



POSITIVE TECHNOLOGIES

Актуальные киберугрозы

I 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	9
Хакинг	10
Эксплуатация веб-уязвимостей	11
Подбор учетных данных	12
DDoS	13
Категории жертв	14
Государственные учреждения	14
Медицинские учреждения	16
Финансовая отрасль	17
Образование	18
Частные лица	19
Как защититься организации	20
Как вендору защитить свои продукты	21
Как защититься обычному пользователю	21



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

Киберпреступный мир постоянно меняется, и мы меняем свои подходы к анализу данных, исследуя новые векторы кибератак. Компания Positive Technologies продолжает делиться с вами информацией об актуальных угрозах информационной безопасности. Эта информация основана на нашей собственной экспертизе, результатах многочисленных расследований и на сведениях из авторитетных источников.

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

- Количество уникальных киберинцидентов продолжило расти и на 32% превысило показатели аналогичного периода в 2017 году.
- Существенно выросла доля атак, нацеленных на получение данных. Причем злоумышленников преимущественно интересовали персональные данные, а также учетные записи и пароли для доступа к различным сервисам и системам. Злоумышленники в дальнейшем либо пытаются продать эту информацию на черном рынке, либо продолжают с ее помощью свои атаки.
- Самым распространенным методом атак стало использование вредоносного ПО. Этот метод злоумышленники часто комбинировали с другими, например с социальной инженерией или эксплуатацией веб-уязвимостей.
- Самым используемым типом вредоносного ПО стало шпионское. С его помощью злоумышленники получали не только персональные данные пользователей и коммерческую тайну компаний, но и учетные данные от различных сервисов и систем, что позволяло развивать атаку на внутреннюю инфраструктуру.
- Больше других от кибератак пострадали частные лица, причем пять из каждых шести атак были совершены с использованием вредоносного ПО. Причиной большого числа успешных атак может быть отсутствие антивирусов на устройствах жертв, а также невнимательное отношение к загружаемым из интернета файлам и открываемым ссылкам.
- В 2017 году мы отмечали рост ботнетов, в том числе за счет новых IoT-устройств; существенно увеличилась мощность DDoS-атак. И вот, в последний день зимы была зафиксирована самая мощная DDoS-атака в истории — 1,35 терабита в секунду.

Наши прогнозы:

- Рост количества уникальных кибератак продолжится.
- Злоумышленники продолжат развивать уже существующие векторы атак, в том числе на государственные и финансовые организации.
- Появятся новые образцы вредоносного ПО, преимущественно шпионского и используемого для майнинга криптовалюты.
- Фишинговые атаки будут посвящены тематике предстоящего чемпионата мира по футболу.
- Будут новые масштабные DDoS-атаки, в том числе политической направленности.



Сводная статистика

В I квартале 2018 года мы отметили значительные изменения в мотивации злоумышленников. Так, выросла доля атак, направленных на получение данных (36% — вместо 23%, среднегодового значения в 2017-м). Это не означает, что преступников стали меньше интересовать деньги, финансовую выгоду они преследовали более чем в половине кибератак (53%). Основная причина кроется в том, что вслед за атакой, в ходе которой были получены данные, злоумышленники либо продолжают преступные действия в адрес жертвы или ее клиентов и контрагентов (например, если была украдена клиентская база), либо попытаются продать информацию на черном рынке.

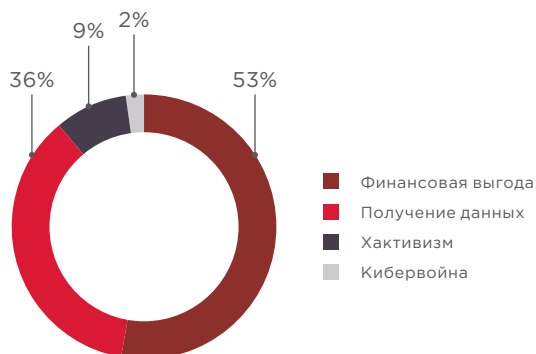


Рисунок 1. Мотивы злоумышленников

В 36% атак злоумышленникам становилась известна конфиденциальная информация жертвы. Мы рассмотрели, какая информация больше всего привлекала преступников. В трети случаев (33%) это были персональные данные, а в 28% — учетные записи и пароли для доступа к различным сервисам и системам. Стоит отметить, что, получив учетные данные, злоумышленники часто продолжали атаку и получали доступ к критически важным инфраструктурным объектам, таким как базы данных, рабочие станции директоров и бухгалтеров, серверы управления (например, веб-ресурсами).

