



POSITIVE TECHNOLOGIES

Актуальные киберугрозы

II квартал 2018 года



Содержание

Обозначения	2
Тренды и прогнозы	3
Сводная статистика	4
Динамика атак	7
Методы атак	8
Использование вредоносного ПО	8
Социальная инженерия	10
Хакинг	11
Подбор учетных данных	12
Эксплуатация веб-уязвимостей	13
DDoS	14
Категории жертв	15
Государственные организации	15
Медицинские учреждения	16
Криптовалютные биржи	17
Торговля	18
Частные лица	19
Как защититься организации	21
Как вендору защитить свои продукты	22
Как защититься обычному пользователю	22



Обозначения

Объекты атак



Инфраструктура



Веб-ресурсы



Пользователи



Банкоматы и POS-терминалы



Мобильные устройства



IoT

Методы атак



Использование вредоносного ПО



Подбор учетных данных



Социальная инженерия



Хакинг



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



Торговля



Частные лица



Телекоммуникационные компании



Криптовалютные биржи



Другие сферы



Тренды и прогнозы

Компания Positive Technologies продолжает рассказывать об актуальных угрозах информационной безопасности, основываясь на собственной экспертизе, результатах многочисленных расследований, а также данных авторитетных источников.

Подводя итоги II квартала 2018 года, мы отмечаем следующие тенденции:

- Количество уникальных киберинцидентов продолжило расти и на 47% превысило показатели аналогичного периода в 2017 году.
- Преобладали целенаправленные атаки — на конкретные организации и их клиентов, на криптовалютные биржи. В ходе этих атак злоумышленники были довольно изобретательны. Они не только использовали вредоносное ПО, но и искали уязвимости нулевого дня, узнавали пароли администраторов с помощью социальной инженерии, получали доступ к ресурсам контрагентов.
- Во второй половине квартала произошло большое количество (в два раза больше, чем за I квартал) атак на криптовалютные площадки, в результате которых злоумышленники похитили более 100 млн долл. США.
- Продолжила расти доля кибератак, выполненных с целью получения информации. Причем злоумышленники больше всего были заинтересованы в персональных и учетных данных, а также в данных банковских карт. Их похищали в основном посредством компрометации различных онлайн-площадок — интернет-магазинов, сервисов для продажи билетов, бронирования отелей и т. п.
- Частные лица страдали от различного вредоносного ПО: большую его часть они устанавливали сами по невнимательности или незнанию, однако встречались и такие методы атак, когда, например, новые смартфоны продавались в магазине с уже установленным в прошивку ВПО.

Если говорить о прогнозах, то, вероятно, сохранится тенденция к увеличению доли атак, направленных на хищение данных. Многие компании уделяют недостаточно внимания защите обрабатываемой информации (особенно персональных и медицинских данных), что делает ее легкой добычей даже для низкоквалифицированных хакеров (которых с каждым днем становится все больше). Полученная информация затем продается на теневом рынке и используется для других кибератак.



Сводная статистика

Во II квартале 2018 года продолжила расти доля атак, направленных на получение данных. В 40% киберинцидентов злоумышленники были нацелены на получение информации, а в 39% — на финансовую выгоду. В нашем аналитическом исследовании «Рынок преступных киберуслуг»¹ мы подробно рассмотрели спрос и предложение теневого рынка на различные данные (персональные, учетные, платежные и т. д.). Так, например, 59% всех предложений о продаже данных в дарквебе — учетные записи пользователей для доступа к различным ресурсам, в том числе к банковским приложениям. Учетные данные могут продаваться поштучно по цене до 10 \$ или целыми партиями до нескольких миллионов записей, стоимость которых достигает сотен долларов. Поэтому вслед за атакой, в которой была получена информация, довольно скоро может последовать новая — на владельцев этих данных или на компанию, учетные данные сотрудников которой были скомпрометированы.

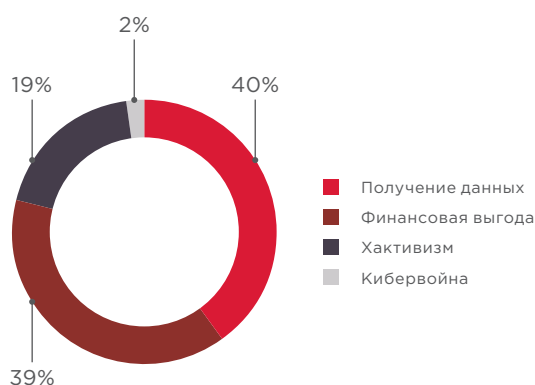


Рисунок 1. Мотивы злоумышленников

Мы рассмотрели, какая информация больше всего привлекала преступников во II квартале 2018 года. В половине случаев это были персональные данные (30%) либо учетные записи и парольная информация для доступа к различным сервисам и системам (22%), в том числе и к онлайн-банкам частных лиц. В 15% случаев были украдены данные платежных карт, их злоумышленники чаще всего получали с помощью шпионского ВПО или со скомпрометированных сайтов.

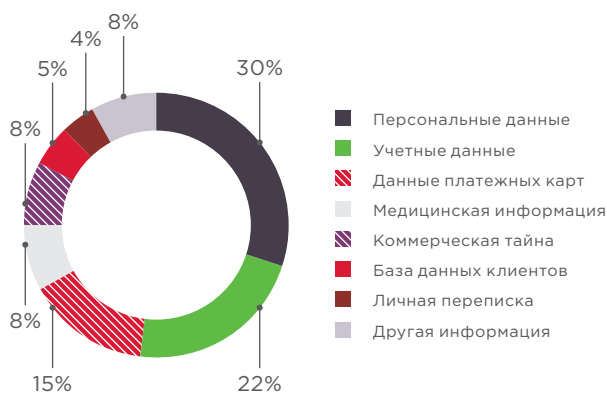


Рисунок 2. Типы украденных данных

¹ ptsecurity.com/ru-ru/research/analytics/darkweb-2018/



Во II квартале 2018 года мы отметили большое количество целенаправленных атак на различные организации, причем доля целевых атак превысила долю массовых и составила 54%. Далее мы рассмотрим подробнее атаки, направленные на государственные и медицинские учреждения, поскольку именно в них чаще всего заинтересованы киберпреступники, а также атаки на криптовалютные биржи, предприятия торговли и на частных лиц.

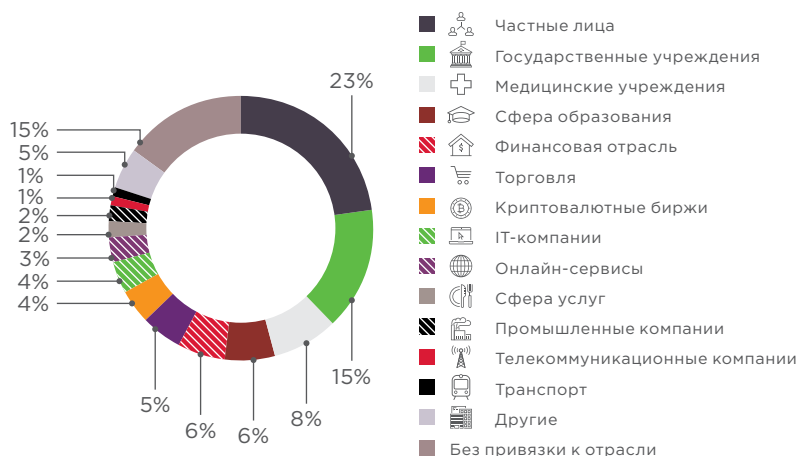


Рисунок 3. Категории жертв

Масштабные кибератаки, преимущественно вредоносные эпидемии, которые не ограничиваются воздействием на какую-то одну отрасль, мы отнесли к категории «без привязки к отрасли».

