АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ

II КВАРТАЛ 2017 ГОДА

POSITIVE TECHNOLOGIES

СОДЕРЖАНИЕ

Обозначения ... 3
Введение ... 4
Резюме ... 4
Динамика количества инцидентов ... 6
Методы атак ... 7
- Использование вредоносного ПО ... 7
- Компрометация учетных данных ... 9
- Социальная инженерия ... 10
- Эксплуатация уязвимостей ПО ... 12
- Эксплуатация веб-уязвимостей ... 13
- DDoS ... 14

Объекты атак ... 15
- Инфраструктура ... 15
- Веб-ресурсы ... 16
- Пользователи ... 17
- Мобильные устройства ... 18
- Банкоматы и POS-терминалы ... 19
- IoT ... 20

Выводы ... 22

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 организации


Медицинские учреждения


Сфера образования


Оборонные предприятия


Промышленные компании


Онлайн-сервисы


Сфера услуг


Транспорт


Разработка ПО


Розничная торговля


Частные лица


Другие сферы

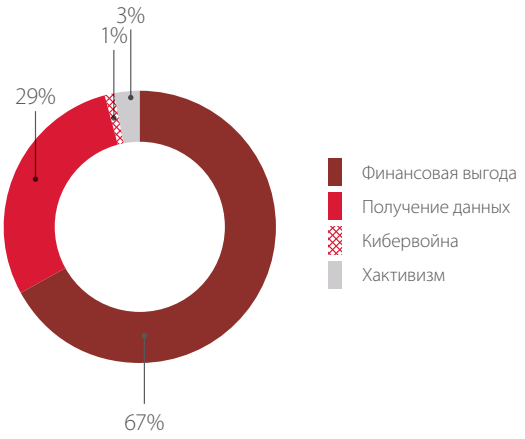
ВВЕДЕНИЕ

Пока все следили за развитием событий, связанных с нашумевшими шифровальщиками WannaCry и NotPetya, злоумышленники не сидели сложа руки. Продолжая ежеквартальный выпуск обзоров, мы делимся информацией об актуальных угрозах информационной безопасности, основанной на собственной экспертизе, результатах многочисленных расследований, а также данных авторитетных источников.

РЕЗЮМЕ

Две трети атак (67%) были совершены с целью получения прямой финансовой выгоды (например, за счет получения выкупа за восстановление данных, зашифрованных трояном) и еще 29% — с целью получения данных.

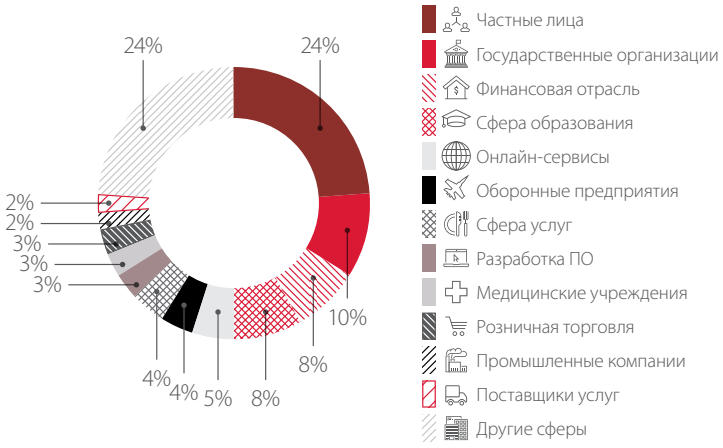
Больше половины атак (55%) носили массовый характер и проводились в основном с помощью вредоносного программного обеспечения (ВПО).



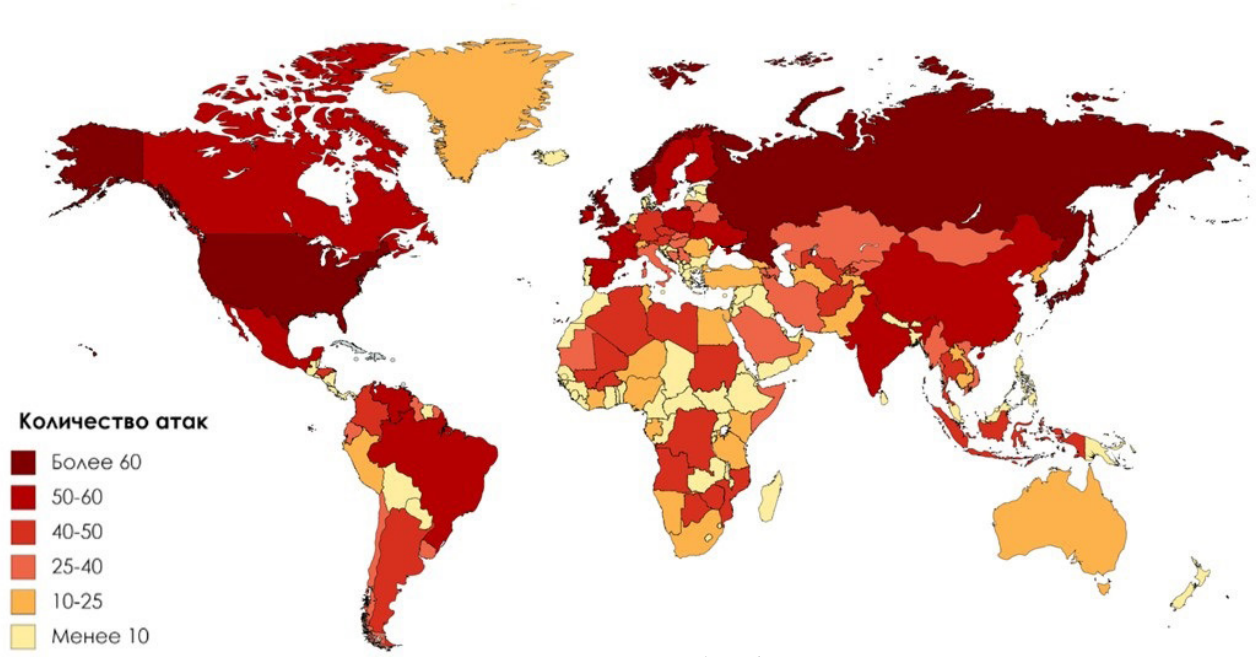
Мотивы злоумышленников

Во II квартале злоумышленники проявили повышенный интерес к частным лицам, на них (а точнее на их деньги и данные) было направлено 24% атак.