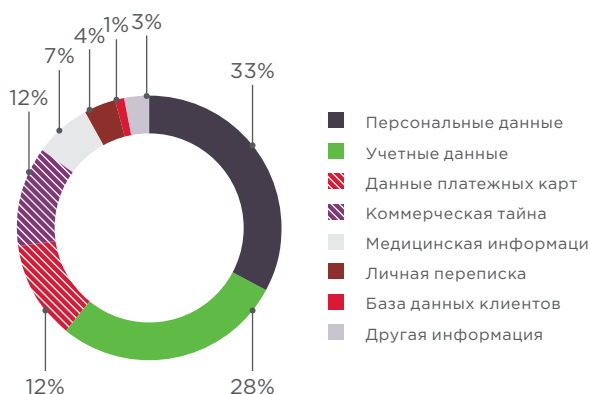


Рисунок 2. Типы украденных данных

Самая значительная часть атак (28%) была направлена на частных лиц. Продолжила расти и доля киберинцидентов, нацеленных на государственные учреждения: в I квартале 2018 года они составили 16% всех атак. Далее мы остановимся подробнее на атаках, направленных на государственные и медицинские учреждения, финансовую отрасль, сферу образования и на частных лиц. Масштабные кибератаки, преимущественно вредоносные эпидемии, которые не ограничиваются воздействием на какую-то одну отрасль, мы отнесли к категории «без привязки к отрасли».

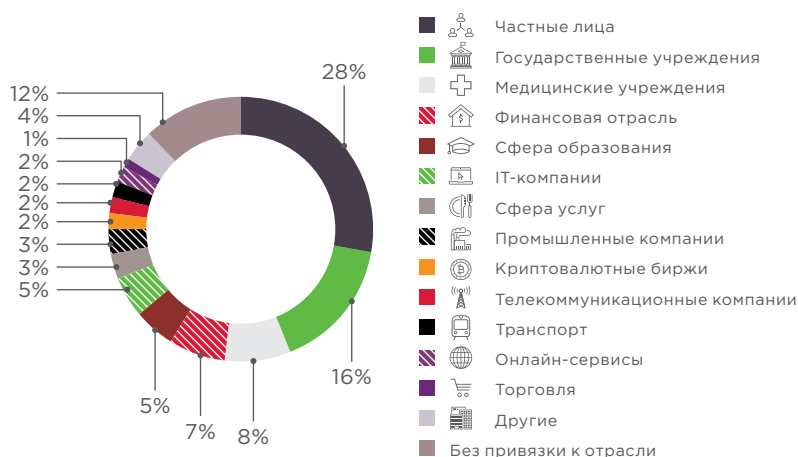


Рисунок 3. Категории жертв

Доля атак, нацеленных на инфраструктуру, в I квартале 2018 года составила 52%. Веб-ресурсы атаковали реже, чем в прошлом году, а доля направленных на них атак составила 19% — вместо 26% в 2017.

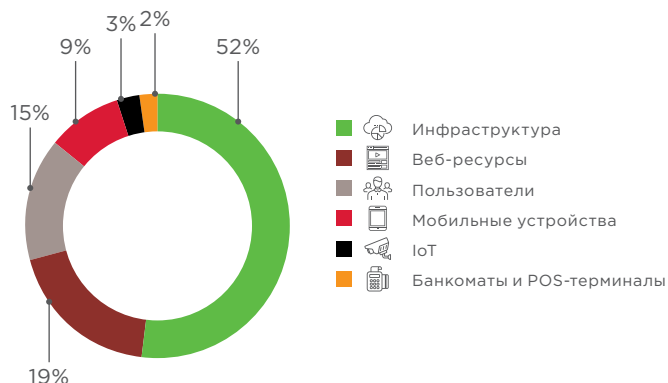


Рисунок 4. Объекты атак

В рамках одной кибератаки стали все чаще применяться одновременно несколько методов. Например, в 18% атак злоумышленники одновременно использовали и вредоносное ПО, и методы социальной инженерии, а в 5% — эксплуатировали веб-уязвимости и применяли вредоносное ПО. Далее мы подробнее остановимся на каждом методе и укажем, какие объекты и отрасли больше всего от них пострадали.