Доля атак, нацеленных на инфраструктуру, во II квартале 2018 года составила 44%, доля атак на веб-ресурсы выросла по сравнению с аналогичным периодом прошлого года и составила 32% против 23%. Кроме того, по сравнению с I кварталом выросла доля атак на IoT-устройства: это связано главным образом с появлением новых ботнетов, таких как PyRoMinelot, Muhstik, Wicked Mirai.

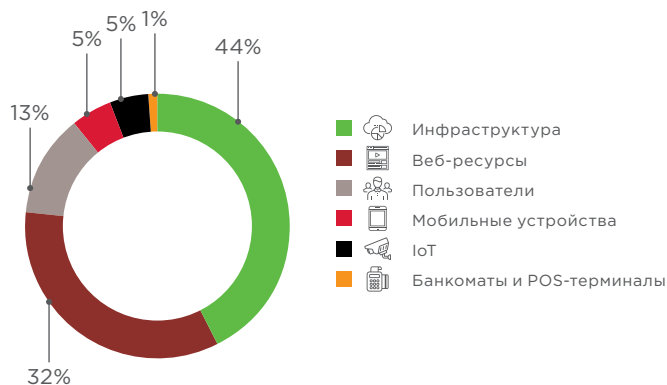


Рисунок 4. Объекты атак

Во II квартале 2018 года снизилась доля атак, в которых злоумышленники использовали вредоносное ПО (49% вместо 63% в I квартале). На 12% по сравнению с I кварталом текущего года выросла доля атак, в которых были подобраны учетные данные. Далее мы подробнее остановимся на каждом методе и укажем, какие объекты и отрасли больше всего от них пострадали.

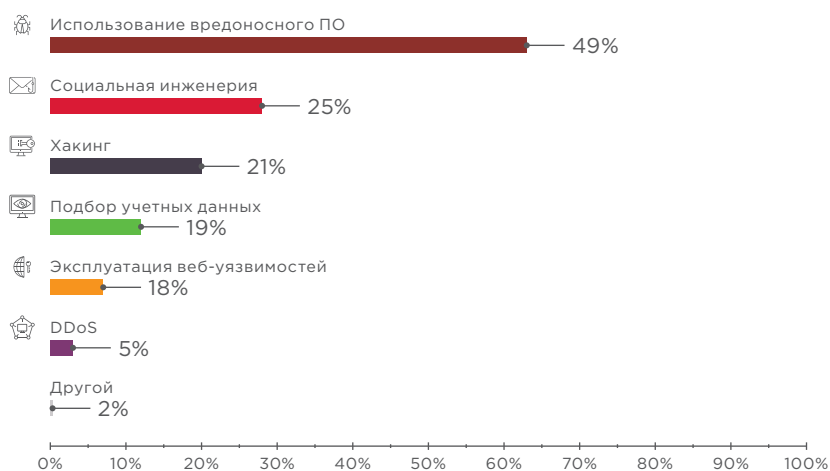


Рисунок 5. Методы атак

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

		Отрасль														
		Государственные учреждения	Финансовая отрасль	Промышленные компании	Медицинские учреждения	Онлайн-сервисы	Сфера услуг	IT-компании	Сфера образования	Торговля	Телекоммуникационные компании	Частные лица	Транспорт	Криптовалютные биржи	Другие	Без привязки к отрасли
Всего атак		46	18	7	26	9	8	12	19	15	4	72	2	14	15	49
Объект	Инфраструктура	19	13	5	15	1	3	7	12	3	2	21	1	1	4	33
	Веб-ресурсы	22		1	6	7	3	4	4	9	1	16	1	12	8	6
	Пользователи	1	4		5	1	1	1	3	2		21		1		1
	Мобильные устройства	1										13				1
	Банкоматы и POS-терминалы		1				1			1						
	IoT	3		1							1	1			3	8
Метод	Атаки с использованием ВПО	21	7	3	10	3	4	4	7	5	1	47			1	43
	Социальная инженерия	10	9		6	2	2	2	4	1	1	27		1		15
	Подбор учетных данных	8	4		10			2	8	2	1	12	1	5	3	4
	Хакинг	8	6	3	2	2	2	6	2	2	3	6	1	8	3	13
	Эксплуатация веб-уязвимостей	13		1	4	4	2	2	3	8	1	6		3	7	4
	DDoS	6	1	2		2		2				1			2	
	Другой	1	1								1	3			1	
Мотив	Финансовая выгода	12	12	1	2	3	3	1	7	3		39	1	13	1	26
	Получение данных	17	4	2	23	3	4	7	7	11	3	25	1	1	5	14
	Хактивизм	14	2	3	1	3	1	4	5	1	1	8			9	9
	Кибервойна	3		1												
Интенсивность цвета показывает долю атак в рамках одной отрасли		<div><div></div><div></div><div></div><div></div><div></div></div> <div>0%10%20%30%40%100%</div>														



Динамика атак

Количество уникальных киберинцидентов во II квартале 2018 года на 47% превысило показатели аналогичного периода в 2017 году.

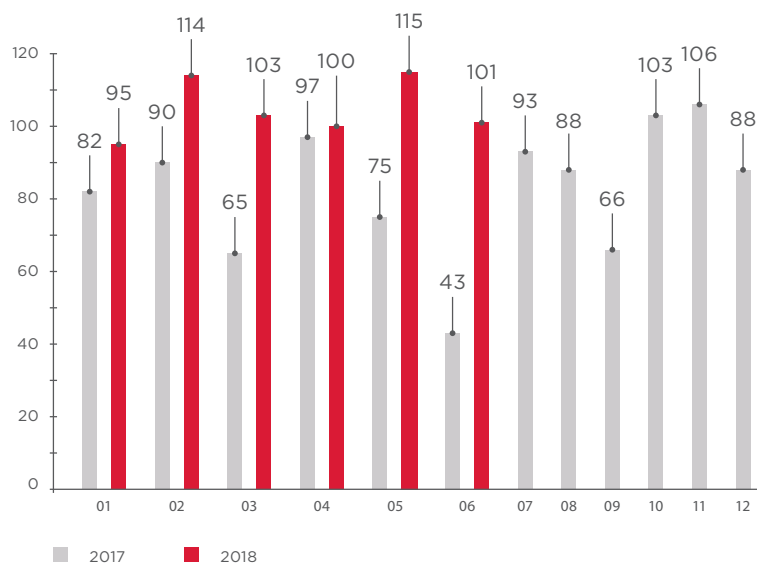


Рисунок 6. Количество инцидентов в 2017 и 2018 годах (по месяцам)