США и Россия по-прежнему наиболее частые жертвы кибератак, однако во II квартале 2017 года больше четверти атак (28%) были масштабные и затронули одновременно десятки стран и сотни (в отдельных случаях тысячи) компаний. В большинстве массовых атак было невозможно отнести инцидент к одной из перечисленных отраслей, в таком случае его относили к категории «Другие сферы», этим объясняется столь существенная ее доля.



Категории жертв, пострадавших от атак, совершенных во II квартале 2017 года

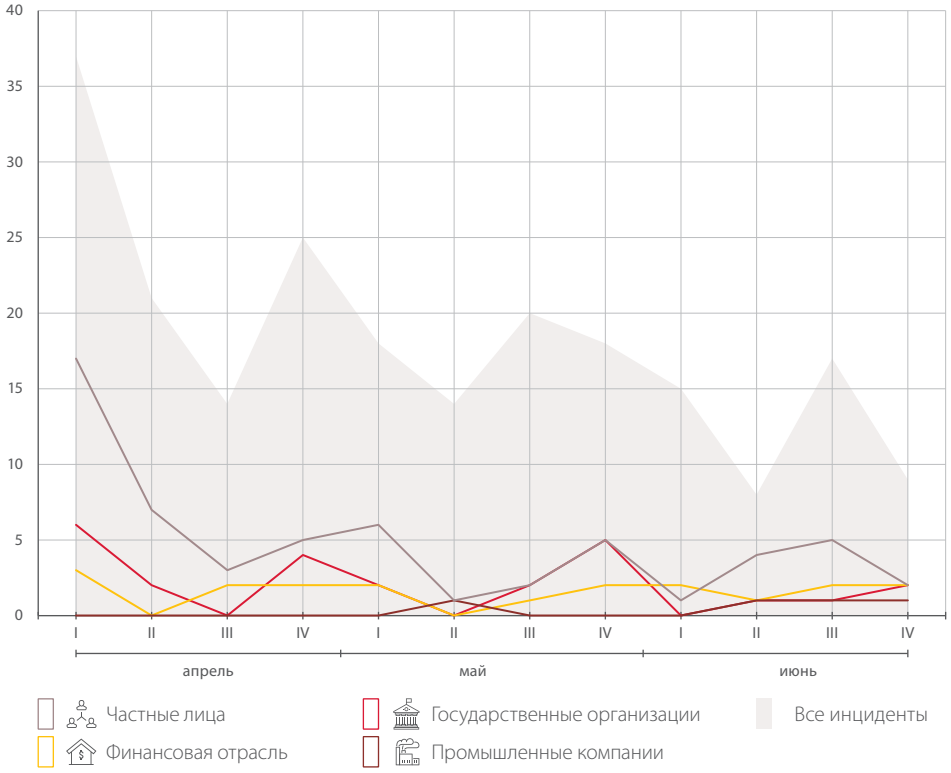


География кибератак во II квартале 2017 года

		Отрасль											
		Финансовая отрасль	Государственные организации	Медицинские учреждения	Сфера образования	Оборонные предприятия	Промышленные компании	Онлайн-сервисы	Сфера услуг	Частные лица	Разработка ПО	Розничная торговля	Другие сферы
Объект	Инфраструктура	5	13	4	10	7	4	2	2	8	4		27
	Веб-ресурсы	9	7	1	5	1		9	2	7	2	4	3
	Пользователи	1	1	3	3	1		1		28	1		1
	Банкоматы и POS-терминалы	3							2			3	
	Мобильные устройства		1			1			3	15	1		
	Сетевое оборудование и периферийные устройства												1
	IoT												5
Метод	Атаки с использованием ВПО	7	4	2	2	1	3		4	28	3	5	20
	Компрометация учетных данных	1	7	2	2	2		3	1	13	1	1	
	DDoS	2	3					1			1		1
	Социальная инженерия	3	2		5	3			1	10	1		5
	Эксплуатация уязвимостей в ПО	2	5	2	3	2		2	1	3	2		9
	Эксплуатация веб-уязвимостей	3	3	2	4			5	2	1		1	2
	Неизвестен				2	2	1	1		2			
Мотив	Финансовая выгода	16	9	8	14	1	3	10	7	37	8	5	23
	Кибершпионаж	2	12		4	7		2	2	18		1	13
	Хактивизм		3			2							1
	Кибервойна						1						

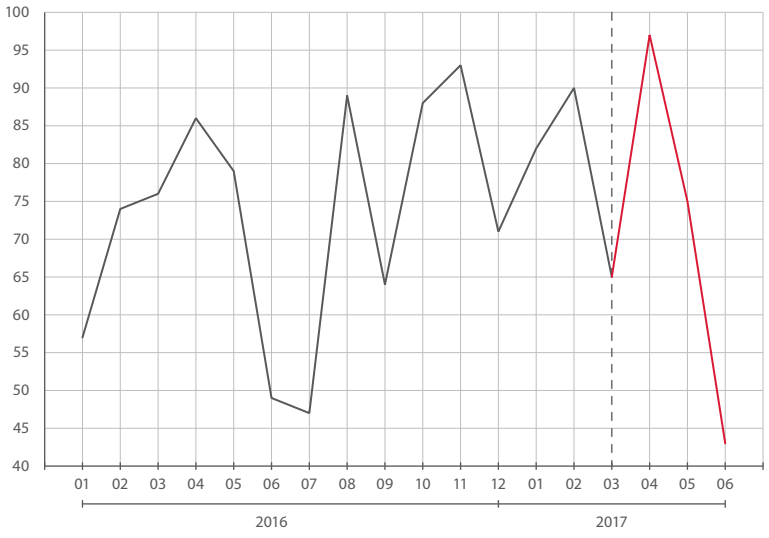
Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) и отраслям

