли этих атак составили 13%, 8% и 9% соответственно). Однако больше всего кибератак было направлено на частных лиц (32%).



Как мы уже отмечали, множество атак в IV квартале были массовыми и большинство из них затрагивали одновременно две, три, десять и более стран. Среди лидеров по числу произошедших уникальных киберинцидентов мы отметили США, Россию, Австралию, Корею, Японию и Китай.



В случае масштабных атак, поражающих сотни и тысячи компаний, бывает невозможно отнести инцидент к одной из перечисленных отраслей; в таком случае его относили к категории «Другие сферы», этим объясняется столь существенная ее доля.

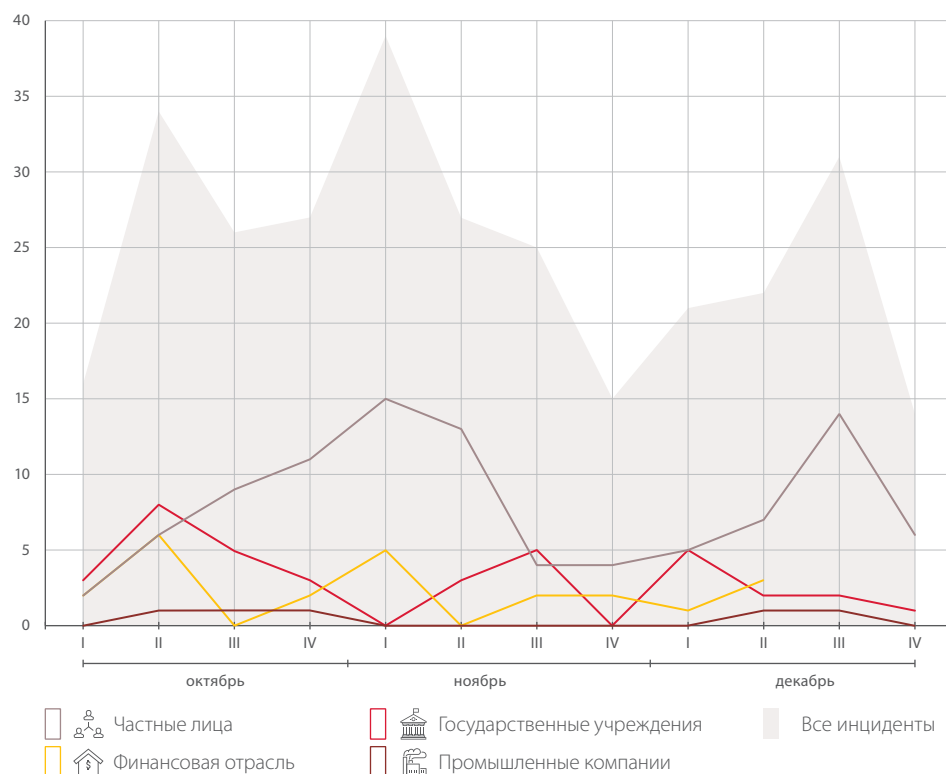


География кибератак в IV квартале 2017 года

		Отрасль										
		Финансовая отрасль	Государственные учреждения	Медицинские учреждения	Сфера образования	Промышленные компании	Онлайн-сервисы	Сфера услуг	Частные лица	Розничная торговля	IT-компании	Другие сферы
Объект	Инфраструктура	12	22	7	9	5	4	9	29	2	8	31
	Веб-ресурсы	3	12	1	1		15	5	19	1	5	6
	Пользователи	4		10	4		3	2	22	1		6
	Банкоматы и POS-терминалы	3							1	2		1
	Мобильные устройства	2	2						23			1
	IoT		1						3		1	2
Метод	Атаки с использованием ВПО	17	11	5	6	2		4	51		3	23
	Компрометация учетных данных		2	6	1		3	1	8	1	2	5
	DDoS	2	8				4					2
	Социальная инженерия	3	2	5	2	3	2	1	13			3
	Эксплуатация уязвимостей в ПО	1	7		3		3		10	2	2	5
	Эксплуатация веб-уязвимостей		3	1	1		8	4	7	1	3	2
	Другой	1	4	1	1		2	6	7	2	4	7
Мотив	Финансовая выгода	24	16	10	8	2	20	7	84	5	11	30
	Получение данных		11	8	5	1	1	5	12	1	3	11
	Хактивизм		8		1	1	1	4				5
	Кибервойна		2			1						1

Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) и отраслям

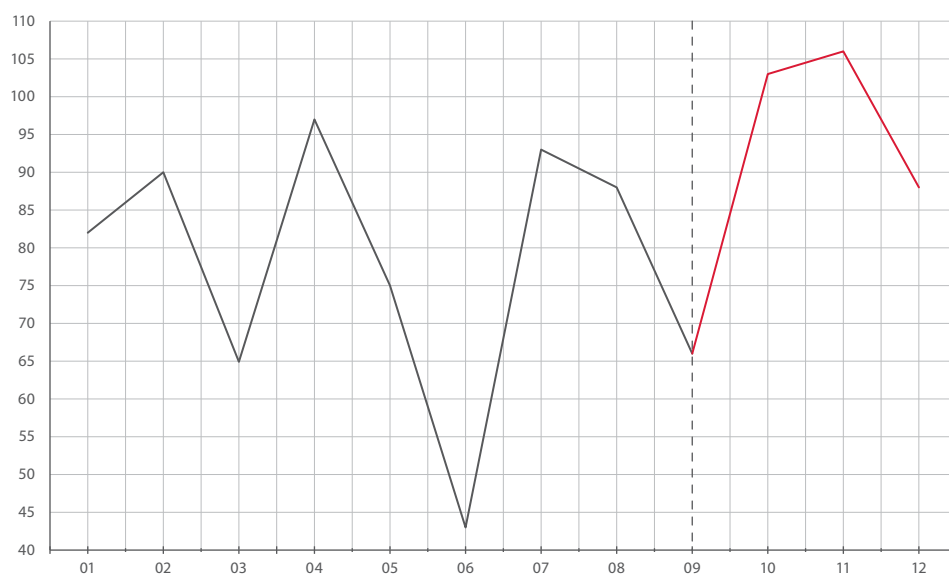
## ДИНАМИКА КОЛИЧЕСТВА ИНЦИДЕНТОВ



Количество инцидентов в IV квартале 2017 года

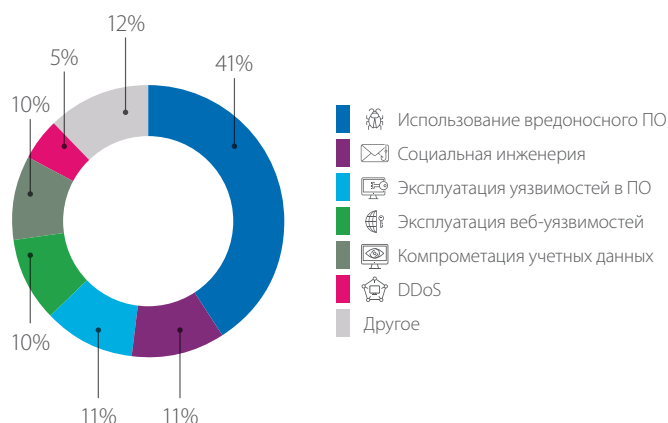
В IV квартале было зафиксировано больше уникальных инцидентов, чем в предыдущие периоды. В начале ноября и конце декабря мы видим рост количества атак на частных лиц. Это можно связать с периодами распродаж («черная пятница», предновогодние ярмарки), когда люди склонны совершать спонтанные покупки, в том числе на подозрительных сайтах.

После роста кибератак в октябре и ноябре в декабре мы видим небольшой спад. Однако о произошедших киберинцидентах, как правило, становится известно спустя какое-то время, и наиболее вероятно, что компании, ставшие жертвами в этот период, еще не завершили расследования и не готовы делиться информацией либо и вовсе еще не знают о том, что были атакованы, и обнаружат следы компрометации уже в первом квартале 2018 года.



Количество инцидентов в 2017 году

## МЕТОДЫ АТАК



Распределение киберинцидентов по методам атак

## ИСПОЛЬЗОВАНИЕ ВРЕДНОСНОГО ПО



Во второй половине декабря биткойн пошел на спад, однако нестабильность криптовалюты, по-видимому, не пугает инвесторов. Мы видим, что число желающих заработать на криптовалюте за счет чужих ресурсов продолжает расти. Мы наблюдаем тенденцию к появлению нового ВПО, которое незаметно для жертвы «майнит» криптовалюту в кошелек злоумышленника. Например, был обнаружен плагин для популярного браузера Chrome, который устанавливал в браузере майнер Coinhive<sup>1</sup>. Этот майнер также продолжает совершенствоваться<sup>2</sup> и теперь может запускаться в фоновом окне, скрывающемся за панелью задач и иконкой часов, а также ограничивает потребляемую мощность процессора, чтобы не вызывать подозрений.