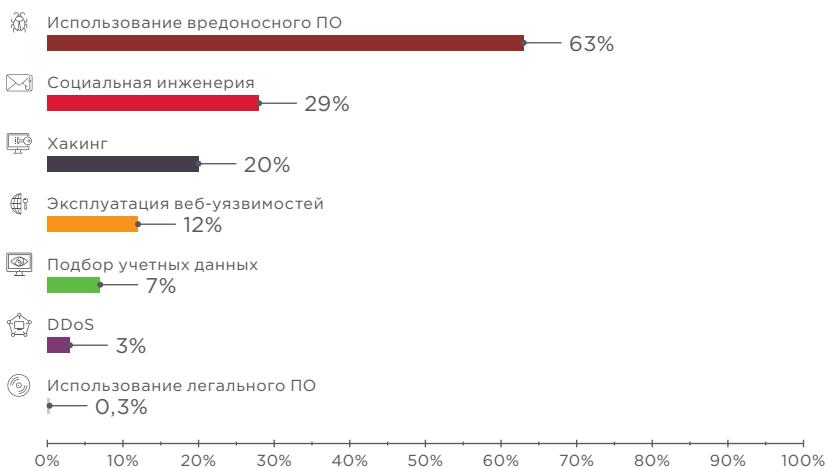


Рисунок 5. Методы атак



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		51	22	9	24	3	10	15	16	4	6	87	6	7	12	38
Объект	Инфраструктура	30	12	7	19	1	5	3	9	1	4	31	2	1	9	29
	Веб-ресурсы	12	4	1	3	2		8	3		1	14	2	4	1	3
	Пользователи	8	4	1	2	2	2	4	3	2	1	11	2	2	2	
	Мобильные устройства		1									27				
	Банкоматы и POS-терминалы		1				2			1		2				
	IoT	1					1		1			2				6
Метод	Атаки с использованием ВПО	29	11	6	11	1	5	5	5	3	2	73	2	1	6	37
	Социальная инженерия	18	9	2	3	2	2	2	6	1	2	28	1	2	6	5
	Подбор учетных данных	3	1		3	1	1		2		1	6	1	2		1
	Хакинг	9	7	3	6		2	2	4	1	2	8	1	3	3	10
	Эксплуатация веб-уязвимостей	5	2	1	3	2		7	2	1		9	1	1	2	
	DDoS	6	1					2			1					
	Другой														1	
Мотив	Финансовая выгода	9	14	5	8	1	7	7	3	1	1	68	4	7	3	26
	Получение данных	25	8	2	15	3	3	5	11	3	4	18	2		6	8
	Хактивизм	13		1	1	1		3	2		1				2	4
	Кибервойна	4		1								1			1	

Интенсивность цвета
показывает долю атак
в рамках одной отрасли





Динамика атак

Количество уникальных киберинцидентов в I квартале 2018 года на 32% превысило показатели аналогичного периода в 2017 году. Причем большинство атак произошли (либо были выявлены) в феврале и марте, в то время как в январе мы преимущественно узнавали подробности масштабных вредоносных кампаний, раскрытых антивирусными вендорами. Возможно, после долгих новогодних праздников специалисты по ИБ не сразу обнаруживали, что их организации стали жертвами киберпреступников.

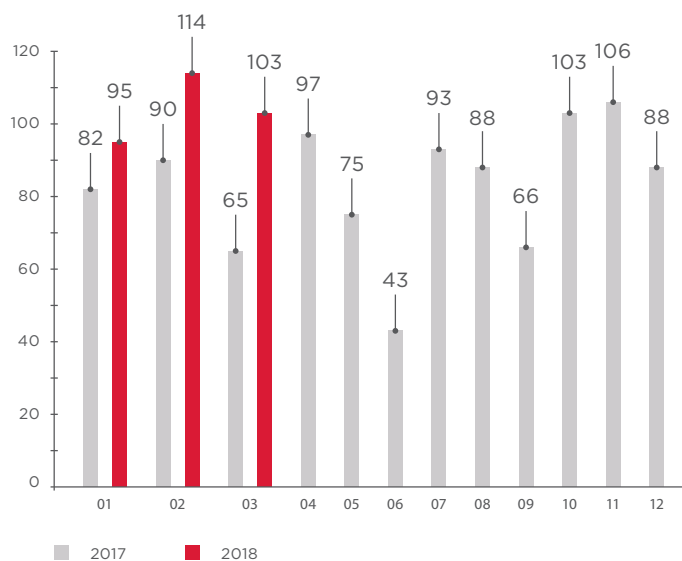


Рисунок 6. Количество инцидентов в 2017 и 2018 годах (по месяцам)