ДИНАМИКА КОЛИЧЕСТВА ИНЦИДЕНТОВ



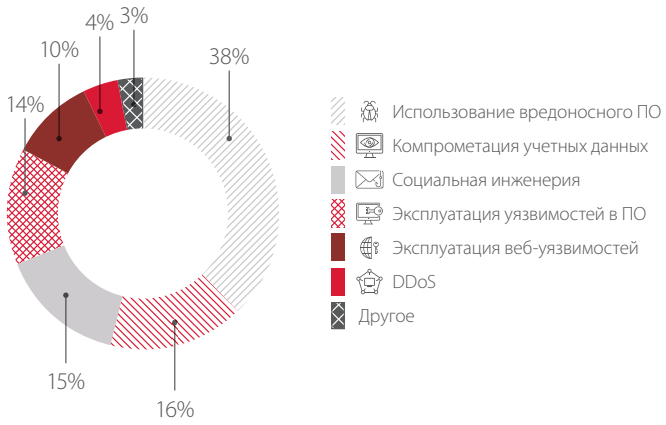
Количество инцидентов во II квартале 2017 года

В июне мы отметили уменьшение количества уникальных инцидентов: видимо, у хакеров тоже бывает отпуск :) В это время преобладали масштабные кампании, направленные на большое количество организаций, которые в ходе анализа учитывались как один инцидент. Если проводить аналогию с 2016 годом, то после летнего затишья (в июне и июле) злоумышленники могут активизироваться в осенние месяцы (октябрь, ноябрь), поэтому стоит оставаться начеку.



Количество инцидентов в 2016 и 2017 годах

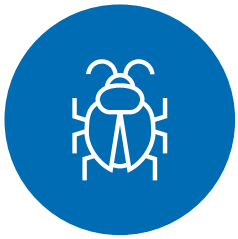
МЕТОДЫ АТАК

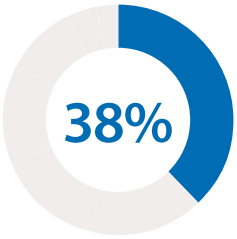


Распределение киберинцидентов по методам атак

При анализе инцидентов мы рассматриваем только уникальные события, таким образом все происшествия, связанные с заражением одним трояном или его модификациями, учитываются как один масштабный инцидент. Доля атак с использованием ВПО выросла на 3%. Социальная инженерия применялась чаще, чем в I квартале, и составила 15% всех атак. Во II квартале сократилось количество DDoS-атак, при этом появились новые ботнеты из IoT-устройств, поэтому в III квартале можно ожидать роста этой категории атак.

ИСПОЛЬЗОВАНИЕ ВРЕДОНОСНОГО ПО





Пострадавшие по всему миру

Наиболее атакуемые объекты:

44% 20% 13%

Больше всего пострадали:

35% 20% 9%

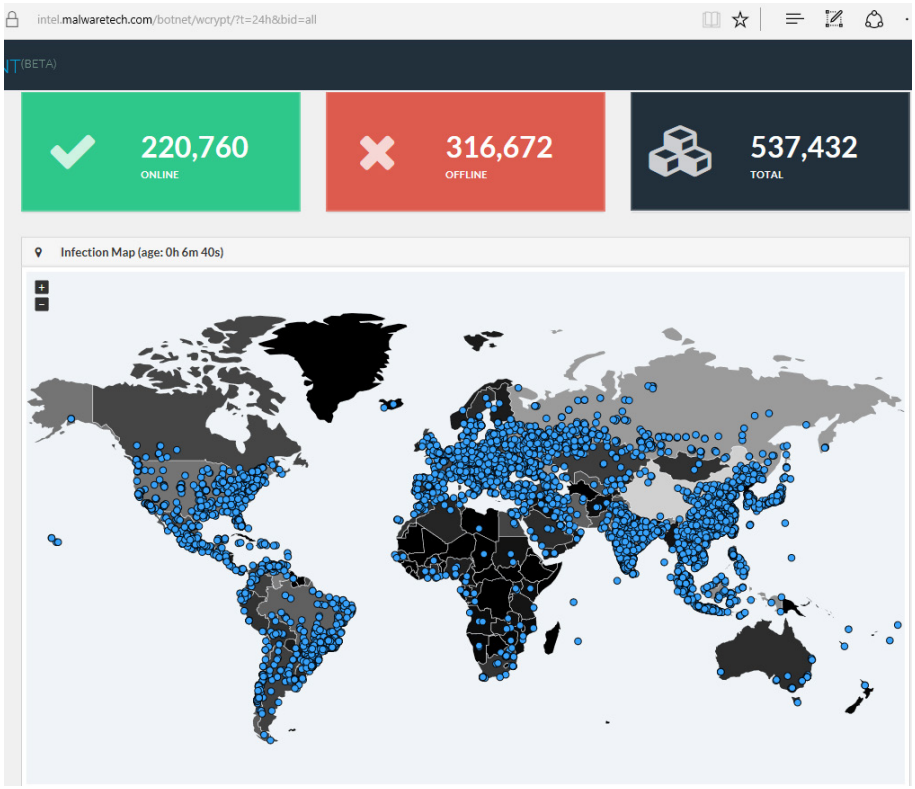
Ущерб > 1 млрд долл. США

Заражено > 1 млн устройств

Тема вредоносного ПО, шифрующего данные пользователей и требующего выкуп за расшифровку, совсем не нова, однако именно она была самой обсуждаемой в мировом ИБ-сообществе в мае и июне 2017 года. Компании как минимум в 150 странах мира понесли серьезные убытки из-за нарушений в работе информационных инфраструктур, данные в которых были зашифрованы троянами-вымогателями.