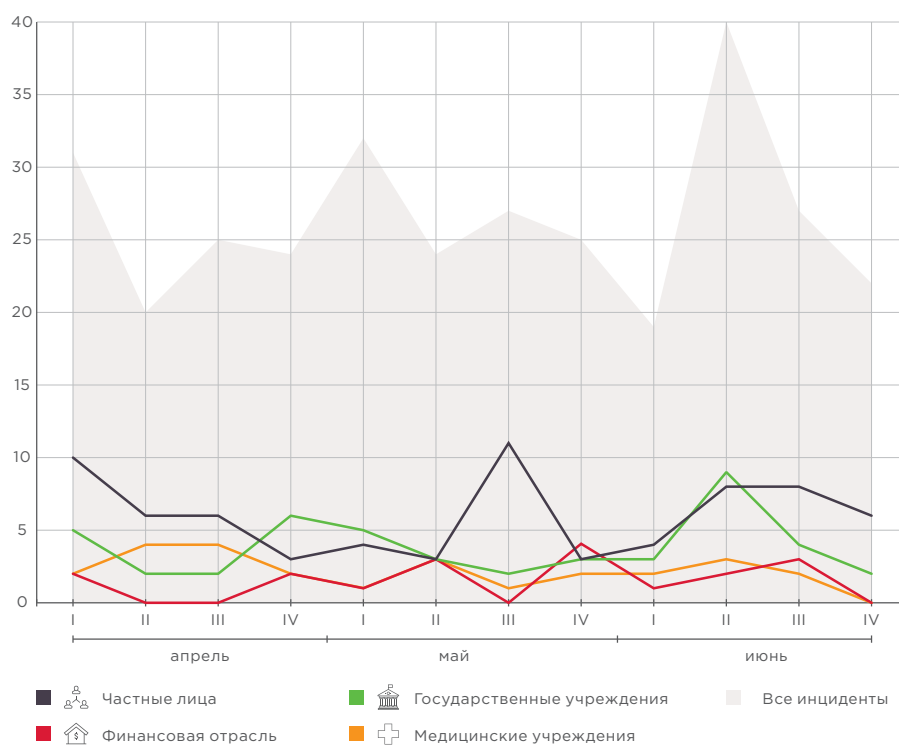


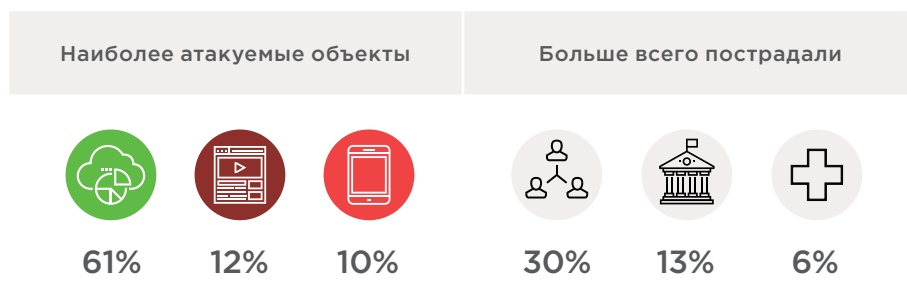
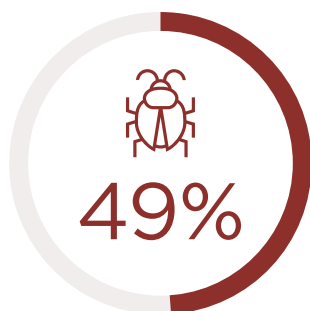
Рисунок 7. Количество инцидентов в I квартале 2018 года (по неделям)



Методы атак

Далее мы подробнее остановимся на каждом методе атак и укажем, какие объекты и отрасли больше других страдали от них.

Использование вредоносного ПО



Итак, киберпреступники активно собирают данные с компьютеров жертв. Для этих целей они используют шпионское ПО (26% заражений) или ВПО для удаленного управления (22%). Во II квартале встретилось меньше киберинцидентов с использованием шифровальщиков и майнеров, чем в первые месяцы года. Злоумышленники продолжают активно использовать уязвимости из базы АНБ для создания вредоносного ПО. Так, майнер *PyRoMine*, применяя эксплойт *EternalRomance (MS17-010)*, не только использовал вычислительные мощности жертвы, но и создавал скрытый аккаунт с правами администратора и возможностью удаленного подключения, что могло быть лишь подготовкой к последующей атаке.

Тремя основными путями заражения во II квартале 2018 года стали:

- компрометация серверов и рабочих станций; злоумышленники предварительно получали доступ к целевой системе, используя уязвимости, социальную инженерию или подбирая пароль (29% случаев);
- сайты, при посещении которых вредоносное ПО устанавливалось на устройство жертвы (29%);
- электронная почта: вредоносное вложение или ссылка на зараженный ресурс отправлялись жертве в письме (23%).



Рисунок 8. Типы вредоносного ПО

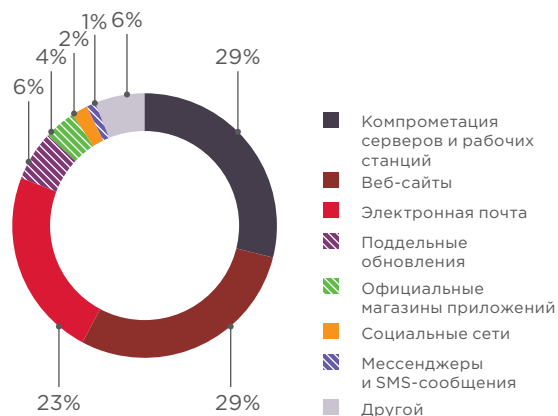


Рисунок 9. Способы распространения ВПО



Именно вредоносные рассылки используются в большинстве АРТ для проникновения в целевую систему. Во II квартале 2018 года эксперты РТ ESC отметили ряд целенаправленных атак, в ходе которых жертвам были направлены документы MS Word, которые на деле оказывались загрузчиками вредоносного ПО.

Приложение №1
к Контракту № _____
от «__» _____ 2018 г.

Календарный план выполнения работ				
№ Этапа	Наименование и вид работ	Срок выполнения	Стоимость в т.ч. НДС, рублей	Подтверждающий документ
1.	Поставка Технологического оборудования (ЛСР № 02-02-03);	X1 + 9 мес. ¹	88 409 395,47	1. Товарная накладная (ТОРГ-12). 2. Акт технической приемки Технологического оборудования.
2.	Монтаж Технологического оборудования (ЛСР № 02-02-02);	X2 + 1 мес. ²	100 221,34	1. Акт о приемке выполненных работ (форма КС-2). 2. Справка о стоимости выполненных работ и затрат (форма КС-3).
3.	– Пуско-наладочные работы на Технологическом оборудовании (ЛСР № 09-01-02); – подготовка обслуживающего персонала; – участие в ПСИ (по отдельному плану Заказчика).	X2 + 3,5 мес.	17 530 908,43	1. Акт о приемке выполненных работ (форма КС-2). 2. Справка о стоимости выполненных работ и затрат (форма КС-3). 3. Акт ПСИ.
ИТОГО:			106 040 525,24	

¹ X1 – дата получения аванса.
² X2 – дата получения уведомления о строительной готовности (включая готовность системы электроснабжения и линий связи) к монтажу Технологического оборудования.

ЗаказчикГенеральный подрядчик

Рисунок 10. Пример вредоносного вложения в целенаправленной атаке

Для того чтобы письмо выглядело наиболее правдоподобно, злоумышленники могут подменить адрес отправителя. Так, например, в ходе одной из атак, зафиксированных экспертами РТ ESC, бэкдор отправлялся якобы от лица российской государственной корпорации «Ростех».

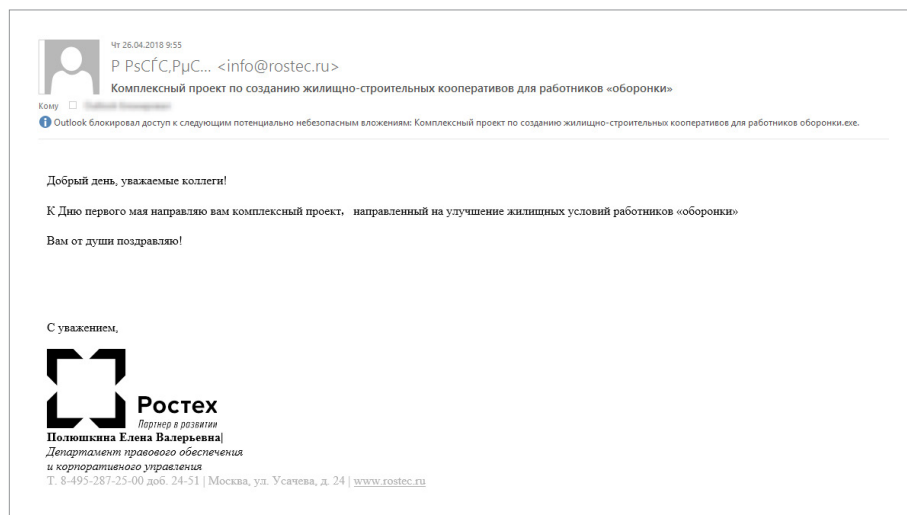


Рисунок 11. Пример фишингового письма

Кроме того, специалисты РТ ESC обнаружили фишинговую атаку, нацеленную на крупную российскую IT-компанию, в ходе которой распространялся троян PlugX. Это вредоносное ПО представляет собой RAT (remote access trojan) и уже несколько лет используется злоумышленниками в атаках на различные компании с целью шпионажа.