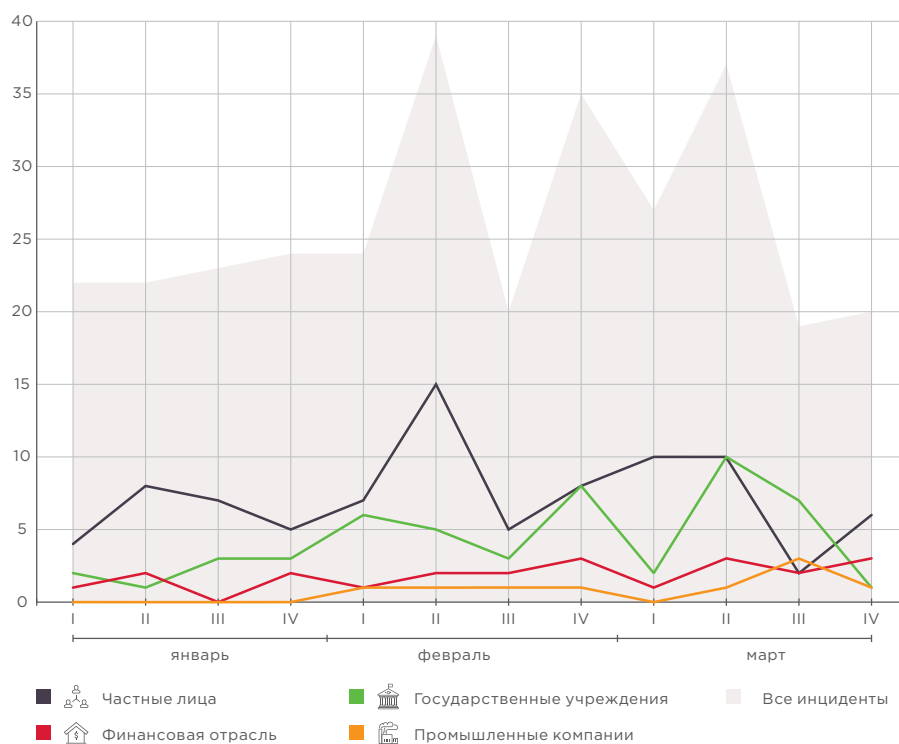


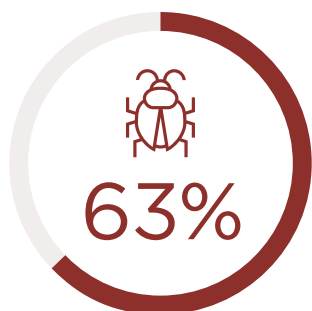
Рисунок 7. Количество инцидентов в I квартале 2018 года (по неделям)



Методы атак

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

Использование вредоносного ПО



Самым распространенным методом атак является использование вредоносного ПО. Этот метод злоумышленники часто комбинируют с другими, например социальной инженерией или эксплуатацией веб-уязвимостей. В I квартале 2018 года вредоносное ПО применялось в 63% уникальных кибератак. Причем в 30% случаев использовалось шпионское ПО — вредоносные программы, нацеленные на получение чувствительной информации с зараженного устройства, преимущественно учетных данных. В 23% атак злоумышленники распространяли майнеры криптовалюты. Большую популярность в I квартале получил троян WannaMine, заразивший по всему миру более 500 000 устройств (преимущественно Windows-серверов) и использующий их мощности для генерации криптовалюты Monero. Для распространения это ВПО использует эксплойты EternalBlue (CVE-2017-0144) и EsteemAudit (CVE-2017-0176).

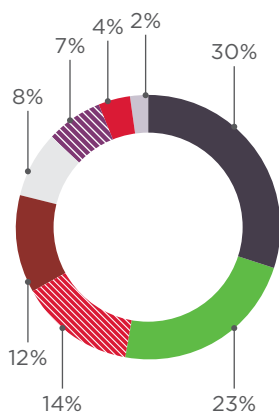
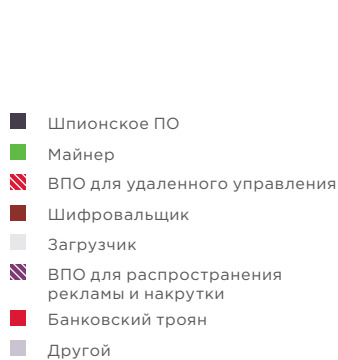