Эпидемия WannaCry (WanaCypt0r, WCry)[1] показала, что, не открывая подозрительные письма, не переходя по подозрительным ссылкам, можно все равно стать жертвой. По данным Intel[2], общее количество зараженных компьютеров превысило 530 тысяч. Несмотря на то что на биткойн-кошельки разработчиков WannaCry от жертв поступило всего около 50 BTC (128 000 долл. США), общий ущерб компаний составил более миллиарда долларов.

1 www.ptsecurity.com/upload/corporate/ru-ru/analytics/WannaCry-analytics-rus.pdf
2 intel.malwaretech.com/botnet/wcrypt/



Карта распространения WannaCry

Другая масштабная вредоносная кампания в конце июня была вызвана шифровальщиком NotPetya (также известным под именами ExPetr, PetrWrap, Petya, Petya.A и др.)[3]. Отличительной чертой этой эпидемии было то, что целью преступников не была финансовая выгода, они не стремились рассылать ключ восстановления в обмен на выплаты. ВПО распространялось для вывода из строя информационных систем, уничтожения файлов и саботажа. Однако злоумышленники допустили ошибки в коде при реализации алгоритма шифрования, что позволило экспертам Positive Technologies найти возможность восстановления данных в тех случаях, когда троян NotPetya имел административные привилегии и зашифровал жесткий диск целиком[4]. Однако более 40 жертв заплатили выкуп на общую сумму, эквивалентную 10 000 долл. США. Исходный вектор заражения NotPetya был направлен на украинские организации и реализован через бэкдор в программе бухгалтерского учета M.E.Doc[5]. ВПО попадало на компьютеры жертв вместе с официальными обновлениями и запускало в зараженной системе другое ВПО. Таким образом, вредоносная кампания была хорошо спланирована и реализована через атаку на разработчика ПО и включала компрометацию сервера обновлений и получение доступа к исходному коду программы.

Кроме того, во II квартале получили популярность и другие вредоносные программы, такие как семейство шифровальщиков-вымогателей Jaff, распространяемое через PDF-документы, прикрепленные к спам-сообщениям электронной почты[6], и SOREBRECT, внедряющееся в процесс Windows svchost.exe с помощью легитимной утилиты командной строки PsExec и уничтожающее исходный вредоносный файл[7].

Одновременно с эпидемией WannaCry мы наблюдали инциденты, связанные с другим ВПО (Adylkuzz[8]), использовавшим ту же уязвимость MS17-010[9]. Это ВПО не стало столь популярным в СМИ, поскольку не требовало выкуп. Однако большое количество компьютеров было заражено, а многие жертвы при этом не знали, что оказались атакованы. Исходный вектор заражения был аналогичен WannaCry: им служил доступный из сети Интернет уязвимый узел,

3 www.ptsecurity.com/ru-ru/about/news/283092/
4 habrahabr.ru/company/pt/blog/332618/
5 blog.talosintelligence.com/2017/07/the-medoc-connection.html
6 isc.sans.edu/forums/diary/Jaff+ransomware+gets+a+makeover/22446/
7 blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/
8 securingtomorrow.mcafee.com/mcafee-labs/adylkuzz-coinminer-spreading-like-wannacry/
9 technet.microsoft.com/en-us/library/security/ms17-010.aspx

на котором не были установлены актуальные обновления ПО и ОС. Интересна была цель атакующих: они использовали вычислительные мощности зараженных компьютеров для генерации криптовалюты. При анализе транзакций известного нам кошелька злоумышленника мы подсчитали, что подконтрольные вычислительные мощности позволяют хакеру зарабатывать порядка 2000 долл. США в сутки.

Во II квартале набирает обороты тренд «вымогатели как услуга» (ransomware as a service), о котором мы рассказывали в первом квартале[10]. Появляются новые сервисы по сдаче троянов в аренду, например дистрибьютор Petya или Mischa получает от 25% до 85% от суммы платежей жертв[11], а другой троян-шифровальщик Karmen продается на черном рынке за 175 долл. США[12].

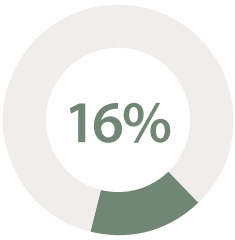
Как защититься организации

+ 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 в том случае, 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.

КОМПРОМЕТАЦИЯ УЧЕТНЫХ ДАННЫХ



Больше всего пострадавших в США, России и Южной Корее

Наиболее атакуемые объекты:

42% 36% 18%

Больше всего пострадали:

39% 21% 9%

Ущерб > 20 млн долл. США

Пострадали > 1,5 млн человек

Компрометация учетных данных широко используется злоумышленниками как в ходе целенаправленного воздействия на инфраструктуру организаций, так и в ряде атак на частных лиц. Например, взломанные аккаунты в социальных сетях или адреса электронной почты

10 www.ptsecurity.com/upload/corporate/ru-ru/analytics/Current-Cyberattacks-rus.pdf
11 www.bleepingcomputer.com/news/security/petya-and-mischa-ransomware-affiliate-system-publicly-released/
12 www.recordedfuture.com/karmen-ransomware-variant/

используются хакерами для спам-рассылок, а также для публикации различной информации от лица жертвы[13].

Истории о вымогательском ПО неразрывно связаны с криптовалютой, поскольку злоумышленники предпочитают брать выкуп в биткойнах. Однако в последнее время выросло количество атак на биткойн-кошельки. Так, от компрометации учетных данных пользователей пострадали сразу две крупнейшие криптовалютные биржи Южной Кореи. Получив доступ к персональным данным 31 800 пользователей Bithumb[14], злоумышленники затем смогли получить доступ и к их счетам. Потери от этой атаки оценили в 1 миллиард вон (890 000 долл. США). А в ходе атаки на Tapizon злоумышленники получили доступ к четырем кошелькам и в общей сложности похитили около 3816 биткойнов (5,3 млн долл. США)[15].