Социальная инженерия



Наиболее атакуемые объекты



49%



34%



9%



34%



13%



11%

Киберпреступники продолжают изобретать новые методы воздействия на пользователей, которые позволили бы им заразить целевую систему вредоносным ПО, украсть деньги или получить доступ к конфиденциальной информации. В мае исследователи из Lookout рассказали² об атаках на чиновников, дипломатов, военнослужащих и других высокопоставленных лиц из Пакистана, Афганистана, Индии, ОАЭ, в ходе которых была похищена важная информация с их смартфонов, включая изображения, аудиозаписи и текстовые сообщения. Для того чтобы заразить мобильные телефоны шпионским ПО, злоумышленники заводили с жертвами беседу в социальной сети Facebook, в ходе которой делились фишинговой ссылкой, например на видеозапись, при переходе по которой на смартфон устанавливалось вредоносное ПО из стороннего магазина приложений.

Тогда же в мае еще одна вредоносная кампания, распространяющаяся через Facebook, была обнаружена экспертами Radware³. Фишинговые ссылки отправлялись от зараженных ранее лиц и вели на фальшивую страницу YouTube, где жертве предлагалось установить расширение для браузера Google Chrome. Вредоносные расширения маскировались под легитимные в официальном каталоге Chrome Web Store, а на деле превращали зараженный компьютер в новое звено ботнета: похищали учетные данные пользователей в Facebook и Instagram, а затем продолжали распространение вредоносного ПО среди друзей жертвы. При этом мощности зараженных устройств использовались для майнинга криптовалюты.

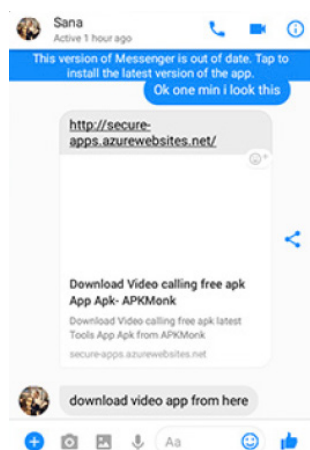


Рисунок 12. Фишинг через социальную сеть Facebook

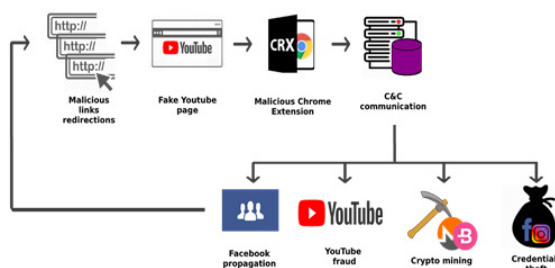


Рисунок 13. Схема фишинга через Facebook



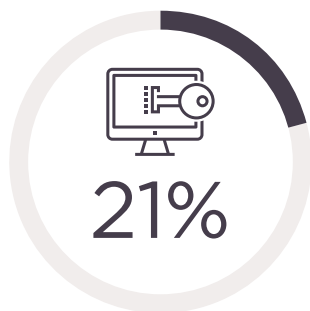
Продолжает вести активность, направленную на организации в Белоруссии и Казахстане, группировка SongXY. В рамках данной кампании злоумышленники с помощью целевых фишинговых рассылок распространяют вредоносное ПО CMstar и Lurid для компрометации целевой системы.

² info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf

³ blog.radware.com/security/2018/05/nigelthorn-malware-abuses-chrome-extensions/



Хакинг



Наиболее атакуемые объекты



63%



21%



15%



12%



12%



11%

Больше всего пострадали

Как мы уже говорили, большинство кибератак состоят из цепочек спланированных действий злоумышленников. Хакинг — эксплуатация уязвимостей ПО и оборудования, использование ошибок в механизмах защиты или других недостатков атакуемых систем — часто является первым шагом киберпреступников.

Для того чтобы заразить целевую систему вредоносным ПО, не всегда возможно отправить троян по электронной почте. Например, когда речь идет о создании ботнета из IoT-устройств. Уязвимость в тайваньских роутерах фирмы DrayTek⁴ позволила злоумышленникам получать права администратора и менять параметры DNS, перенаправляя весь трафик пользователей на неизвестный сервер. К счастью, производитель признал наличие уязвимости и оперативно выпустил обновление безопасности для этих устройств.

Продолжая тему интернет-трафика и DNS, отметим, что уязвимости в публичных DNS-серверах делают возможным фишинг в адрес посетителей сайтов. Так, например, в апреле злоумышленники скомпрометировали несколько DNS-серверов с целью перенаправления пользователей криптокошелька MyEtherWallet на фишинговый сайт⁵. Как правило, в случае подобной атаки браузер жертвы предупреждает о некорректности используемого SSL-сертификата, однако многие это уведомление игнорируют. В результате этой атаки злоумышленникам, предположительно, удалось украсть порядка 160 тыс. долл. США.

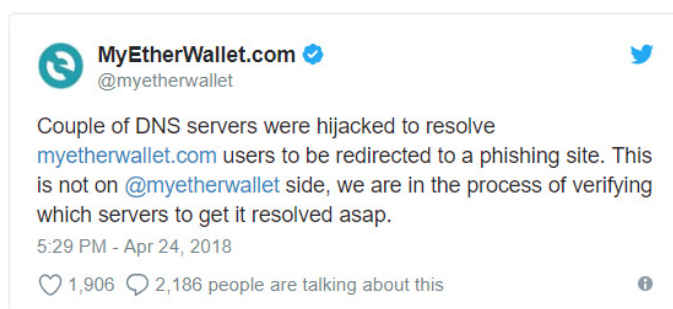


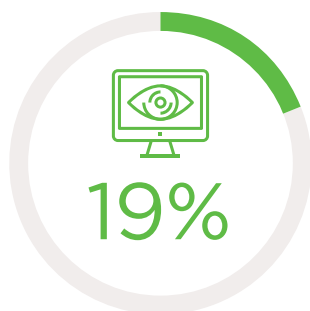
Рисунок 14. Уведомление об атаке на пользователей MyEtherWallet.com

⁴ draytek.com/en/about/news/2018/notification-of-urgent-security-updates-to-draytek-routers

⁵ habr.com/post/354384/



Подбор учетных данных



Наиболее атакуемые объекты



42%



33%



17%

Больше всего пострадали



20%



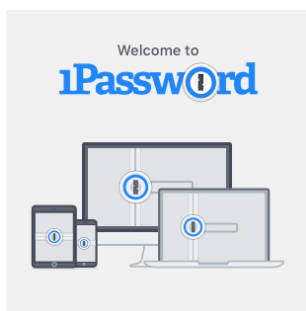
17%



13%

Существует множество инструментов, которые помогают пользователям сохранять сложные пароли, однако получив доступ к менеджеру паролей, злоумышленник получает неограниченный доступ ко всем ресурсам жертвы. Так, ICO-стартап Taylor потерял более 1,47 млн долл. США в мае 2018 года⁶. По словам организаторов, киберпреступники получили доступ к одному из устройств сотрудника и к файлам 1Password, хранящимся на нем, включая пароли от платформы. Следующим шагом стал перевод всей криптовалюты на счет преступников.