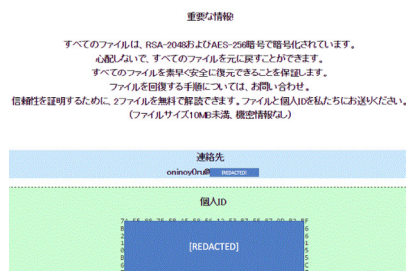
Поскольку грамотность пользователей постепенно повышается, злоумышленникам приходится придумывать новые способы распространения ВПО. Например, при распространении банковского трояна Emotet злоумышленники воспользовались доверием людей к сайтам, принадлежащим ИБ-компаниям, и через домен McAfee (cp.mcafee.com) перенаправляли жертв на сторонний веб-ресурс, с которого на компьютер загружался вредоносный документ MS Word<sup>3</sup>.

<sup>1</sup> [bleepingcomputer.com/news/security/chrome-extension-uses-your-gmail-to-register-domains-names-and-injects-coinhive/](http://bleepingcomputer.com/news/security/chrome-extension-uses-your-gmail-to-register-domains-names-and-injects-coinhive/)

<sup>2</sup> [blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/](http://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/)

<sup>3</sup> [twitter.com/benkow\\_/status/930148339034869764](https://twitter.com/benkow_/status/930148339034869764)

Еще один необычный вектор использования ВПО был отмечен экспертами в ходе расследования атак на восточноевропейские банки<sup>4</sup>. Злоумышленники по объявлениям в интернете набирали дропов, которые оформляли банковские карты в банке-жертве. Затем преступники компрометировали внутреннюю инфраструктуру банка для того, чтобы увеличить лимит овердрафта на полученных дропами картах, а также для получения доступа к управлению банкоматами. По команде хакеров дропы снимали наличные в банкоматах. Злоумышленники же после снятия денег в качестве последнего шага операции запускали на банкоматах файл dropper.exe. Это ВПО повреждало главную загрузочную запись ОС банкомата (после чего ОС становилась незагружаемой), а затем удаляло себя и перезапускало систему. Таким образом злоумышленники заставляли следы, чтобы в ходе расследования специалисты не смогли определить всю последовательность событий.



Сообщение о выкупе на компьютерах,  
зараженных ONI

Мы отмечаем появление новой тенденции к использованию вымогательского ПО не с целью финансовой выгоды, а для сокрытия истинных мотивов киберпреступных действий. В конце октября исследователи рассказали о кампании против японских организаций<sup>5</sup>, в ходе которой злоумышленники рассылали фишинговые письма, содержащие вредоносные документы, после открытия которых на компьютер устанавливался инструмент удаленного администрирования Ammyy Admin RAT. Получив доступ в информационную систему, преступники компрометировали критически важные активы компании. После завершения всех действий злоумышленники запускали вредоносное ПО ONI и MBR-ONI, которое зашифровывало диск и отображало на экране требование выкупа. Различие этих двух программ в том, что MBR-ONI, как правило, наблюдалась на сервере Active Directory и в других критически важных системах и не предполагала дешифровку данных; ее целью было уничтожение следов шпионской кампании. Отметим также, что MBR-ONI является модификацией легальной утилиты для шифрования — DiskCryptor.

#### Как защититься организации

- + Своевременно обновлять используемое ПО.
- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Контролировать появление небезопасных ресурсов на периметре сети.
- + Регулярно создавать резервные копии систем и хранить их на выделенных серверах отдельно от сетевых сегментов рабочих систем.
- + Повышать осведомленность пользователей и сотрудников в вопросах ИБ.

#### Как защититься обычному пользователю

- + Своевременно обновлять используемое ПО по мере выхода патчей.
- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Наиболее важные файлы хранить не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности.
- + Не переходить по ссылкам из всплывающих окон, даже если рекламируемые компания или продукт вам знакомы.
- + Проверять все вложения, полученные по электронной почте, с помощью антивирусного ПО.
- + Не загружать файлы с подозрительных веб-ресурсов или из других неизвестных источников.

4 [trustwave.com/Resources/SpiderLabs-Blog/Post-Soviet-Bank-Heists---A-Hybrid-Cybercrime-Study/](http://trustwave.com/Resources/SpiderLabs-Blog/Post-Soviet-Bank-Heists---A-Hybrid-Cybercrime-Study/)

5 [cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan](http://cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan)



## СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



Больше всего пострадавших в США, Австралии и России



Наиболее атакуемые объекты

Больше всего пострадали

Ущерб > 42 млн долл. США

Пострадали > 2 млн человек



62%



26%



9%



38%

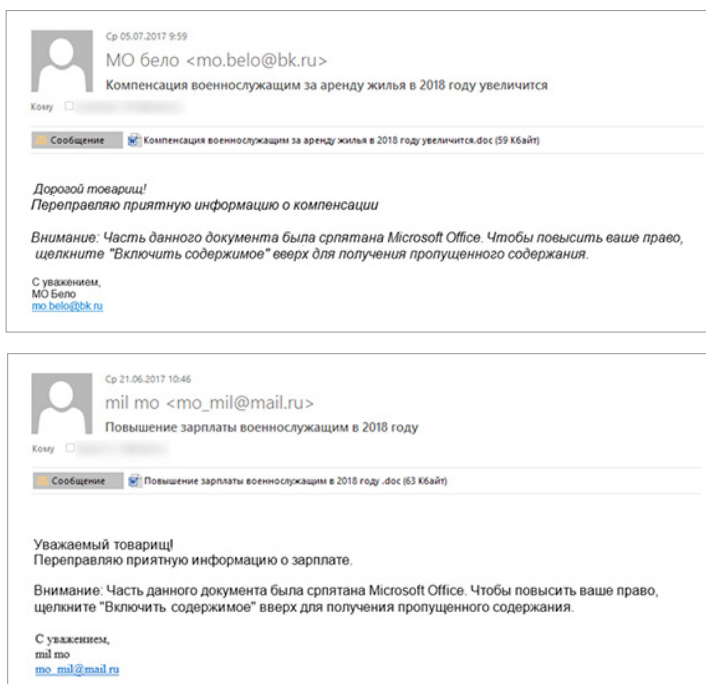


15%



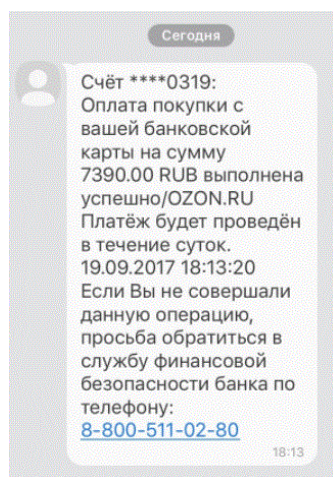
9%

В апреле 2017 года команда PT ESC зафиксировала активность группировки, проводящей новую вредоносную кампанию, направленную на организации военно-промышленного комплекса России и стран СНГ. В рамках данной кампании (которую мы называем SongXY), злоумышленники с помощью целевых фишинговых рассылок распространяли вредоносное ПО CMstar и Lurid для компрометации целевой системы. Тематика фишинговой рассылки была связана с военной и политической сферой, а письма предназначались как для организаций, так и для отдельных лиц. В середине сентября мы отметили, что злоумышленники сменили тактику и вместо вредоносной нагрузки в некоторые документы добавили ссылку на изображение. При открытии такой документ обращался на сервер злоумышленников с запросом на получение изображения, и на сервере оставалась информация об IP-адресе и версии MS Office на целевой системе. Так злоумышленники собирали статистику по доставленным письмам, а сведения об используемой версии ПО позволяли подобрать подходящий эксплойт для последующих атак.



Примеры фишинговых писем от SongXY

Главной задачей кампании SongXY был шпионаж, и используемое вредоносное ПО (Pilot RAT, Lurid, Gh0st, RAT mini) после попадания в корпоративную систему жертвы позволяло злоумышленникам не только скрыто следить за пользователями, но и удаленно контролировать зараженную систему. В ходе расследования специалистам PT ESC удалось



Пример фишингового сообщения

установить, что не менее 17 компаний из Японии, Монголии, Белоруссии, России, США, Таджикистана, Узбекистана, Киргизии, Казахстана и Украины стали жертвами SongXY. В эти организации незамедлительно были направлены уведомления о компрометации.