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 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.
+ Для хранения криптовалюты[16] рекомендуется использовать «холодный» кошелек, доступ к которому невозможен по сети Интернет. Примерами могут служить бумажные или аппаратные кошельки, кошельки с мультиподписью или с офлайн-подписью транзакций.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Больше всего пострадавших в США, Великобритании, России

Наиболее атакуемые объекты:

63% 37%

Больше всего пострадали:

33% 17% 13%

Ущерб > 50 тыс. долл. США

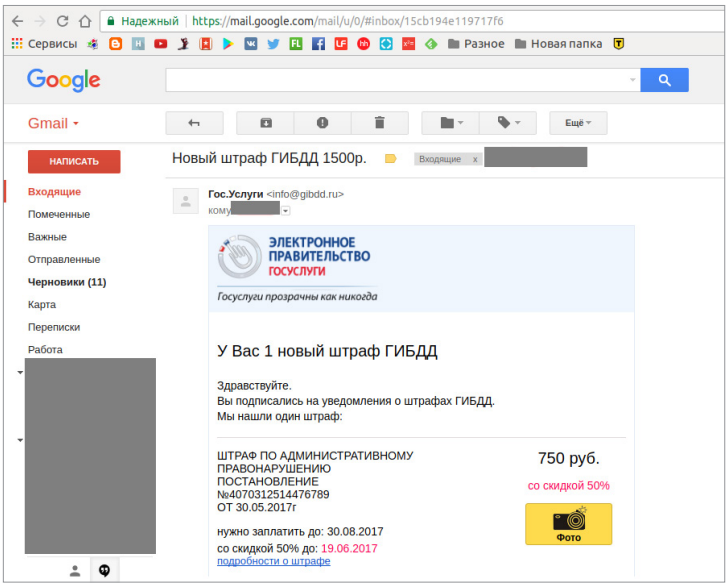
Пострадали > 500 тыс. человек

13 news.softpedia.com/news/hacktivist-defaces-250-isis-twitter-accounts-with-adult-content-515153.shtml
14 xakep.ru/2017/07/05/bithumb-hack/
15 happycoin.club/koreyskaya-birzha-yapizon-povtorit-put-bitfinex-i-vyipustit-dolgovyie-tokenyi-fei/
16 Согласно ст. 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)» выпуск на территории Российской Федерации денежных суррогатов запрещен.

Во II квартале 2017 года выросло количество атак с использованием социальной инженерии. В частности, группировка Cobalt, деятельность которой мы отмечаем с 2016 года, продолжает атаковать банки по всему миру, используя новые схемы проникновения в целевую систему[17]. Масштаб их кампаний значительно увеличился.

Конечно, от социотехнических атак страдают не только организации, нередки случаи, когда целью нарушителей становятся обычные люди. Например, в ходе фишинговой кампании злоумышленники с помощью спам-рассылок заманивали потенциальных жертв на поддельные страницы PayPal и выманивали у них данные банковских карт и другую чувствительную информацию[18]. Киберпреступники не подменяли URL своего сайта, поэтому внимательные пользователи могли обратить внимание на подозрительную ссылку. А невнимательные отправляли злоумышленникам не только банковскую информацию, но и «селфи» с удостоверением личности в руках.

Беспроигрышный с точки зрения преступников сценарий это фишинг от лица госструктур. В ходе одной из таких кампаний жертвы получали извещения о штрафах ГИБДД под видом уведомления с портала «Госуслуги». Достоверность письма подтверждалась логотипом электронного правительства, а в самом письме содержалась якобы фотография автомобиля нарушителя. Однако при попытке открыть фотографию жертва перенаправлялась на поддельный сайт, требующий ввести учетные данные от электронной почты.



Пример фишингового письма

Как защититься организации

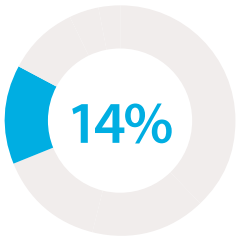
+ Обучать сотрудников и пользователей основам ИБ.
+ Использовать антивирусное ПО, в том числе специализированное, позволяющее пользователям отправлять подозрительные файлы на проверку перед открытием вложения из письма.
+ Использовать SIEM-решения для своевременного обнаружения атаки, если инфраструктура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

Как защититься обычному пользователю

+ Использовать эффективные средства антивирусной защиты на всех устройствах.
+ Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно в том случае, когда браузер предупреждает об опасности.
+ С осторожностью относиться к сайтам с некорректными сертификатами и учитывать, что введенные на них данные могут быть перехвачены злоумышленниками.
+ Проверять все вложения, полученные по электронной почте, с помощью антивирусного ПО.

17 www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cobalt-2017-rus.pdf
18 phishme.com/smile-new-paypal-phish-victims-sending-selfie/

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ ПО



Больше всего пострадавших в США и Австралии

Наиболее атакуемые объекты:

87% 6% 3%

Больше всего пострадали:

19% 16% 10%

Ущерб > 200 тыс. долл. США

Помимо известных уязвимостей в ПО, которые позволяют вредоносным программам выполнять опасные действия на зараженном устройстве, злоумышленники продолжают находить и использовать новые уязвимости нулевого дня.

Наибольшую популярность получили уязвимости в продуктах компании Microsoft, а именно Microsoft Office. Так, по данным FireEye[19], группировки APT28 и Turla использовали уязвимости нулевого дня в Microsoft Office, позволяющие удаленно выполнять произвольный код, в качестве первоначальных векторов проникновения в целевую систему. Например, злоумышленники распространяли эксплойты для уязвимости CVE-2017-0261[20] посредством электронных писем, содержащих документ Microsoft Word со встроенным вредоносным EPS-контентом (Encapsulated PostScript — формат для обработки графических файлов в Microsoft Office). Затем с помощью другой уязвимости CVE-2017-0263[21] получали привилегии администратора и, соответственно, полный контроль над системой. Примечательно, что указанная уязвимость нулевого дня в ОС Windows (CVE-2017-0263) была выявлена экспертом Positive Technologies[22].