Пользователи CMS-платформы WordPress, не уделяющие достаточно внимания защите своих учетных данных (в частности, не использующие двухфакторную аутентификацию), стали во II квартале жертвами массовых кибератак⁷. Злоумышленники получали административный доступ к сайтам, устанавливали плагин Jetpack, с помощью которого перенаправляли посетителей на фишинговые ресурсы. Таким образом компании, использующие WordPress для поддержки сайта, становились невольными участниками кибератак на своих клиентов.



⁶ medium.com/smarttaylor/this-is-a-dark-day-for-taylor-ded587463da7

⁷ threatpost.ru/wordpress-sites-attacked-through-jetpack-plugin-vulnerability/26249/



Эксплуатация веб-уязвимостей



Наиболее атакуемые объекты



86%



14%



22%



14%



10%

Больше всего пострадали

Для шантажа жертв и получения финансовой выгоды киберпреступники используют все доступные им методы, в том числе ищут на просторах интернета уязвимые сайты и угрожают их владельцам хищением баз данных клиентов или остановкой работы. Похожая ситуация произошла в мае с сервисом по продаже билетов Ticketfly⁸, когда злоумышленник предлагал за вознаграждение рассказать администрации ресурса об уязвимостях, а получив отказ, осуществил дефейс главной страницы сайта и оставил сообщение, содержащее ссылки на клиентскую базу данных.

Дефейс продолжают использовать и хактивисты в атаках на государственные сайты. Так, жертвами киберпреступников в Индии стали министерство обороны и верховный суд⁹, а в Италии — администрация города Болонья¹⁰.

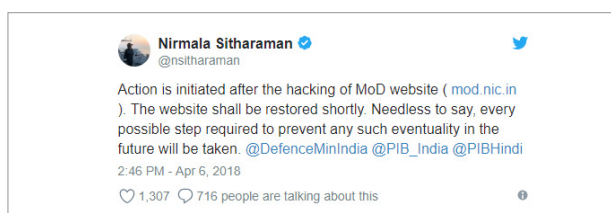


Рисунок 15. Сообщение о взломе сайта министерства обороны Индии



Рисунок 16. Дефейс сайта администрации города Болонья

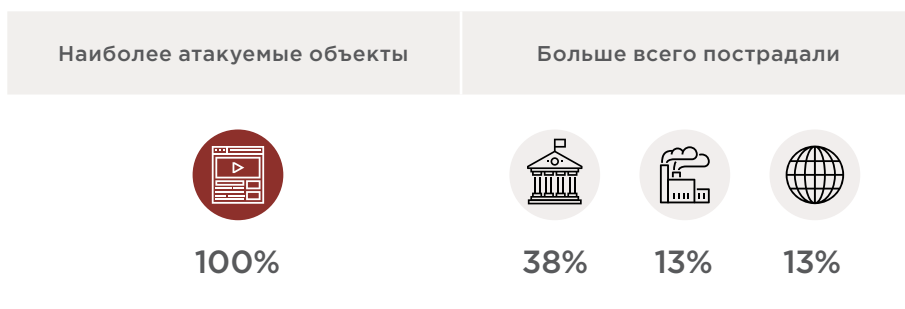
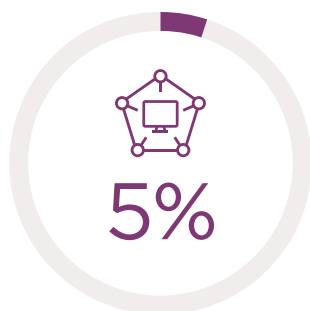
В апреле злоумышленник из Пакистана атаковал веб-ресурсы «Тайских авиалиний», включая официальный сайт, почтовый сервер, платежную систему, систему бронирования. В результате этой атаки он не только подменил главные страницы сайтов, но и получил доступ к персональным данным клиентов.

8 twitter.com/ticketfly/status/1002144038319882240

9 bankinfosecurity.asia/supreme-court-website-defaced-a-10867

10 bologna.repubblica.it/cronaca/2018/04/26/news/bologna_il_sito_del_comune_sotto_attacco_informatico-194878573/

DDoS



DDoS — это оружие конкурентов, недовольных клиентов и хактивистов. Больше всего подобных атак традиционно приходится на государственные учреждения. Кроме того, политические события, широко освещаемые в интернете, часто привлекают злоумышленников. Так, например, сайт мексиканской политической оппозиционной партии подвергся атаке во время финала телевизионных дебатов¹¹.

Киберпреступники используют DDoS-атаки и для получения финансовой выгоды. В этом случае они шантажируют жертву, выводя из строя важные для компании веб-ресурсы и требуя выкуп за прекращение атаки. Подобный инцидент эксперты PT ESC расследовали в июне, когда злоумышленники выполнили серию кратковременных (длительностью менее 2 минут) DDoS-атак на сайт компании для демонстрации своих возможностей и угрожали продолжить атаку в случае отказа в переводе денежных средств. Для атаки киберпреступники использовали вредоносное ПО Wreckuests — свободно распространяемую утилиту для проведения DDoS-атак типа HTTP flood. Wreckuests генерировала большое количество GET-запросов со случайными параметрами через сеть прокси-серверов, что и приводило к отказу в обслуживании сайта из-за чрезмерной нагрузки.

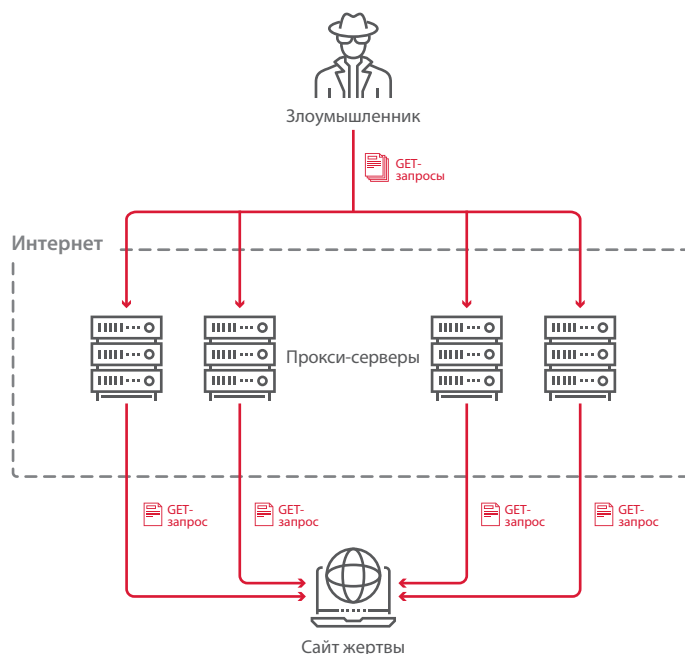


Рисунок 17. Схема DDoS-атаки с использованием ВПО Wreckuests

¹¹ reuters.com/article/uk-mexico-election-cyber/cyber-attack-on-mexico-campaign-site-triggers-election-nerve-idUKKBN1J93CQ



Категории жертв

Далее мы подробнее остановимся на анализе атак на отдельные отрасли, которые нам показались наиболее интересными во II квартале 2018 года.