Осенью PT ESC зафиксировал более 20 фишинговых рассылок в адрес банков России, Казахстана и Белоруссии от группировок Cobalt и Silence APT group. Обе группировки используют метод supply chain attack, при котором компрометируют и используют ИТ-инфраструктуру компании-подрядчика для отправки от ее лица фишинговых писем либо регистрируют фишинговые домены, похожие на доверенные (например, Cobalt в своих рассылках использовал visa-pay.com, swift-alliance.com, cards-cbr.ru, billing-cbr.ru и другие). Такой подход позволяет обойти спам-фильтры и сделать письмо максимально доверенным.

Мошенники продолжают использовать старые схемы обмана в новом облики. Так, в октябре была отмечена массовая рассылка сообщений в Viber якобы от банка «ВТБ 24» (отправителем значился VTB 24) о финансовых операциях, которых жертва не совершала<sup>6</sup>. По указанному в сообщении номеру отвечали, естественно, злоумышленники, которые представлялись работниками банка и для «идентификации клиента» требовали назвать номер карты и код CVV2. Если жертва эту информацию называла, то преступники получали доступ к ее денежным средствам.

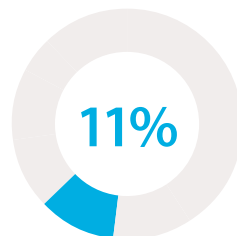
#### Как защититься организации

- + Обучать сотрудников и пользователей основам ИБ.
- + Использовать антивирусное ПО, в том числе специализированное, позволяющее пользователям отправлять подозрительные файлы на проверку перед открытием вложения из письма.
- + Использовать SIEM-решения — для своевременного обнаружения атаки, если инфраструктура оказалась заражена.

#### Как защититься обычному пользователю

- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности.
- + С осторожностью относиться к сайтам с некорректными сертификатами и учитывать, что введенные на них данные могут быть перехвачены злоумышленниками.
- + Быть предельно внимательным при вводе своих учетных данных на веб-сайтах и во время работы с онлайн-платежами.
- + Проверять все вложения, полученные по электронной почте, с помощью антивирусного ПО.

## ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ ПО



Больше всего пострадавших в США, Японии и Канаде



Наиболее атакуемые объекты



58%



21%



9%

Больше всего пострадали



30%



21%



9%

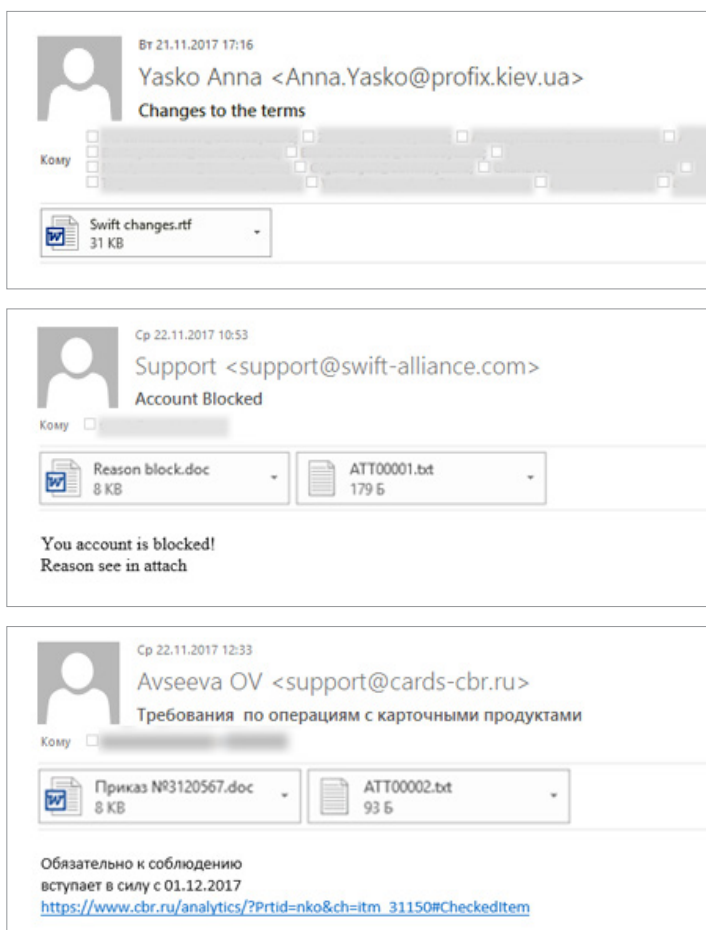
Ущерб > 31 млн долл. США

Пострадали > 20 млн человек

<sup>6</sup> [news.mail.ru/incident/31311775/](https://news.mail.ru/incident/31311775/)

Злоумышленники находят применение уязвимостям практически сразу после появления в интернете публикаций о них (так называемых white papers). Причем некоторые исследователи так спешат поделиться своими открытиями, что едва дожидаются выхода патчей от производителей.

В конце ноября PT ESC стало известно о том, что группировка Cobalt начала использовать в своих атаках на банки новую уязвимость в MS Office CVE-2017-11882. Эта уязвимость была опубликована на сайте Microsoft 14 ноября, и вендор отметил, что для временного устранения уязвимости недостаточно изменить настройку, следует либо полностью отключить редактор формул в Microsoft Office, либо установить обновление безопасности. Уязвимость была обнаружена экспертами компании Embedi, и исследователи одновременно с публикацией обновления выложили в общий доступ на [github.com](https://github.com) свой proof of concept (задокументированный сценарий, демонстрирующий эксплуатацию уязвимости), который подтверждал возможность выполнения произвольного кода без взаимодействия с пользователем. Позднее появилось еще несколько руководств по использованию данной уязвимости. Этими общедоступными материалами и воспользовались, судя по всему, злоумышленники для генерации вредоносных RTF-файлов, которые в дальнейшем направлялись в фишинговых рассылках в банки. Из-за того, что нарушители работали быстрее, чем компании успели установить обновления, этот инцидент затронул довольно большое число финансовых учреждений в России и на Украине.



Примеры фишинговых писем от группировки Cobalt

Следующее событие не является атакой или инцидентом, попавшим в нашу статистику, но мы хотим обратить на него ваше внимание. Эстония занимает лидирующую позицию в мире по цифровизации правительства и государственных органов. Основным документом гражданина этой страны является ID-карта с электронным чипом, заменяющим обычную подпись. Даже выборы в Эстонии с 2007 года проводятся онлайн. Однако функционирование электронного государства во многом зависит от применяемых подходов к обеспечению безопасности. Поэтому в октябре, после того как стало известно об уязвимости

в Trusted Platform Module — системе для безопасного создания ключей шифрования RSA, которая использовалась в чипах многих устройств (в том числе и эстонских ID-карт), — властям Эстонии пришлось отозвать 760 000 электронных сертификатов<sup>7</sup>. Таким образом Эстония показала, что исключение риска взлома ID-карт и необходимая защита цифрового государственного управления должны быть важнее, чем затраты на обновление сертификатов и поддержание должного функционирования всех государственных систем.

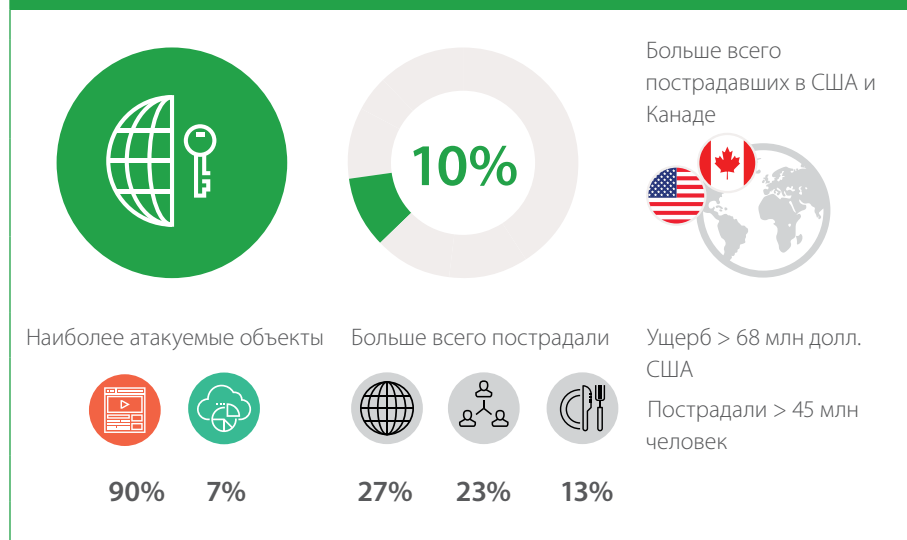
#### Как защититься организации

- + Применять средства централизованного управления обновлениями и патчами для используемого ПО.
- + Применять автоматизированные средства анализа защищенности и выявления уязвимостей в ПО.
- + Использовать межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты веб-ресурсов.
- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Минимизировать, насколько это возможно, привилегии пользователей и служб.