APT-группировка OilRig в ходе атак на 120 израильских государственных и коммерческих компаний[23] использовала другую уязвимость нулевого дня в Microsoft Office — CVE-2017-0199. Эксплойт преимущественно внедрялся в файлы с расширением .doc и позволял после обращения к удаленному командному серверу загрузить и выполнить на компьютере жертвы файл HTA (HTML-приложение, запускаемое вне браузера), замаскированный под RTF. Таким образом злоумышленники могли внедрять в целевую систему различное вредоносное ПО.

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[24].
+ Использовать эффективные средства антивирусной защиты на всех устройствах.

19 www.fireeye.com/blog/threat-research/2017/05/eps-processing-zero-days.html
20 cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0261
21 cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0263
22 www.securityfocus.com/bid/98258
23 securityaffairs.co/wordpress/58464/hacking/oilrig-apt-target-israel.html
24 Отсутствие web application firewall является уязвимостью согласно обновленному списку топ-10 уязвимостей OWASP (2017).

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 в том случае, 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

Больше всего пострадавших в США и Великобритании

Наиболее атакуемые объекты:

100%

Больше всего пострадали:

22% **17%** **13%**

Ущерб > 3,4 млн долл. США

Пострадали > 80 млн человек

Недостаточная защищенность веб-ресурсов во II квартале стала причиной утечки чувствительной информации, принадлежащей более чем 80 миллионам человек по всему миру. Самой масштабной была атака на американскую образовательную социальную сеть Edmodo, в результате которой был похищен дамп базы данных, содержащий чувствительную информацию 77 миллионов пользователей, включая адреса электронной почты[25]. Предполагается, что злоумышленник удаленно выполнил произвольный код на языке Python. Примечательно, что на черном рынке эту информацию продавали всего за 1000 долл. США.

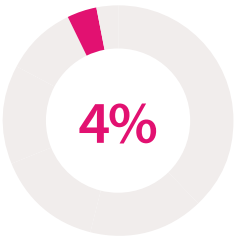
Как защититься организации

+ Проводить регулярный анализ защищенности веб-приложений, включая анализ исходного кода.
+ Использовать межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты[26].
+ 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.

25 benhamouglobalventures.com/2017/06/07/deep-dive-into-the-edmodo-data-breach/

26 Отсутствие web application firewall является уязвимостью согласно обновленному списку топ-10 уязвимостей от OWASP (2017).

DDOS



Больше всего пострадавших в Китае, США и Южной Корее

Наиболее атакуемые объекты:

87% 13%

Больше всего пострадали:

38% 25% 13%

16 часов — среднее время простоя инфраструктуры

Во II квартале доля DDoS-атак на фоне других инцидентов остается небольшой. Исследователи обнаруживают новые ботнеты из IoT-устройств, однако известий о новых инцидентах, связанных с высоконагруженными атаками, поступает немного. Возможно, злоумышленники копят ресурсы, чтобы в дальнейшем реализовать масштабные атаки. А возможно, причина кроется в том, что компании, деятельность которых была нарушена из-за DDoS-атак, стараются не афишировать это. Например, в течение двух дней был недоступен сервис Skype для пользователей из Европы и части США. И хотя представители Microsoft не назвали причину сбоя, предполагается, что сервис стал именно жертвой DDoS-атаки. Ответственность за случившееся взяла на себя группировка CyberTeam[27], специализирующаяся на таком виде атак.

Злоумышленники продолжают шантажировать компании угрозами DDoS-атак. Так, сразу несколько южнокорейских банков (KB Kookmin Bank, Shinhan Bank, Woori Bank, KEB Hana Bank и NH Bank) стали жертвами шантажистов, которые требовали порядка 315 000 долл.[28] Но поскольку нарушений в работе этих финансовых учреждений замечено не было, то либо угрозы оказались беспочвенны, и злоумышленники не обладали необходимыми для атаки ресурсами, либо банки достаточно защищены, либо заплатили требуемую сумму.

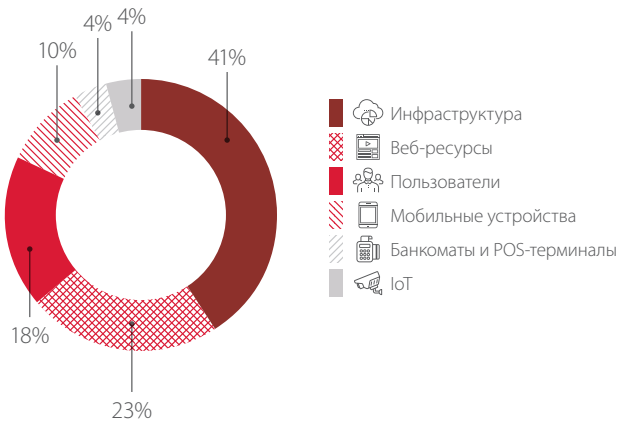
Как защититься организации

+ 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.

27 twitter.com/ CyberTeam /status/876926485428305920
28 www.scmagazineuk.com/hackers-threaten-south-korean-banks-with-ddos-attacks/article/671607/

ОБЪЕКТЫ АТАК

Инфраструктура компаний и веб-ресурсы являются наиболее атакуемыми объектами.

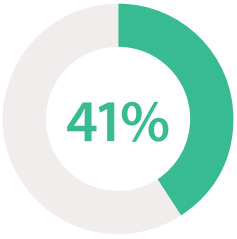


Распределение киберинцидентов по объектам

Во II квартале отмечается снижение количества атак на веб-ресурсы (23% — вместо 33% в I квартале) и увеличение доли атак на мобильные устройства (10% вместо 2%). Кроме того, во мы ввели категорию объектов «IoT», в которую вошли преимущественно маршрутизаторы, IP-камеры и видеорегистраторы.

Ниже 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, на Украине и в России

Наиболее популярные методы атак:

40% 31% 13%

Больше всего пострадали:

27% 15% 12%

Ущерб > 3 млн долл. США

Наибольшее количество инцидентов во II квартале 2017 года были связаны с заражением информационной инфраструктуры компаний вредоносным ПО. Однако это не единственный вектор атак на инфраструктуру. Так, группировка APT10 продемонстрировала нестандартный способ проникновения в корпоративную сеть жертв[29]. В ходе целевых атак злоумышленники сначала получали доступ в сети провайдеров облачных сервисов, а затем по доверенным каналам связи проникали в корпоративную сеть целевой организации. В ходе атак использовались вредоносное ПО PlugX и новый троян RedLeaves.