Государственные организации



Ущерб более
150 тыс. долл. США

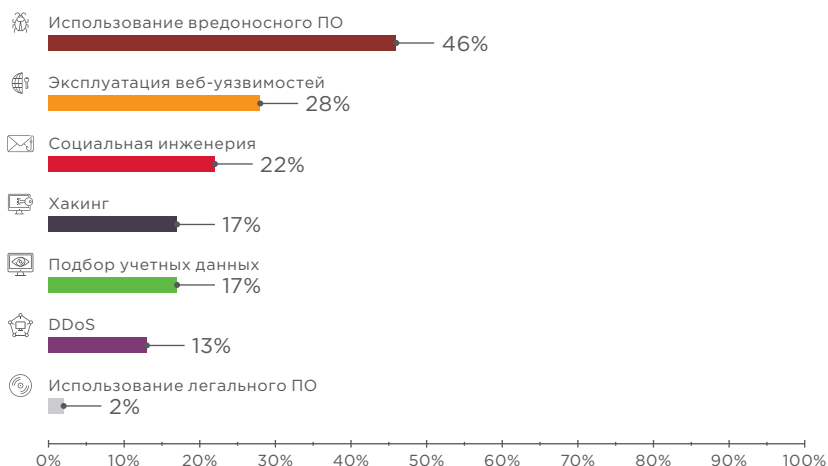


Рисунок 18. Методы атак на государственные организации в Q2 2018

- Веб-ресурсы
- Инфраструктура
- IoT
- Пользователи (сотрудники)
- Мобильные устройства

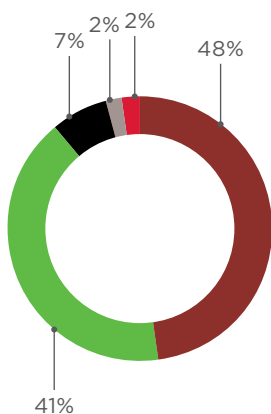


Рисунок 19. Объекты атак

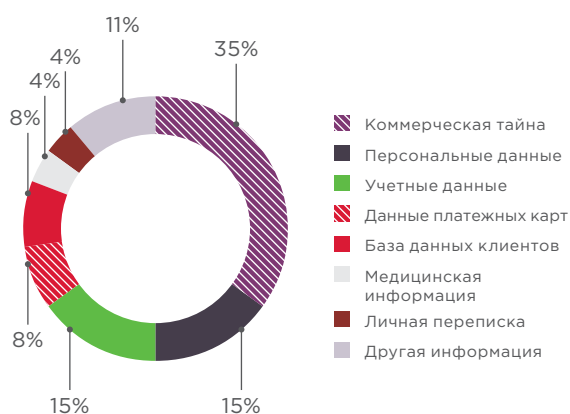


Рисунок 20. Украденные данные

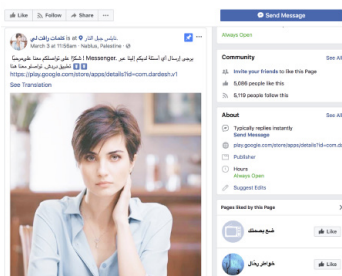


Рисунок 21. Фишинговый
профиль в Facebook со ссылкой
на вредоносный мессенджер
Dardesh

Государственные организации продолжают оставаться излюбленной мишенью для киберпреступников. Конечно, злоумышленников в первую очередь интересует коммерческая тайна целевых организаций, однако мы отмечаем учащение случаев атак на сотрудников и слежки за ними. Так, например, группировки APT-C-23¹² и mobile APT¹³ распространяли вредоносное ПО, используя методы социальной инженерии и официальный магазин приложений Google Play.

Злоумышленники из APT-C-23 от лица молодых девушек в социальных сетях убеждали жертв установить зараженный мессенджер Dardesh из Google Play, который загружал второй компонент вредоносного ПО, замаскированный под программу для настройки. После этого киберпреступники могли тайно следить за жертвами, в том числе записывать аудио и копировать данные.

¹² blog.lookout.com/desert-scorpion-google-play

¹³ blog.lookout.com/viperrat-google-play



Пострадали более
1 млн человек

Медицинские учреждения

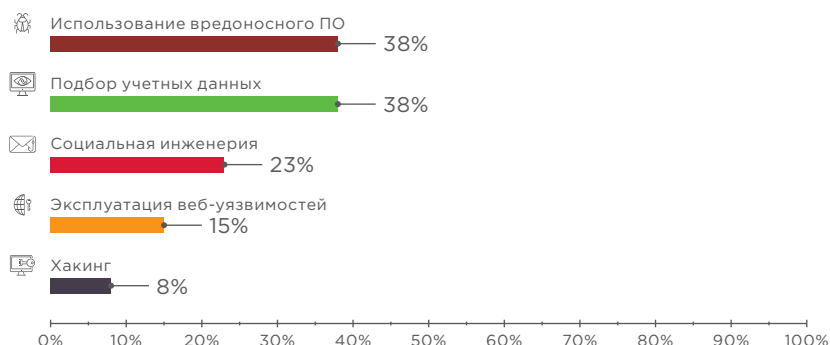


Рисунок 22. Методы атак на медицинские учреждения в Q2 2018

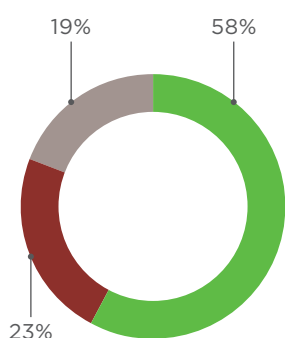
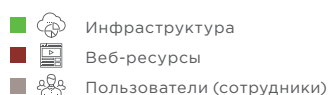


Рисунок 23. Объекты атак

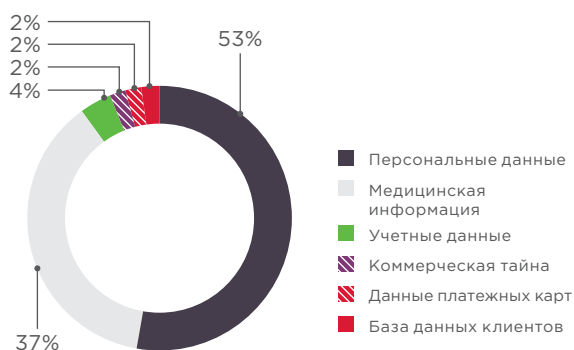


Рисунок 24. Украденные данные

Медицинские учреждения обрабатывают большое количество данных. А поскольку основная цель их работы это помощь людям, защите этих данных обычно уделяется недостаточно внимания. Как следствие, в 88% кибератак на медицинские учреждения во II квартале 2018 года были похищены данные. Причем помимо персональных сведений и привычных видов медицинских данных злоумышленники начинают интересоваться и другой информацией, например результатами генетических исследований. Так, в апреле стало известно об атаке на компанию Sangamo Therapeutics¹⁴, занимающуюся расшифровкой генома человека и терапией генетических заболеваний. Злоумышленники скомпрометировали электронную почту одного из топ-менеджеров и потенциально могли развить атаку на внутренние ресурсы компании.

Другая серьезная проблема — обеспечение непрерывной работы всей медицинской инфраструктуры. Злоумышленники не стесняются требовать выкуп за разблокировку данных в медицинских учреждениях, как, например, в случае с шифровальщиком SamSam¹⁵, который вот уже на протяжении трех лет атакует государственные учреждения и больницы. Это вредоносное ПО шифрует все данные на серверах, блокируя этим работу медучреждений, и требует выкуп за расшифровку. От непрерывной работы медицинских систем зависят жизни людей, а восстановление данных из резервных копий требует времени. Поэтому больницы часто выплачивают требуемые суммы даже в тех случаях, когда возможность восстановить работу в принципе имеется.