#### Как защититься обычному пользователю

- + Своевременно обновлять используемое ПО.
- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Для повседневной работы в ОС использовать учетную запись без привилегий администратора.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности.
- + Проверять все вложения, полученные по электронной почте, с помощью антивирусного ПО.
- + Не загружать файлы с подозрительных веб-ресурсов или из других неизвестных источников.

### ЭКСПЛУАТАЦИЯ ВЕБ-УЯЗВИМОСТЕЙ



Уязвимости веб-приложений, как правило, используются в трех основных сценариях — при атаке непосредственно на сайт (например, в ICO для подмены реквизитов кошелька); для доступа в корпоративную сеть компании через ее веб-ресурсы; для дальнейшего использования уязвимого сайта (например, для хостинга вредоносного ПО и атак на пользователей).

Каждое четвертое веб-приложение подвержено критически опасной уязвимости «Внедрение операторов SQL». Эксплуатация этой уязвимости позволяет злоумышленнику получить информацию о пользователях. Это и случилось в ноябре с крупным поставщиком услуг веб-хостинга и оператором дата-центров Hetzner<sup>8</sup>. В результате использования

<sup>7</sup> [xakep.ru/2017/11/06/estonian-id-roca/](http://xakep.ru/2017/11/06/estonian-id-roca/)

<sup>8</sup> [hetzner.co.za/news/konsoleh-database-compromise/](http://hetzner.co.za/news/konsoleh-database-compromise/)

SQL-инъекций в базу данных злоумышленникам удалось получить доступ к клиентским данным (включая имена, адреса и телефоны), доменным именам, FTP-паролям, сведениям о банковском счете (без данных кредитных карт).



Дефейс школьных сайтов

Сайты государственных организаций нередко используются как площадка для пропаганды или выражения протеста. Так, за несколько месяцев группа киберпреступников взломала сотни веб-ресурсов полицейских участков и школ<sup>9</sup> и опубликовала на них пропаганду «Исламского государства».

Другая группировка — Anonymouse — нацелилась на веб-сайты неонацистов и в ноябре атаковала 12 сайтов в рамках операции #OpDomesticTerrorism<sup>10</sup>.



Дефейс неонацистского сайта

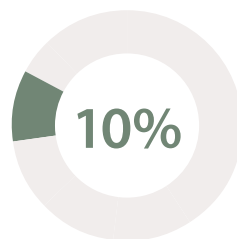
### Как защититься организации

- + Проводить регулярный анализ защищенности веб-приложений, включая анализ исходного кода.
- + Использовать межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты.
- + Внедрить процессы обеспечения безопасности на протяжении всего цикла жизни веб-приложения.
- + Использовать актуальные версии веб-серверов и СУБД. Отказаться от использования библиотек и фреймворков, обладающих известными уязвимостями.

<sup>9</sup> [ibtimes.co.uk/pro-isis-hackers-hijack-800-us-schools-sites-saddam-hussein-photo-i-love-islamic-state-message-1646210](http://ibtimes.co.uk/pro-isis-hackers-hijack-800-us-schools-sites-saddam-hussein-photo-i-love-islamic-state-message-1646210)

<sup>10</sup> [ibtimes.co.uk/opdomesticterrorism-anonymous-hackers-take-down-over-dozen-neo-nazi-sites-new-wave-attacks-1647385](http://ibtimes.co.uk/opdomesticterrorism-anonymous-hackers-take-down-over-dozen-neo-nazi-sites-new-wave-attacks-1647385)

## КОМПРОМЕТАЦИЯ УЧЕТНЫХ ДАННЫХ



Больше всего пострадавших в США, Австралии и Японии



Наиболее атакуемые объекты



50%



32%



18%



29%



18%



11%

Больше всего пострадали

Ущерб > 14 млн долл. США

Пострадали > 57 млн человек

Подмены криптокошельков продолжают. В конце октября были зафиксированы атаки на оборудование с ОС ethOS, занимающееся майнингом Ethereum<sup>11</sup>. Злоумышленники сканировали интернет в поисках такого оборудования с заводскими учетными данными для SSH-соединения (ethos:live и root:live), чтобы получить к нему доступ и заменить идентификатор кошелька на свой собственный. По данным Bitdefender, на кошелек злоумышленников было сделано только десять денежных переводов на общую сумму около 600 \$.

### Как защититься организации

- + Применять парольную политику, предусматривающую строгие требования к минимальной длине и сложности паролей.
- + Не использовать одинаковые учетные записи и пароли для доступа к различным ресурсам.
- + Не хранить пароли пользователей в открытом виде (или в зашифрованном с помощью обратимого алгоритма).
- + Ограничить срок использования паролей (не более 90 дней).
- + Использовать двухфакторную аутентификацию там, где это возможно, например для защиты привилегированных учетных записей.
- + Своевременно удалять или блокировать корпоративные учетные записи бывших сотрудников.

### Как защититься обычному пользователю

- + Использовать 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 использовать один и тот же пароль для разных систем (для сайтов, электронной почты и др.).
- + Менять все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.
- + Использовать двухфакторную аутентификацию там, где это возможно, например для защиты электронной почты.

<sup>11</sup> [labs.bitdefender.com/2017/11/ethereum-os-miners-targeted-by-ssh-based-hijacker/](https://labs.bitdefender.com/2017/11/ethereum-os-miners-targeted-by-ssh-based-hijacker/)

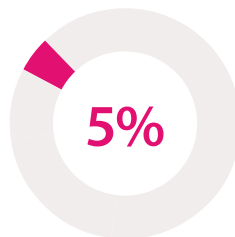
## DDoS



Наиболее атакуемые объекты



100%



Больше всего пострадали



50%



25%



13%

Больше всего пострадавших в Китае и США



Наиболее частыми объектами DDoS-атак остаются государственные веб-ресурсы, которые в этих случаях выступают своего рода площадкой для выражения различных общественных мнений. В октябре 2017 года проходил референдум о независимости Каталонии, в ходе которого более 90% жителей проголосовали за независимость, однако властями Испании мероприятие не было признано законным. Действия правительства вызвали недовольство со стороны многих граждан, а также спровоцировали серию DDoS-атак хактивистов Anonymous<sup>12</sup> на сайты автономного сообщества Мадрид, Конституционного суда Испании, сайты министерств экономики, развития, юстиции и других.



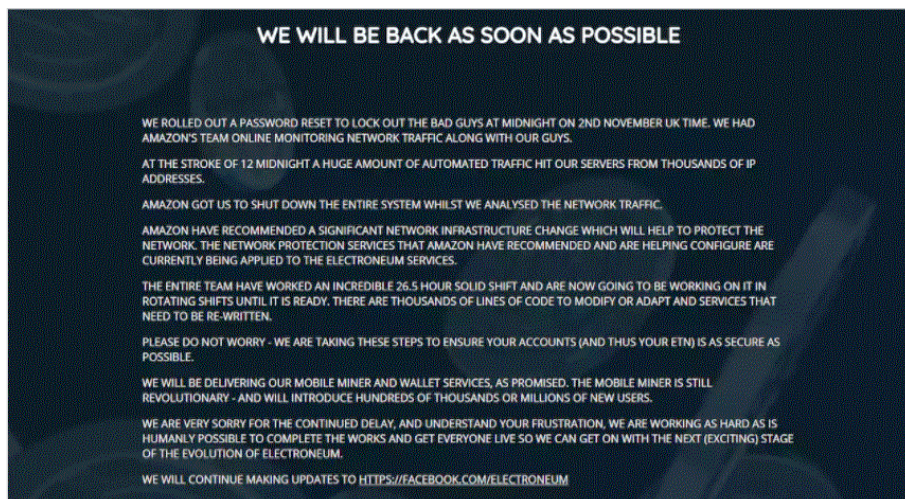
DDoS-атака на правительственный сайт Испании

Риск DDoS-атак особенно актуален для криптовалютных бирж и ICO, которые в последнее время собирают большие деньги, не уделяя достаточного внимания вопросам безопасности. Так, британский стартап Electroneum<sup>13</sup>, собравший в ходе своего ICO 40 млн долларов, стал жертвой преступников. В результате DDoS-атаки был заблокирован не только сайт, но и доступ инвесторов к их счетам: для того чтобы в ходе развития атаки не пострадали счета клиентов, Electroneum на всякий случай заблокировал и их.