Рисунок 8. Типы вредоносного ПО

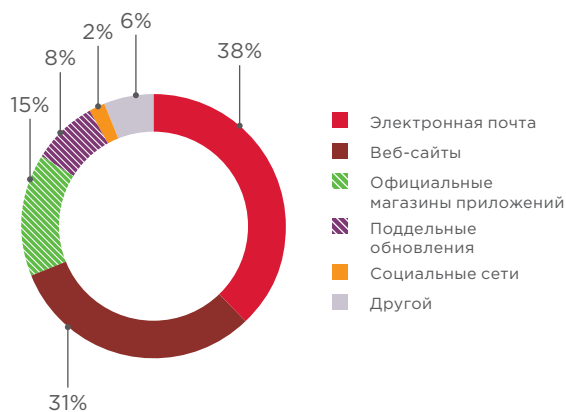


Рисунок 9. Способы распространения ВПО

Примечательно, что в 38% атак с использованием этого метода ВПО рассылалось жертвам по электронной почте. Чаще всего таким образом распространяли шпионское ПО, ПО для удаленного управления (RAT) и шифровальщики. Скомпрометированные веб-сайты, а также фишинговые веб-ресурсы преимущественно устанавливали на устройство жертвы майнеры криптовалют и шпионское ПО.



Социальная инженерия



Наиболее атакуемые объекты



53%



39%



7%

Больше всего пострадали



31%



20%



10%

Методы социальной инженерии применяются злоумышленниками преимущественно вместе с вредоносным ПО (примером могут служить фишинговые сайты, содержащие ВПО), но не только. Так, в I квартале 2018 года прошла ожидаемая волна атак, нацеленных на персональные данные сотрудников американских компаний. В начале каждого календарного года в организациях в США принято формировать справки на каждого работника по форме W-2. Эти документы содержат персональную информацию о сотруднике, включая имя, адрес, номер социального страхования, а также сведения о заработной плате и уплаченных налогах за прошедший год. Злоумышленники заинтересованы в этой информации и, чтобы ее заполучить, направляют в компании (часто директорам) фишинговые письма, в которых представляются партнерами или налоговыми агентами и требуют предоставить справки W-2 по всем сотрудникам.

ICO-проекты не теряют своей популярности среди инвесторов и тем самым привлекают злоумышленников. Так, в начале 2018 года произошли сразу две схожие атаки на пользователей проектов [Expertu](#) и [Bee Token](#). В первом случае злоумышленники похитили список электронных адресов людей, подписавшихся на уведомления от Expertu, и за пять дней до официального старта ICO разослали фальшивые письма о начале продаж токенов. Указанный в письмах Ethereum-кошелек для перевода средств принадлежал злоумышленникам, и в результате этой атаки были украдены более 150 000 долл. США. Аналогично поступили злоумышленники и в случае атаки на инвесторов Bee Token: выдали себя за организаторов и распространили собственные письма и сообщения в мессенджере о начале ICO.

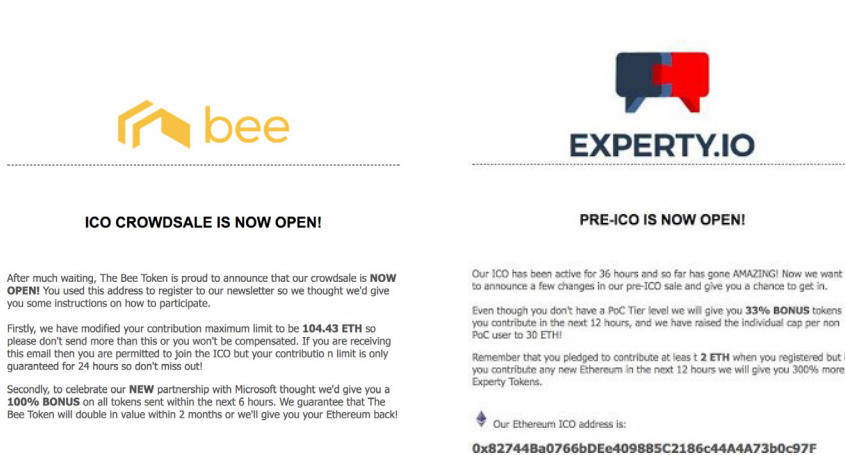
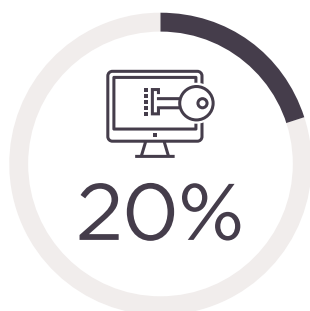