¹⁴ sec.gov/Archives/edgar/data/1001233/000119312518119788/d562135d8k.htm

¹⁵ healthitsecurity.com/news/samsam-ransomware-attackers-target-healthcare-providers



Ущерб более
100 млн долл. США

Криптовалютные биржи

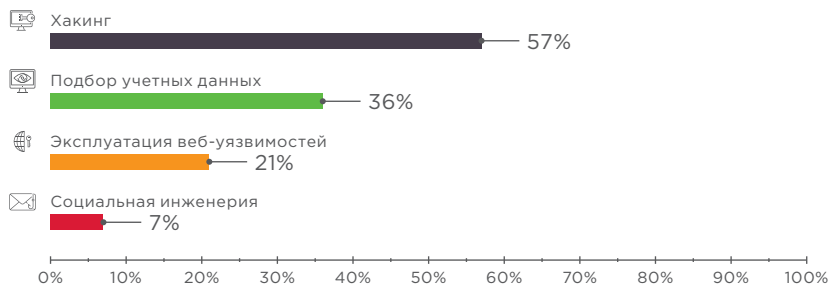


Рисунок 25. Методы атак на криптовалютные биржи в Q2 2018

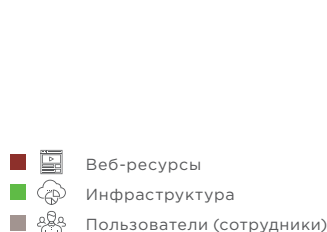


Рисунок 26. Объекты атак

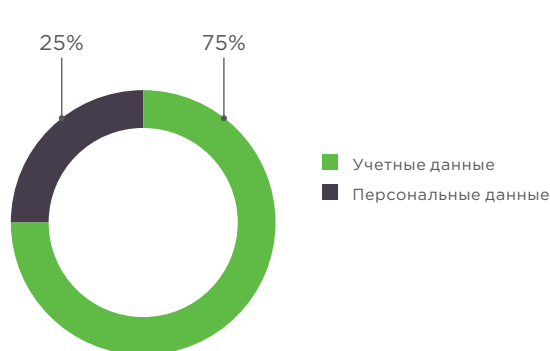
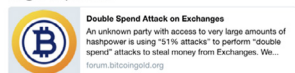


Рисунок 27. Украденные данные



An unknown party accessing large amounts of hashpower is using "51% attacks" to perform "double spend" attacks on Exchanges. We have been advising all exchanges to increase their confirmations requirement and to review large deposits.



6:47 PM - 18 May 2018



\$XVG @vergecurrency is once again under attack, someone is 51%ing the chain and invalidating all legit blocks. All pools and miners suffer from this, the attacker is getting all blocks currently.

10:51 AM - 22 May 2018

Рисунок 28. Новости об атаках на криптовалютные сети

Во II квартале 2018 года произошел ряд атак «51 процент» на криптовалюты, поддерживающие алгоритм консенсуса proof of work (PoW). В ходе данной атаки злоумышленник (чаще всего это группа людей) получает в распоряжение «контрольный пакет» генерирующих мощностей сети (хешрейта), то есть мощности большие, чем у всей остальной сети. Злоумышленник, который контролирует больше половины хешрейта, получает возможность манипулировать операциями и, например, не подтверждать новые транзакции или отзываться совершенные транзакции, используя одну и ту же монету несколько раз.

В результате атак на криптовалютные сети Verge¹⁶, Monacoin¹⁷, Bitcoin Gold¹⁸, ZenCash¹⁹, Litecoin Cash²⁰ злоумышленники смогли заработать десятки миллионов долларов. Несмотря на то что в ходе этих атак преступники воруют деньги не напрямую у пользователей, в конечном счете все равно могут пострадать именно клиенты криптовалютных сетей, поскольку атакованные ресурсы рискуют обанкротиться, организаторы могут запретить обналичивать криптовалюту — и, несомненно, происходящее отражается на курсе криптовалют.

¹⁶ news.bitcoin.com/verge-struck-by-second-pow-attack-in-as-many-months/

¹⁷ newsbtc.com/2018/05/22/japans-monacoin-network-still-suffering-selfless-mining-attack/

¹⁸ forum.bitcoingold.org/t/double-spend-attacks-on-exchanges/1362

¹⁹ bitcoinist.com/zenscash-target-51-attack-loses-500k-double-spend-transactions/

²⁰ cryptocurrencynews.com/litecoin-cash-lcc-51-attack/



Пострадали более
48 млн человек

Торговля

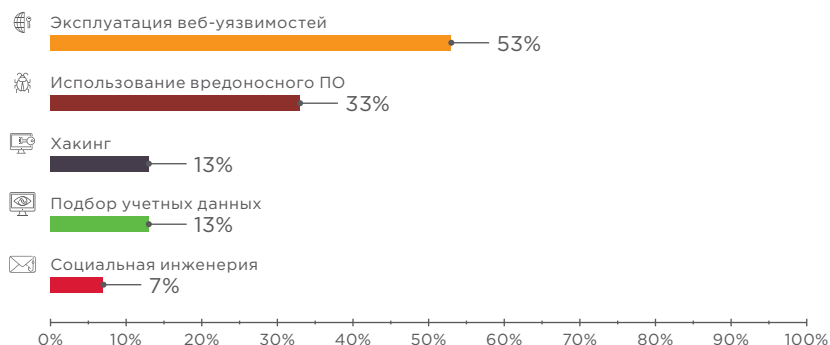


Рисунок 29. Методы атак в сфере торговли в Q2 2018

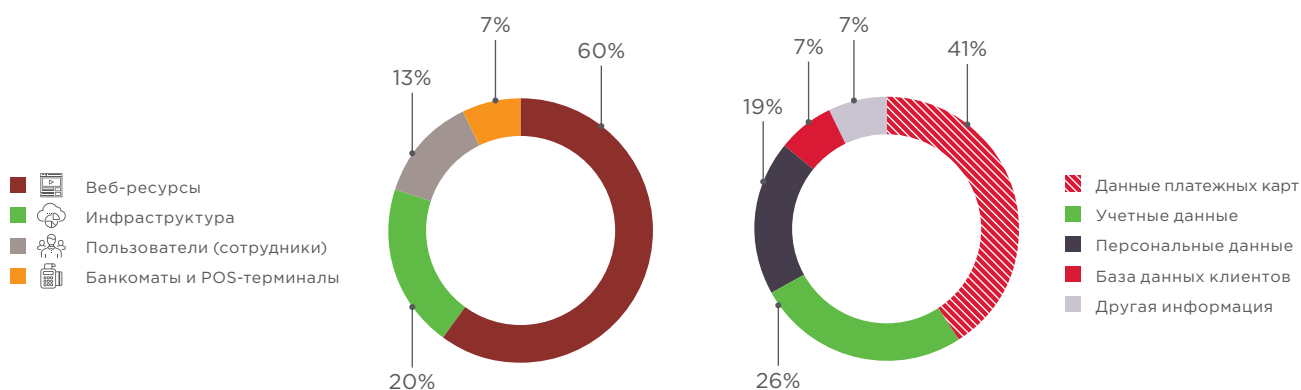


Рисунок 30. Объекты атак

Рисунок 31. Украденные данные

Из-за атак на розничные и интернет-магазины страдают преимущественно их клиенты. Причем некоторые кибератаки могут оставаться незамеченными по несколько месяцев, например до тех пор, пока на теневом рынке не появится в продаже база с данными банковских карт.

Именно так стало известно о крупнейшей атаке в сфере розничной торговли, в результате которой злоумышленники похитили данные более 5 млн банковских карт из торговых сетей Saks Fifth Avenue и Lord & Taylor²¹. Кража происходила с помощью вредоносного ПО, установленного на POS-терминалы в розничных магазинах, а значит, для клиентов и продавцов оплата покупки выглядела обычным образом.

Более половины (60%) атак в сфере торговли были нацелены на веб-ресурсы. Интернет-магазины, бизнес которых построен на работе сайта, несут серьезные потери в случае нарушения его работы. Так, например, из-за дефейса главной страницы сайта временно прекращал свою работу сервис по продаже билетов Ticketfly. Кроме того, именно веб-уязвимости могут позволить злоумышленникам получить доступ к персональным и банковским данным пользователей. Например, онлайн-пекарни Panera Bread²² не обеспечили достаточную защиту веб-ресурсов, в результате чего имена, адреса электронной почты и физические адреса, даты рождения и последние четыре цифры номеров кредитных карт нескольких миллионов клиентов были доступны в виде обычного текста.