<sup>12</sup> [politica.elpais.com/politica/2017/10/21/actualidad/1508574710\\_898791.html](http://politica.elpais.com/politica/2017/10/21/actualidad/1508574710_898791.html)

<sup>13</sup> [telegraph.co.uk/technology/2017/11/06/british-cryptocurrencyelectroneum-hit-cyber-attack-raising-30m/](http://telegraph.co.uk/technology/2017/11/06/british-cryptocurrencyelectroneum-hit-cyber-attack-raising-30m/)





DDoS на ICO Electroneum

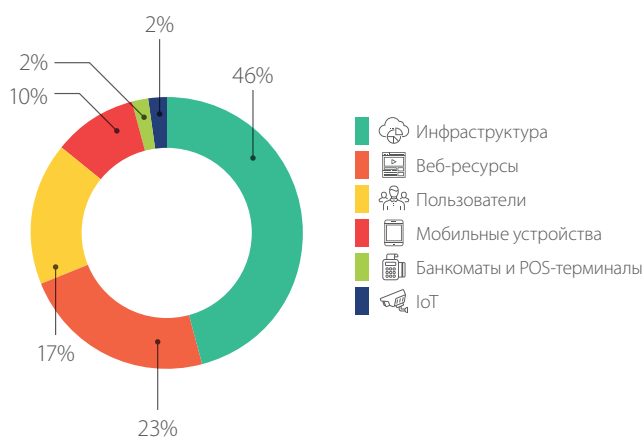
#### Как защититься организации

- + Настроить конфигурацию серверов и сетевых устройств таким образом, чтобы нейтрализовать типичные сценарии атаки (например, TCP- и UDP-флуд или множественные запросы к БД).
- + Отслеживать количество запросов к ресурсам в секунду.
- + Воспользоваться сервисом анти-DDoS.
- + При проведении ICO привлечь специалистов для анализа смарт-контрактов и комплексной защиты инфраструктуры от кибератак, например воспользовавшись услугами [ico.positive.com](http://ico.positive.com).



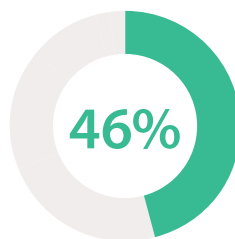
## ОБЪЕКТЫ АТАК

Мы видим, что в течение всего года распределение киберинцидентов по объектам атак в процентном соотношении меняется незначительно.



Распределение киберинцидентов по объектам

### ИНФРАСТРУКТУРА



Больше всего пострадавших в США, России, Южной Корее, Италии



Наиболее популярные методы атак

Больше всего пострадали

Ущерб > 143 млн долл. США



55%



14%



7%



22%



17%



9%

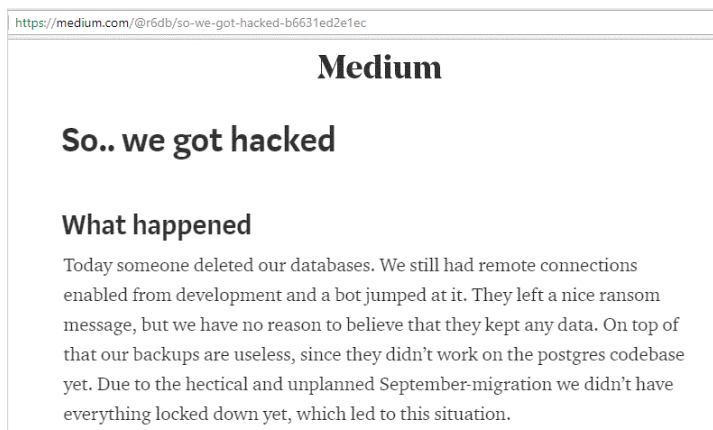
В инфраструктуре организации, как правило, присутствует множество бизнес-систем и компонентов, компрометация которых недопустима. Когда речь идет о банках, то одной из важнейших и наиболее хорошо защищаемых систем является система переводов SWIFT. В октябре злоумышленникам удалось внедрить вредоносное ПО в инфраструктуру и терминал для доступа в SWIFT<sup>14</sup> крупнейшего тайваньского банка Far Eastern International Bank и вывести с клиентских счетов в Шри-Ланку, Камбоджу и США сумму в размере 60 млн долларов. Однако благодаря своевременно принятым мерам практически все деньги удалось вернуть. Чуть позднее в октябре атаке подвергся непальский банк NIC Asia Bank<sup>15</sup>, и несмотря на то, что злоумышленникам удалось перевести через международную межбанковскую систему SWIFT 4 млн долларов, 3,9 из них удалось оперативно восстановить.

Киберпреступники высоко ценят свое время и стремятся максимально автоматизировать этапы атаки. Поэтому они все чаще используют ботов, которые самостоятельно ищут в интернете открытые порты, подбирают учетные данные к устройствам, доступным из сети, выявляют сайты, развернутые на уязвимых CMS. Зачастую объектами атак становятся незащищенные базы данных, которые злоумышленники находят в интернете с помощью скриптов, затем удаляют их содержимое и требуют выкуп за восстановление данных.

<sup>14</sup> [taipeitimes.com/News/front/archives/2017/10/08/2003679926](http://taipeitimes.com/News/front/archives/2017/10/08/2003679926)

<sup>15</sup> [bankinfosecurity.com/report-attackers-hacked-nepalese-banks-swift-server-a-10437](http://bankinfosecurity.com/report-attackers-hacked-nepalese-banks-swift-server-a-10437)

Осенью из-за забывчивости инженеров, не заблокировавших вовремя порты для удаленного подключения к серверу, была нарушена работа игрового сервиса R6DB<sup>16</sup>. Автоматизированный бот получил доступ к серверу, удалил БД PostgreSQL и оставил сообщение с требованием выкупа.



Атака на игровой сервис R6DB

В мире происходит глобальная информатизация, меняющая порядки во всех сферах, в том числе и в образовании. Школьный дневник теперь не спрятать от родителей, ведь доступ к оценкам в любое время можно получить через интернет. И мы отмечаем пугающую тенденцию среди подрастающего поколения: учащиеся взламывают компьютерную систему образовательного учреждения, чтобы подменить оценки. Например, в США<sup>17</sup> студент купил кейлоггер и, получив с его помощью доступ к компьютеру преподавателя, поменял оценку с F на A. В России аналогичный инцидент произошел в Новосибирске<sup>18</sup>, где старшеклассник с помощью вредоносного ПО повысил свои привилегии в сервисе «электронный дневник» до уровня администратора и исправлял оценки на более высокие. В ноябре по факту этого правонарушения было заведено уголовное дело (ч. 1 ст. 272 УК РФ), и теперь молодого человека ждет серьезное наказание.

Понедельник / 05.04	Домашнее задание		Оценка
Русский яз.	Упр. 72, 74, 75 (а - в)		
Математика	пар. 23, 24. Примеры - в прикрепленном файле	Контрольная работа "Дроби" Делает успехи	5
Русский яз.	Реферат		
История	Реферат		
Английский яз.	Принести книгу для чтения на англ.		4
Физкультура			5

Электронный дневник

Мы наблюдаем пугающую тенденцию к снижению возраста злоумышленников. Если прежде атаки выполняли опытные программисты, то сегодня мы все чаще видим несовершеннолетних, участвующих в киберпреступлениях. В интернете постоянно мелькает реклама легкого заработка, на которую реагируют подростки, оказываясь влутанными в мошеннические схемы (например, по обналичиванию украденных средств). Опытные киберпреступники, организаторы атак, стараются не рисковать и избегают действий, на которых их могут поймать. Они нанимают неопытных подростков, которые в погоне за деньгами (и по незнанию закона) выполняют различные поручения — и оказываются главными подозреваемыми при расследовании преступления. Мы прогнозируем, что ситуация будет только усугубляться.