29 baesystemsai.blogspot.ru/2017/04/apt10-operation-cloud-hopper_3.html

Основной целью атак на инфраструктуру компаний по-прежнему остаются данные. Однако результаты независимого исследования, проведенного организацией Ponemon Institute при поддержке компании IBM, показывают, что ущерб от утечек данных по всему миру в 2017 году снизился на 10% и составил 3 620 000 долл. США[30].

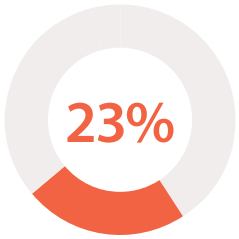
Как защититься организации

+ 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:

40% 28% 14%



Больше всего пострадали:

18% 18% 14%

Больше всего пострадавших в США, Великобритании и России

Ущерб > 10 млн долл. США

Уже стали стандартными такие последствия атак на веб-ресурсы, как получение конфиденциальной информации и проникновение во внутреннюю сеть жертвы. Однако во II квартале 2017 года мы отметили интересный сценарий, который использовала группировка Cobalt при реализации целевых атак преимущественно на финансовые организации[31]. Злоумышленники использовали произвольные уязвимые сайты в качестве хостингов для ВПО. Они размещали вредоносные файлы на уязвимых веб-ресурсах, чтобы затем загрузить их в инфраструктуру жертвы. Таким образом эти ресурсы становились промежуточным звеном в цепочке целевой атаки, а их владельцы — невольными соучастниками атак. Это могло нанести серьезный ущерб их репутации, а также привести к блокировке веб-ресурсов регулятором или изъятию серверного оборудования правоохранительными органами при расследовании совершенного преступления.

Как защититься организации

+ Использовать межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты[32].
+ Проводить регулярный анализ защищенности веб-приложений, включая анализ исходного кода.

30 www.ibm.com/security/data-breach/
31 www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cobalt-2017-rus.pdf
32 Отсутствие web application firewall является уязвимостью согласно обновленному списку топ-10 уязвимостей OWASP (2017).

- Использовать строгую парольную политику, особенно для привилегированных учетных записей.
- Своевременно обновлять используемое ПО.
- Внедрить процессы обеспечения безопасности на протяжении всего цикла жизни веб-приложения.

ПОЛЬЗОВАТЕЛИ

Больше всего пострадавших в США, Великобритании и России

Наиболее популярные методы атак:

33% 30% 25%

Больше всего пострадали:

70% 8% 8%

Пострадали > 1 млн человек

От действий киберпреступников страдают не только организации, но и обычные пользователи. Случается так, что похитив базу данных компании и потребовав за нее выкуп, злоумышленники получают отказ и переключаются на клиентов, чьи данные им удалось получить. Подобная история произошла с клиникой пластической хирургии в Литве[33]. Киберпреступная группировка Tsar Team получила около 25 тысяч личных фотографий более 1500 клиентов клиники и сначала потребовала выкуп в размере 300 биткойнов (около 590 000 долл. США) у самой организации, но получила отказ и тогда переключила внимание на пациентов, требуя с каждого от 61 до 2200 долл. США.

Нередко обычные пользователи становятся жертвами ВПО. Любопытна мотивация нарушителя, распространившего ВПО RensenWare[34]. Вместо пополнения кошелька разработчика для расшифровки файлов жертве необходимо было набрать 0,2 миллиарда очков в игре TH12 — Undefined Fantastic Object. При попытке закрыть программу ключ удалялся без возможности восстановления информации.

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.

33 www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments
34 xakep.ru/2017/04/10/rensenware/

- Не переходить по ссылкам на незнакомые подозрительные ресурсы, особенно в том случае, 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 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

Больше всего пострадавших в России, Австрии, Великобритании

Наиболее популярные методы атак:

76% 14% 5%

Больше всего пострадали:

95% 5%

Во II квартале мы отметили рост числа атак на мобильные устройства, который можно соотнести с увеличением масштабов вредоносных кампаний.

Нередко ВПО удается обойти проверки безопасности официальных магазинов приложений (App Store, Google Play) и попасть на мобильное устройство жертвы под видом легального приложения. Так, например, приложения Funny Videos 2017[35] и HappyTimes Videos[36], размещенные в апреле в Google Play, содержали свежую версию банковского трояна BankBot. ВПО отображало фальшивое окно авторизации поверх интерфейса оригинального банковского приложения и таким образом похищало учетные данные от мобильного банка.

Однако наиболее популярный путь троянов на телефоны жертв это файлы, размещенные в интернете. Зачастую злоумышленники обманом убеждают пользователей скачать программу под видом искомого торрента-файла, музыки, или даже уверяя, что смартфон или планшет заражен вирусами и нужно скачать антивирус. Ссылки на скачивание ВПО также могут приходить по SMS или в популярных мессенджерах (WhatsApp, Telegram, Viber) под видом безобидной рекламы.

Кроме того, злоумышленники активно реализуют фишинговые кампании, пользуясь тем, что мобильные браузеры не полностью отображают ссылки в адресной строке. Киберпреступники регистрируют поддомены, похожие на реальные доверенные ресурсы, а

35 www.clientsidedetection.com/banking_malware_in_google_play_targeting_many_new_apps.html
36 twitter.com/SfyLabs/status/854055785156009984

затем собирают учетные данные пользователей. Например[37], http://m.facebook.com----------validate----step1.rickytaylk[dot]com/sign_in.html, где реальным доменом является rickytaylk.com, а не m.facebook.com, как покажется пользователю.