21 blog.gemalto.com/security/2018/04/03/saksfifthavenuedatabreach/

22 krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/



Рисунок 32. Недостаточная защита веб-ресурсов пекарни Panera Bread

Частные лица



Ущерб более
22 млн долл. США

Пострадали более
765 млн человек



Рисунок 33. Методы атак на частных лиц в Q2 2018

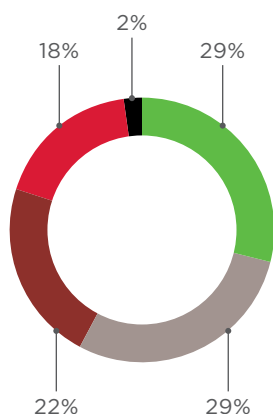
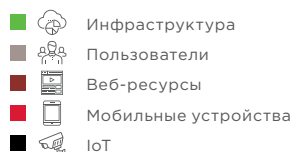


Рисунок 34. Объекты атак

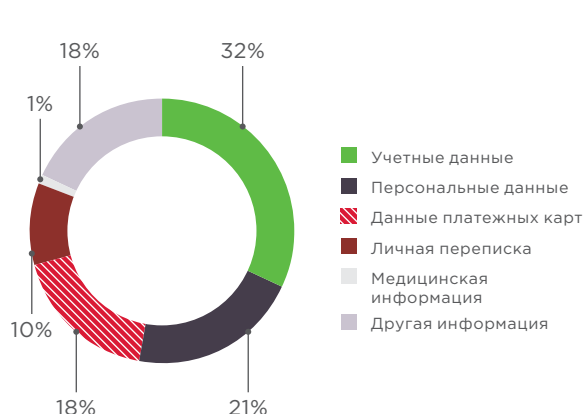


Рисунок 35. Украденные данные

Каждая четвертая кибератака нацелена на частных лиц. А из-за того, что в большинстве своем эти атаки массовые, общее количество жертв исчисляется сотнями миллионов. И никто не может гарантировать, что данные вашей банковской карты по-прежнему известны только вам, а копия вашего паспорта не продается на теневом рынке вместе с другими.

Даже на новом смартфоне, купленном в магазине, может быть установлено вредоносное ПО, особенно это касается устройств китайских производителей. Так, исследователи из Avast обнаружили²³ тысячи мобильных телефонов, на которых было установлено вредоносное ПО Cosiloop на уровне прошивки. Производитель поставлял устройства с предустановленными приложениями-дропперами для скрытого развертывания рекламного ПО. Но поскольку дальнейшая загрузка производилась с командного центра, то помимо надоедливых всплывающих окон на устройство могло быть загружено и шпионское ПО, и шифровальщик, и любое другое ВПО.

В начале лета специалисты по ИБ обнаружили²⁴ вредоносную кампанию, нацеленную на пользователей macOS. Злоумышленники использовали каналы Slack и Discord, посвященные криптовалютам, для распространения сообщений о необходимости ввести на компьютере определенную команду, чтобы решить какие-то проблемы. После ввода вредоносной команды жертвы сами предоставляли атакующим доступ к системе. В дальнейшем злоумышленники могут продолжить атаки, например похищая криптовалюту.



Злоумышленники продолжают втираться в доверие к пользователям, маскируя фишинговые сайты под госсервисы. Во II квартале 2018 года от подобных атак пострадало более 300 тысяч граждан Белоруссии, Казахстана, России и Украины.

Так, например, злоумышленники создали шесть идентичных сайтов «Активный гражданин»²⁵, где за участие в опросе обещали выплатить 65 000 рублей. После прохождения опроса участникам предлагалось активировать аккаунт за 170 рублей, а затем еще предлагался целый список платных услуг, однако никакого вознаграждения, естественно, никто не получал.

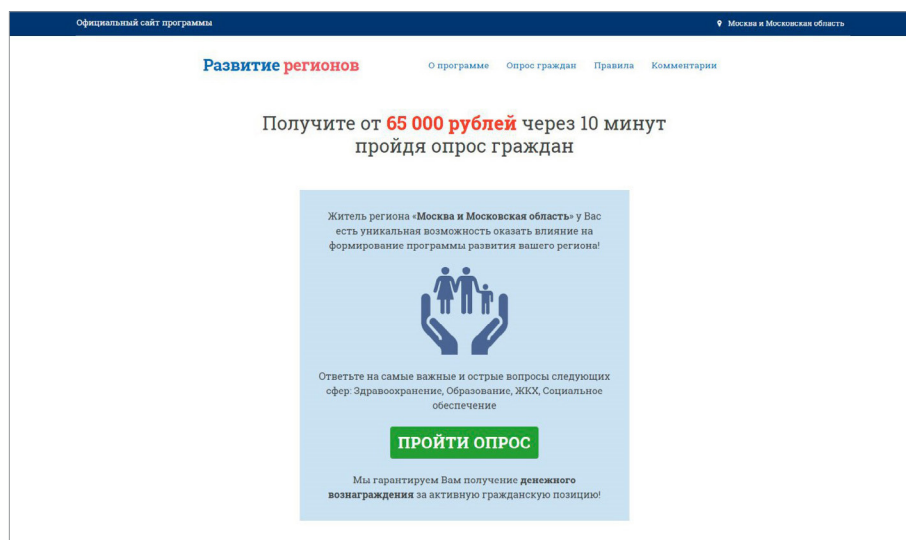


Рисунок 36. Пример сайта злоумышленников

²³ blog.avast.com/android-devices-ship-with-pre-installed-malware

²⁴ objective-see.com/blog/blog_0x32.html

²⁵ group-ib.ru/media/fake-survey/

Как защититься организации

Используйте эффективные технические средства защиты:

- средства централизованного управления обновлениями для используемого ПО;
- антивирусные программы (на всех устройствах), в том числе специализированные, например позволяющие пользователям отправлять подозрительные файлы на проверку перед открытием вложения из письма;
- SIEM-решения — для своевременного обнаружения атаки, если инфраструктура оказалась заражена;
- автоматизированные средства анализа защищенности и выявления уязвимостей в ПО;
- межсетевой экран уровня приложений (web application firewall) в качестве превентивной меры защиты веб-ресурсов;
- специализированный сервис для защиты от DDoS-атак.

Защищайте данные:

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

Не допускайте использования простых паролей:

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

Контролируйте безопасность систем:

- своевременно обновляйте используемое ПО по мере выхода патчей;
- проверяйте и повышайте осведомленность сотрудников в вопросах информационной безопасности;
- контролируйте появление небезопасных ресурсов на периметре сети;
- регулярно проводите тестирование на проникновение для своевременного выявления новых векторов атак на внутреннюю инфраструктуру и оценки эффективности принятых мер по защите;
- регулярно проводите анализ защищенности веб-приложений, включая анализ исходного кода, с целью выявления и устранения уязвимостей, позволяющих проводить атаки, в том числе на клиентов приложения;
- отслеживайте количество запросов к ресурсам в секунду, настройте конфигурацию серверов и сетевых устройств таким образом, чтобы нейтрализовать типичные сценарии атаки (например, TCP- и UDP-флуд или множественные запросы к БД);
- эффективно фильтруйте трафик для минимизации доступных внешнему злоумышленнику интерфейсов сетевых служб.

Позаботьтесь о безопасности клиентов:

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



Как вендору защитить свои продукты:

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

Как защититься обычному пользователю

Не экономьте на безопасности:

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

Защищайте ваши данные:

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

Не используйте простые пароли:

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

Будьте бдительны:

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

О компании

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

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

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