<sup>16</sup> [medium.com/@r6db/so-we-got-hacked-b6631ed2e1ec](https://medium.com/@r6db/so-we-got-hacked-b6631ed2e1ec)

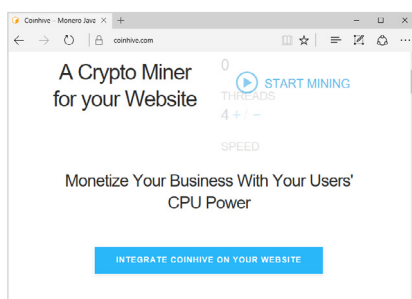
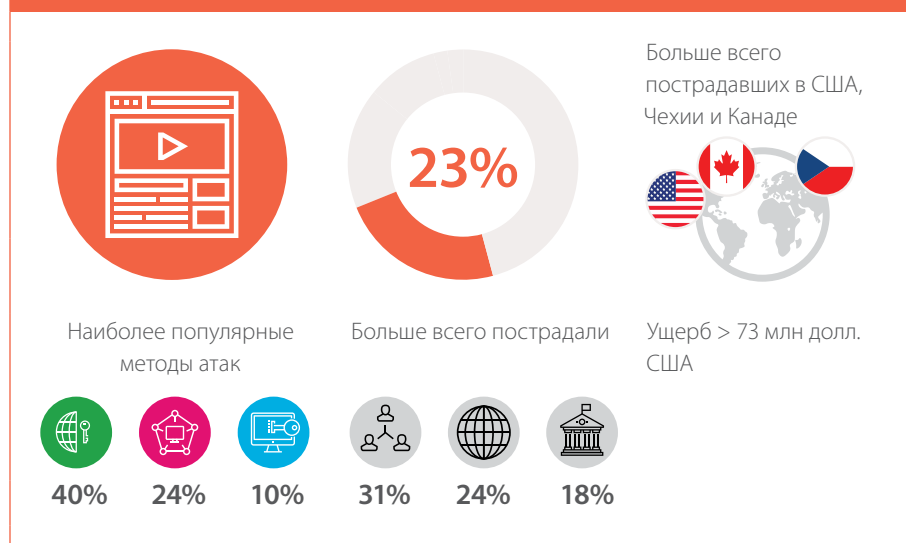
<sup>17</sup> [kansascity.com/news/local/article178522396.html](http://kansascity.com/news/local/article178522396.html)

<sup>18</sup> [54.mvd.rf/news/item/11475724/](http://54.mvd.rf/news/item/11475724/)

### Как защититься организации

- + Использовать строгую парольную политику, особенно для привилегированных учетных записей.
- + Не хранить чувствительную информацию в открытом виде или в открытом доступе.
- + Минимизировать привилегии пользователей и служб.
- + Эффективно фильтровать трафик для минимизации доступных внешнему злоумышленнику интерфейсов сетевых служб.
- + Использовать SIEM-системы для своевременного выявления атак.
- + Использовать межсетевой экран уровня приложений (web application firewall).
- + Регулярно проводить тестирование на проникновение для своевременного выявления новых векторов атак на внутреннюю инфраструктуру и оценки эффективности принятых мер по защите.

### ВЕБ-РЕСУРСЫ



Сервис для установки майнера  
в код веб-приложения

Похоже, что майнинг криптовалюты за счет пользователей сайта скоро будет популярней, чем монетизация с помощью контекстной рекламы. Один из сервисов, предлагающих владельцам сайтов зарабатывать за счет встраивания скриптов для майнинга в код ресурса, — Coinhive — стал жертвой киберпреступников в октябре<sup>19</sup>. В результате подмены параметров DNS JavaScript-код для майнинга загружался не с официального сайта, а с сервера злоумышленников. Таким образом вся криптовалюта попадала к преступникам вместо владельцев сайтов.

Другой сценарий атак это добавление скрипта для майнинга в код скомпрометированного веб-ресурса. Так, в октябре посетители официального сайта D-Link<sup>20</sup>, зашедшие в поисках патча для устранения уязвимостей, связанных с использованием протокола WPA2, генерировали для кого-то криптовалюту Monero.

Наиболее желанной целью злоумышленников в 2017 году стали криптовалютные биржи и сервисы. В IV квартале в результате атаки на сайт NiceHash<sup>21</sup> (сервиса покупки и продажи вычислительных мощностей для майнинга криптовалюты) была скомпрометирована их платежная система и украдены биткойны с кошельков пользователей на общую сумму 4700 BTC (что составляло порядка 62 млн \$).

<sup>19</sup> [coinhive.com/blog/dns-breach](https://coinhive.com/blog/dns-breach)

<sup>20</sup> [seekurity.com/blog/general/d-link-middle-east-dlink-mea-website-is-secretly-mining-cryptocurrencies/](https://seekurity.com/blog/general/d-link-middle-east-dlink-mea-website-is-secretly-mining-cryptocurrencies/)

<sup>21</sup> [reddit.com/r/NiceHash/comments/7i0s6o/official\\_press\\_release\\_statement\\_by\\_nicehash/](https://reddit.com/r/NiceHash/comments/7i0s6o/official_press_release_statement_by_nicehash/)

↑  
657  
↓

**Official press release statement by NiceHash** self:NiceHash  
Submitted 12 days ago by Andrej\_ID  - announcement

Unfortunately, there has been a security breach involving NiceHash website. We are currently investigating the nature of the incident and, as a result, we are stopping all operations for the next 24 hours.

Importantly, our payment system was compromised and the contents of the NiceHash Bitcoin wallet have been stolen. We are working to verify the precise number of BTC taken.

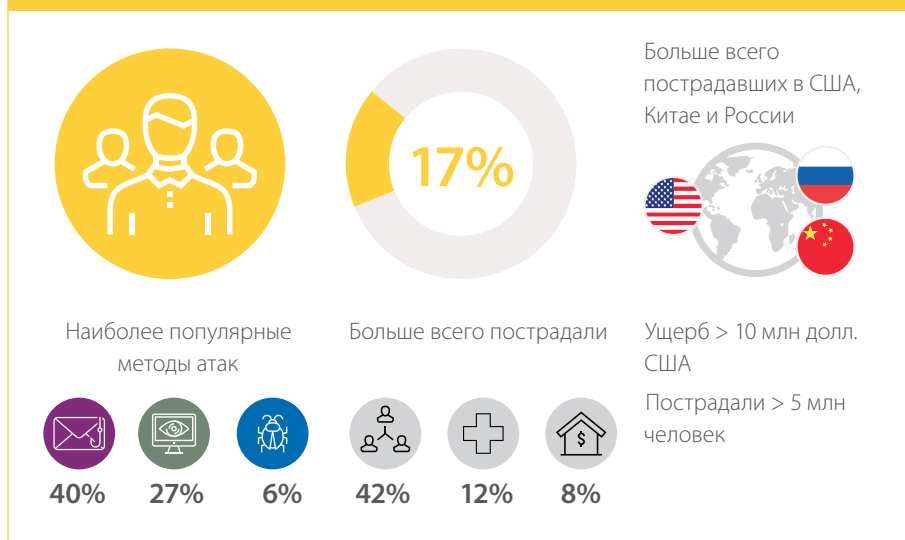
Clearly, this is a matter of deep concern and we are working hard to rectify the matter in the coming days. In addition to undertaking our own investigation, the incident has been reported to the relevant authorities and law enforcement and we are co-operating with them as a matter of urgency.

Сообщение от администрации сервиса NiceHash

### Как защититься организации

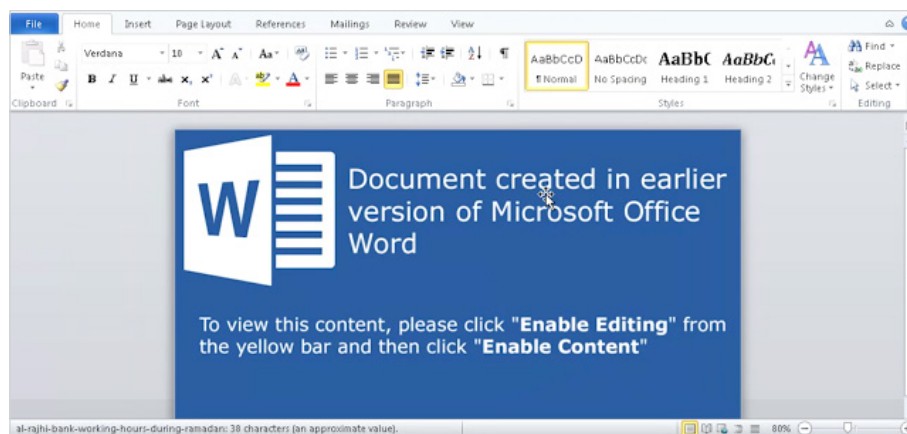
- + Использовать межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты.
- + Проводить регулярный анализ защищенности веб-приложений, включая анализ исходного кода.
- + Использовать строгую парольную политику, особенно для привилегированных учетных записей.
- + Своевременно обновлять используемое ПО.
- + Внедрить процессы обеспечения безопасности на протяжении всего цикла жизни веб-приложения.
- + При проведении ICO привлечь специалистов для анализа смарт-контрактов и комплексной защиты инфраструктуры от кибератак, например, воспользовавшись услугами [ico.positive.com](http://ico.positive.com).

### ПОЛЬЗОВАТЕЛИ



Чаще всего пользователи страдают от атак с использованием социальной инженерии. Однако с ростом компьютерной грамотности и осведомленности людей в вопросах безопасности злоумышленникам приходится придумывать новые сценарии. Например, как рассказывают исследователи Cisco Talos<sup>22</sup>, для распространения банковского трояна Zeus Panda злоумышленники использовали взломанные веб-ресурсы. Необычность этого метода заключалась в том, что злоумышленники с помощью SEO поднимали позиции этих фишинговых сайтов на странице поисковой выдачи. Для этого на скрытых страницах размещали специально отобранные ключевые слова, а рейтинг увеличивали с использованием SEO-ботнета. Когда пользователь переходил на один сайт, вредоносный скрипт переадресовывал его через несколько других веб-ресурсов (поднимая тем самым их рейтинг), а затем загружал на компьютер жертвы зараженный документ Word. В случае открытия этого документа макрос устанавливал банковский троян, который следил за всеми действиями пользователя.