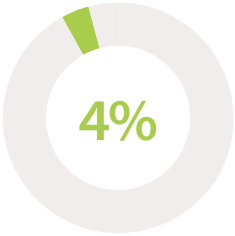
Как защититься обычному пользователю

- 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.
- 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

Наиболее популярные методы атак:

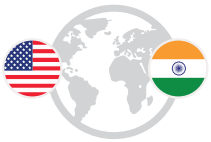
100%



Больше всего пострадали:

38% **38%** **24%**

Больше всего пострадавших в США и Индии



Ущерб > 20 млн долл. США

Во II квартале продолжился рост количества атак на POS-терминалы и банкоматы с использованием ВПО. Так, во второй раз за три года американская сеть магазинов Kmart[38] стала жертвой киберпреступников, заразивших POS-терминалы компании вредоносным ПО. Другая американская торговая сеть Target становилась жертвой аналогичной атаки еще в 2013 году, в результате чего были похищены данные порядка 40 миллионов платежных карт[39]. В мае 2017 года компания закончила выплачивать компенсацию пострадавшим в совокупном размере порядка 18 млн долл.

37 info.phishlabs.com/blog/the-mobile-phishing-threat-youll-see-very-soon-url-padding
38 krebsonsecurity.com/2017/05/credit-card-breach-at-kmart-stores-again/
39 www.pcworld.com/article/2087240/target-pointofsale-terminals-were-infected-with-malware.html

Несмотря на то, что злоумышленники в последнее время стали предпочитать глобальные целевые атаки на финансовые организации, они продолжают изобретать новые способы и новое ВПО для кражи денег из банкоматов. Так, в Индии злоумышленники за несколько минут опустошали банкоматы, инфицировав устройства через USB-накопитель[40]. По сообщению ФинЦЕРТ ЦБ РФ (ATM-ML-FilelessMalware-20170315-01), весной 2017 года была выявлена новая угроза атак на финансовые организации с помощью бестелесного ВПО, ориентированного на банкоматы, а «Лаборатория Касперского» публиковала отчет[41] об атаках с помощью подобного ПО[42].

Что предпринять вендору

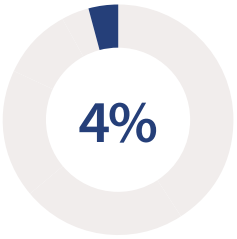
В данной ситуации организации, занимающиеся разработкой и обслуживанием POS-терминалов и ПО для этих устройств, должны принимать меры защиты, включая:

+ 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.

IOT

Наиболее популярные методы атак:

57% 29% 14%



Больше всего пострадали:

57% 29% 14%

Пострадавшие по всему миру

Более 22 млн уязвимых устройств могут оказаться в составе ботнетов

В настоящее время по всему миру существует более 6 миллиардов IoT-устройств[43], среди которых преобладают IP-камеры, маршрутизаторы и другие сетевые устройства, системы контроля и управления доступом, а также составляющие «умного дома». Все они имеют множество недостатков безопасности, которые и позволяют злоумышленникам получать к ним доступ из интернета. Примечательно, что разработчики ПО для этих устройств не торопятся закрывать выявленные уязвимости. Так, эксперты по безопасности выявили ряд уязвимостей в прошивке IP-камер[44], позволяющих нарушителю получить контроль над устройствами и проникнуть во внутреннюю сеть. Однако вендор оставил сообщения о данной проблеме без ответа, а саму проблему, соответственно, без решения. Тем временем появился новый ботнет Persirai, в состав которого вошли 120 тысяч IP-камер, зараженных ВПО[45].

Стоит также отметить, что уязвимости IoT могут использоваться не только для создания ботнетов и последующих DDoS-атак, но и, например, для слежения за частной жизнью людей (в случае взлома IP-камер) или для того, чтобы просто досадить кому-то. Так, в апреле 2017 года

40 economictimes.indiatimes.com/industry/banking/finance/banking/indian-banks-and-atms-had-a-narrow-escape-from-wannacry/articleshow/58689401.cms

41 threatpost.com/fileless-banking-malware-attackers-break-in-cash-out-disappear/124711/

42 Информация об атаках на банкоматы российских банков позднее не подтвердилась. Однако ФинЦЕРТ ЦБ РФ предупреждает о возможной реализации данной угрозы в отношении финансовых организаций в 2017 году.

43 securelist.com/honeypots-and-the-internet-of-things/78751/

44 images.news.f-secure.com/Web/FSecure/%7B43df9e0d-20a8-404a-86d0-70dcca00b6e5%7D_vulnerabilities-in-foscam-IP-cameras_report.pdf

45 blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

в США злоумышленники запустили систему городского оповещения о чрезвычайных ситуациях, в результате чего сирены работали на протяжении полутора часов посреди ночи[46].

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 сети Интернет, 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.

46 www.nytimes.com/2017/04/08/us/dallas-emergency-sirens-hacking.html

ВЫВОДЫ

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

+ Массовая вредоносная кампания может нанести ущерб, суммарно сопоставимый с целенаправленной атакой. А сервис «вымогатели как услуга» набирает серьезные обороты, что позволяет прогнозировать появление целого рынка ransomware в ближайшем будущем.
+ Вместе с ростом рынка криптовалюты растет количество атак на биткойн-кошельки и биржи.
+ Исследователи обнаруживают новые ботнеты из IoT-устройств, однако известий о новых инцидентах, связанных с высоконагруженными атаками, поступает немного. Нельзя исключать возможность, что злоумышленники копят ресурсы, чтобы в дальнейшем реализовать масштабные атаки.
+ Необходимость защиты от киберпреступников на государственном уровне начали осознавать те страны, которые до недавнего времени не имели своих кибервойск. Так, Австралия официально заявила о создании подразделения, специализирующегося на информационных войнах[47], и даже опубликовала соответствующую вакансию на сайте министерства обороны[48]. Вероятно, что в ближайшее время кибервойска продолжат появляться и у других стран.

47 www.abc.net.au/news/2017-06-30/cyber-warfare-unit-to-be-launched-by-australian-defence-forces/8665230
48 www.defencejobs.gov.au/navy/jobs/ElectronicWarfare/