<sup>22</sup> [blog.talosintelligence.com/2017/11/zeus-panda-campaign.html](http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html)



Документ, загружающий Zeus Panda на компьютер жертвы

Другая популярная категория атак на пользователей это кража их учетных и персональных данных, а также данных их банковских карт. Примечательно, что большинство людей даже не подозревают о том, что стали жертвой. В октябре стало известно о масштабной утечке данных 46 млн малайзийцев<sup>23</sup>. База содержала данные абонентов 12 операторов сотовой связи, а также персональные данные 80 тыс. пациентов больницы, и продавалась в даркнете.

#### Как защититься организации

- + Регулярно напоминать клиентам о правилах безопасной работы в интернете, разъяснять методы атак и способы защиты. Предостерегать 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. Разъяснять клиентам порядок действий в случае подозрений о мошенничестве.
- + Уведомлять клиентов о событиях, связанных с информационной безопасностью (например, о попытках авторизации в системе с учетной записью клиента или о транзакциях в интернет-банкинге).
- + Регулярно проводить анализ защищенности веб-приложений, включая анализ исходного кода, с целью выявления и устранения уязвимостей, позволяющих проводить атаки, в том числе на клиентов приложения.

#### Как защититься обычному пользователю

- + Использовать эффективные средства антивирусной защиты на всех устройствах.
- + Своевременно обновлять используемое ПО.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности.
- + С осторожностью относиться к сайтам с некорректными сертификатами (когда браузер предупреждает об этом) и учитывать, что введенные на них данные могут быть перехвачены злоумышленниками.
- + Проверять все вложения, полученные по электронной почте, с помощью антивирусного ПО.
- + Не загружать файлы с подозрительных веб-ресурсов или из других неизвестных источников.
- + Использовать 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 использовать один и тот же пароль для разных систем (для сайтов, электронной почты и др.).
- + Менять все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.

<sup>23</sup> [bankinfosecurity.com/malaysia-stung-by-massive-data-breach-affecting-millions-a-10426](http://bankinfosecurity.com/malaysia-stung-by-massive-data-breach-affecting-millions-a-10426)

## МОБИЛЬНЫЕ УСТРОЙСТВА



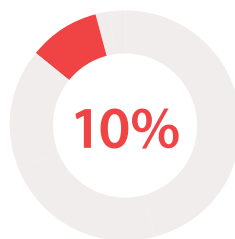
Наиболее популярные  
методы атак



93%



4%



Больше всего пострадали



82%



7%



7%

Больше всего  
пострадавших в США,  
России и Южной Корее



Заражены > 20 млн  
устройств

Все атаки на мобильные устройства в IV квартале 2017 года проводились с использованием вредоносного ПО. Примечательно, что в большинстве случаев вредоносное ПО попадало на телефон жертвы через официальный магазин приложений.

Последнее время вредоносное ПО для мобильных телефонов становится универсальным и, один раз оказавшись на телефоне жертвы, может участвовать в различных сценариях атак. Например, после установки поддельного дополнения к игре Minecraft из Google Play<sup>24</sup> телефон жертвы попадал в ботнет. Злоумышленники использовали этот ботнет для заработка на рекламных объявлениях, которые демонстрировали на зараженных смартфонах. Но по желанию преступников ботнет мог использоваться и для других целей, например для реализации DDoS-атак или для заработка по модели cybercrime as a service (злоумышленники продают возможность загрузить ВПО на устройства, входящие в ботнет, другим людям).

Банковский троян LokiBot<sup>25</sup> умеет не только подделывать интерфейс мобильного банка, чтобы получить учетные данные и, соответственно, доступ к счетам жертвы, но и рассылать с зараженного устройства спам или переходить по нужным ссылкам в браузере. А если ему не предоставить административные права, то этот троян выступает в роли вымогателя и блокирует экран, шифрует данные и требует выкуп.

Скрытый майнинг криптовалюты не обошел стороной и смартфоны. Сразу несколько мобильных троянов (ANDROIDOS\_JSMINER, ANDROIDOS\_CPUMINER, ANDROIDOS\_KAGECOIN<sup>26</sup> и их модификации) использовали вычислительные мощности смартфонов для майнинга различных криптовалют (Magicoин, Feathercoin, VertCoin, MyriadCoin, Unitus). Распространялось это вредоносное ПО как через фишинговые SMS-сообщения, так и под видом легальных приложений в Google Play. На момент исследования прибыль злоумышленников составила порядка 170 долларов.

Mining on 5 wallets , 1623 miners						
Name	Amount	Diff	Block	TTF***	Hash**	Profit*
Magicoин (m7m)	9.365 XMG	5 951	1 531 138	68 mins	6.2 Mh/s	1.12791
Feathercoin (neoscrypt)	40.01 FTC	31.559	1 938 557	3 weeks	60.8 kh/s	0.19824
VertCoin (lys2v2)	50.03 VTC	70 983 k	813 053			0.00000
MyriadCoin (yescrypt)	250 XMY	0.204	2 224 463			0.00000
Unitus (yescrypt)	31.481 URS	0.275	1 167 904			0.00000

\*\*\* estimated average time to find a block at full pool speed

\*\* approximate from the last 5 minutes submitted shares

\* 24h estimation from network difficulty in mBTC/Mh/day (mBTC/Gh/day for sha256 and blake algos)

Прибыль злоумышленников от майнинга на смартфонах жертв

<sup>24</sup> [symantec.com/connect/blogs/android-malware-google-play-adds-devices-botnet-and-performs-ddos-attacks](https://symantec.com/connect/blogs/android-malware-google-play-adds-devices-botnet-and-performs-ddos-attacks)

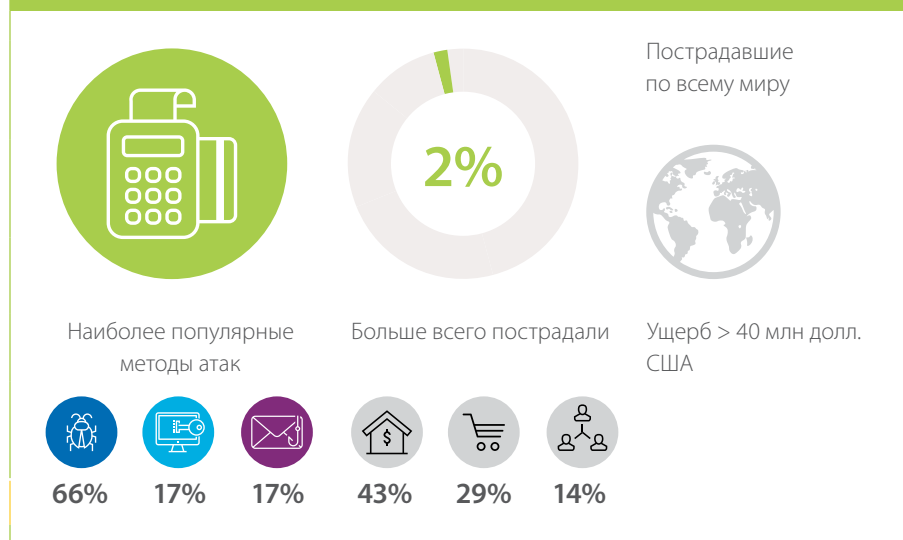
<sup>25</sup> [kaspersky.ru/blog/lokibot-trojan/19131/](https://kaspersky.ru/blog/lokibot-trojan/19131/)

<sup>26</sup> [blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/](https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/)

### Как защититься обычному пользователю

- + Своевременно обновлять используемое ПО.
- + Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно полученным в SMS- и MMS-сообщениях, по почте или в мессенджере.
- + Отключить на мобильных устройствах опцию, разрешающую загрузку и установку приложений из неизвестных источников.
- + Перед установкой приложения обращать внимание на разрешения, которые оно запрашивает, и оценивать их необходимость. Возможно, риск хищения данных окажется весомее установки приложения, которому требуются избыточные привилегии.
- + Не устанавливать неофициальные прошивки и не «рутировать» устройство.
- + Не подключать услугу «Автоплатеж» для автоматического пополнения баланса телефонного номера при снижении до определенной суммы. Ведь если на устройство попадет вирус, отправляющий SMS на платные номера, баланс будет пополняться до тех пор, пока не закончатся деньги на банковском счете.
- + Использовать 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 использовать один и тот же пароль для разных систем (для сайтов, электронной почты, мобильного банка и др.).
- + Менять все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.
- + Использовать двухфакторную аутентификацию там, где это возможно, например для защиты электронной почты.

### БАНКОМАТЫ И POS-ТЕРМИНАЛЫ



В IV квартале люди особенно охотно совершают покупки в магазинах, ведь в это время проходят распродажи и массовые закупки рождественских и новогодних подарков. А злоумышленники тем временем продолжают развивать технологии атак на POS-терминалы и воровать данные платежных карт. В ноябре была замечена новая вариация FrameworkPOS (с фрагментами TRINITY, BlackPOS и BrickPOS) — вредоносное ПО GratefulPOS<sup>27</sup>. На платежный терминал это вредоносное ПО устанавливается вручную, преимущественно из скомпрометированной сети организации, затем извлекает данные платежных карт из оперативной памяти устройства и отправляет их на управляющий сервер, обходя стандартную защиту, поскольку вместо прямого доступа в интернет использует обращения к внутренним DNS-серверам.

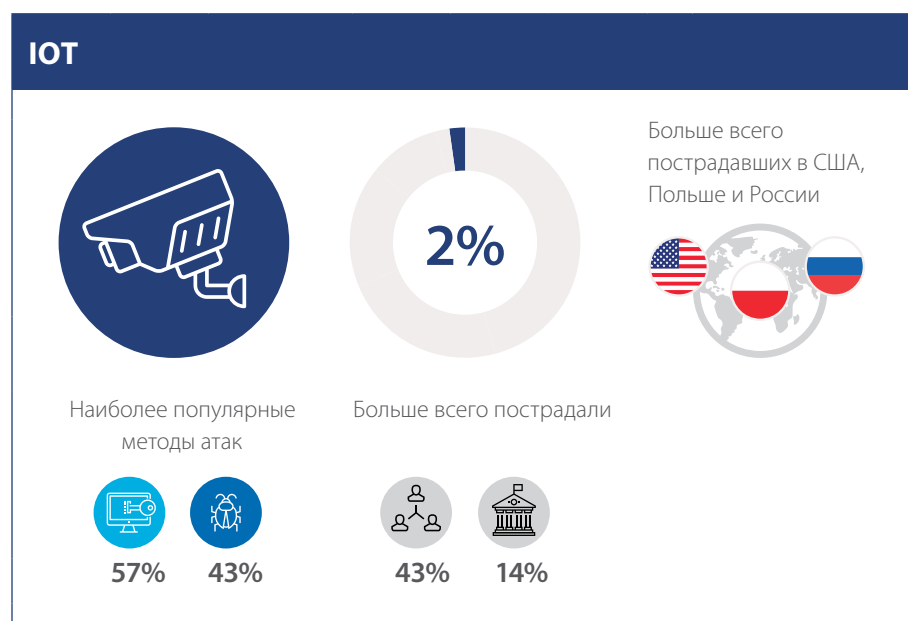
<sup>27</sup> [community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season](https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season)

Злоумышленники все чаще нацеливаются на интернет-магазины и POS-терминалы, поскольку их уровень защищенности сейчас значительно ниже, чем у онлайн-банков, и, соответственно, получить данные банковских карт там оказывается проще.

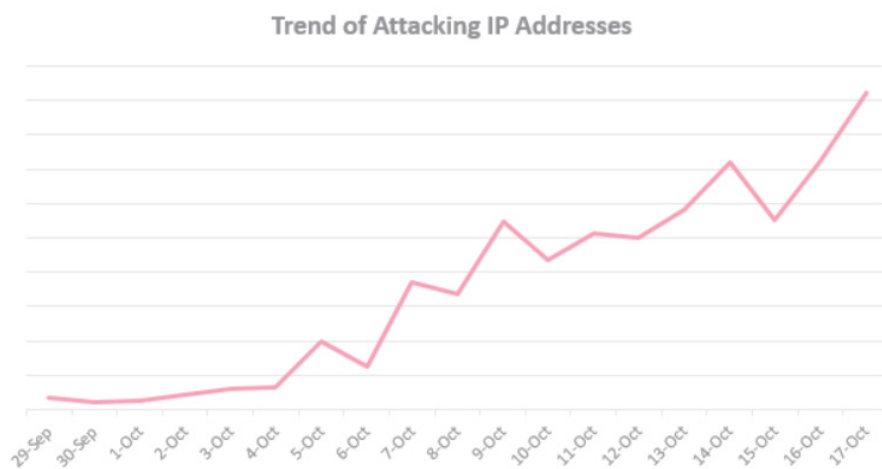
#### Что предпринять вендору

В данной ситуации организации, занимающиеся разработкой и обслуживанием платежных терминалов, банкоматов и ПО для этих устройств, должны принимать меры защиты:

- + использовать специализированное ПО application control на всех банкоматах;
- + шифровать чувствительные данные, передаваемые между устройством и процессинговым центром;
- + проверять целостность входящего трафика от процессингового центра;
- + своевременно устанавливать актуальные обновления.



Ботнеты продолжают пополняться IoT-устройствами. Стало известно о новом вредоносном ПО Reaper, быстро распространившемся на 2 млн девайсов<sup>28</sup> (среди них D-Link, Netgear, Linksys, AVTech, Vacron, JAWS и GoAhead). Зараженные устройства (маршрутизаторы, системы видеонаблюдения, IP-камеры, сетевые накопители и др.) автоматически рассылали вредоносное ПО на другие гаджеты, находящиеся в той же сети.



Динамика распространения ВПО Reaper

<sup>28</sup> [research.checkpoint.com/new-iot-botnet-storm-coming/](https://research.checkpoint.com/new-iot-botnet-storm-coming/)



Примечательно, что несмотря на заложенную в Reaper функциональность для проведения DDoS-атак, пока что их не было зафиксировано. Возможно, владелец ботнета выжидает, когда в его команде окажется еще больше устройств по всему миру. Многие производители зараженных IoT-устройств уже выпустили обновления безопасности, однако не все имеют возможность их установить, например из-за отсутствия понятного интерфейса или из-за заводского пароля, неизвестного пользователю.

#### Что предпринять вендору

- + Внедрить процессы обеспечения безопасности на всех стадиях разработки ПО.
- + Проводить анализ защищенности IoT-устройств перед выпуском прошивки.
- + Своевременно устранять выявленные уязвимости, в том числе по обращениям пользователей и исследователей ИБ.

#### Как защититься организации

- + Сменить стандартные пароли на новые, удовлетворяющие строгой парольной политике.
- + Следить, чтобы IoT-устройства, доступные из интернета, не были подключены в важные сегменты сети.
- + Своевременно обновлять используемое ПО по мере выхода патчей.

#### Как защититься обычному пользователю

- + Сменить стандартные пароли на новые. Использовать сложные пароли, состоящие из незначущих комбинаций букв, цифр и знаков, длиной не менее 8 символов.
- + Своевременно обновлять используемое ПО по мере выхода патчей.
- + При обнаружении уязвимости оповещать вендора.

## ВЫВОДЫ

Подводя итоги IV квартала 2017 года, мы отмечаем следующие тенденции:

- + Злоумышленники придумывают все новые способы распространения вредоносного ПО, все чаще задействуют в своих атаках уязвимые веб-ресурсы.
- + Для продвижения фишинговых веб-ресурсов в поисковых строках киберпреступники начали применять SEO. Для этого они разрабатывают специальные ботнеты, которые переходят по нужной ссылке и тем самым поднимают рейтинг сайта, или добавляют в код специальные инструкции, пробрасывающие посетителя через несколько веб-сайтов, и таким способом тоже увеличивают рейтинг.
- + Появляется новая тенденция по использованию вымогательского ПО не с целью финансовой выгоды, а для сокрытия истинных мотивов киберпреступных действий. Причем данные в ходе таких атак часто уничтожаются безвозвратно.
- + В ходе атак на банки злоумышленники все чаще пытаются вывести деньги через систему межбанковского взаимодействия SWIFT, однако в большинстве случаев потерянные средства удается вернуть.
- + Средний возраст злоумышленника снижается. Мы все чаще видим несовершеннолетних, пойманных на совершении киберпреступления. И дальше ситуация будет только усугубляться.
- + Мир помешался на криптовалюте, и пока одни вкладывают все свои сбережения в нестабильную валюту на бирже, другие пытаются сгенерировать ее за чужой счет. Пользователей охватила волна атак, пожирающая вычислительные мощности устройств. Злоумышленники «майнят» криптовалюту на компьютерах, серверах, на мобильных телефонах.

---

## О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». 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.