Рисунок 10. Фишинговые письма в адрес инвесторов Bee Token и Expertu



Хакинг



Наиболее атакуемые объекты



75%



10%



8%



15%



11%



10%

Больше всего пострадали

В данную категорию попали атаки, в ходе которых злоумышленники эксплуатировали уязвимости ПО, служб ОС, использовали ошибки в механизмах защиты или другие недостатки атакуемых систем. Например, в рамках целенаправленной атаки преступники могут сначала скомпрометировать инфраструктуру жертвы, получить доступ к серверам или компьютерам, на которых обрабатывается критически важная информация, а затем оставить в системе шпионское ПО, которое будет незаметно передавать хакерам конфиденциальную информацию.

Большинства атак этой категории можно было бы избежать, если бы компании вовремя устанавливали обновления ПО. Например, веб-серверы с устаревшим ПО Ruby on Rails, PHP и Microsoft IIS ASP были атакованы майнером [RubyMiner](#). Злоумышленники целенаправленно искали уязвимые веб-серверы с помощью инструмента [p0f](#), а затем удаленно выполняли код на целевой системе с применением одного из шести эксплойтов. Примечательно, что для скрытия своего присутствия сценарий загружался в файл robots.txt. В дальнейшем на сервер загружалась и устанавливалась модифицированная версия штатного приложения XMRIg, которая и генерировала криптовалюту Monero.



Эксплуатация веб-уязвимостей



Наиболее атакуемые объекты



71%



19%



25%



19%



14%

Больше всего пострадали

Онлайн-магазины часто становятся целью киберпреступников. Злоумышленники используют уязвимости веб-ресурсов, чтобы похитить данные платежных карт (а в дальнейшем и денежные средства) посетителей сайтов. Так, в конце 2017 — начале 2018 годов покупатели смартфонов и аксессуаров [OnePlus](#) на официальном сайте производителя стали жертвами мошенничества с банковскими картами. Уязвимости веб-ресурса позволили внедрить в него вредоносный сценарий, который захватывал и передавал преступникам данные покупателей, которые они вводили на сайте. Интересно, что пользователи, сохранившие свою платежную информацию в онлайн-кабинете, не пострадали, так как злоумышленникам не удалось добраться до базы данных.

Веб-уязвимости активно используются злоумышленниками для получения доступа к редактированию информации, публикуемой на сайте. Такого рода атаки могут нанести как финансовый ущерб компаниям, например в случае подмены кошелька для сбора криптовалюты на сайте ICO, так и репутационный.

Например, в январе 2018 года злоумышленники [получили доступ](#) к официальному сайту Футбольной ассоциации Новой Зеландии и опубликовали там поддельную информацию об отставке CEO Энди Мартина.

Похожий [инцидент](#) коснулся предвыборного сайта Ксении Собчак, где в результате дефейса на главной странице была размещена юмористическая картинка.

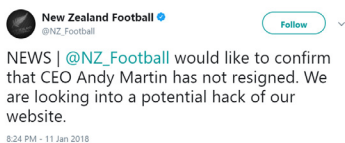


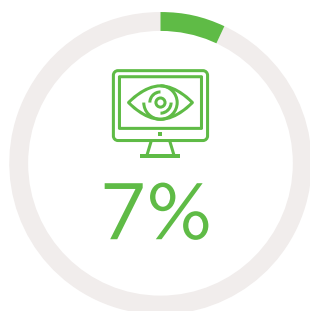
Рисунок 11. Сообщение о взломе веб-сайта в твиттере футбольной ассоциации



Рисунок 12. Дефейс предвыборного сайта Ксении Собчак



Подбор учетных данных



Рекомендации специалистов по информационной безопасности на тему парольной политики (об использовании сложных паролей, регулярной их смене и пр.) часто пропускают мимо ушей. Однако именно подбор учетных данных часто применяется для атак на веб-ресурсы. Так, например, более тысячи сайтов, работающих на CMS-платформе Magento, пострадали от действий злоумышленников, которые подобрали стандартные учетные данные для доступа к системам администрирования. Скомпрометированные сайты затем использовались:

- для перехвата POST-запросов к серверу, содержащих данные банковских карт;
- встраивания кода майнеров криптовалюты для ее генерации на компьютерах посетителей сайтов;
- перенаправления пользователей на фишинговые ресурсы.

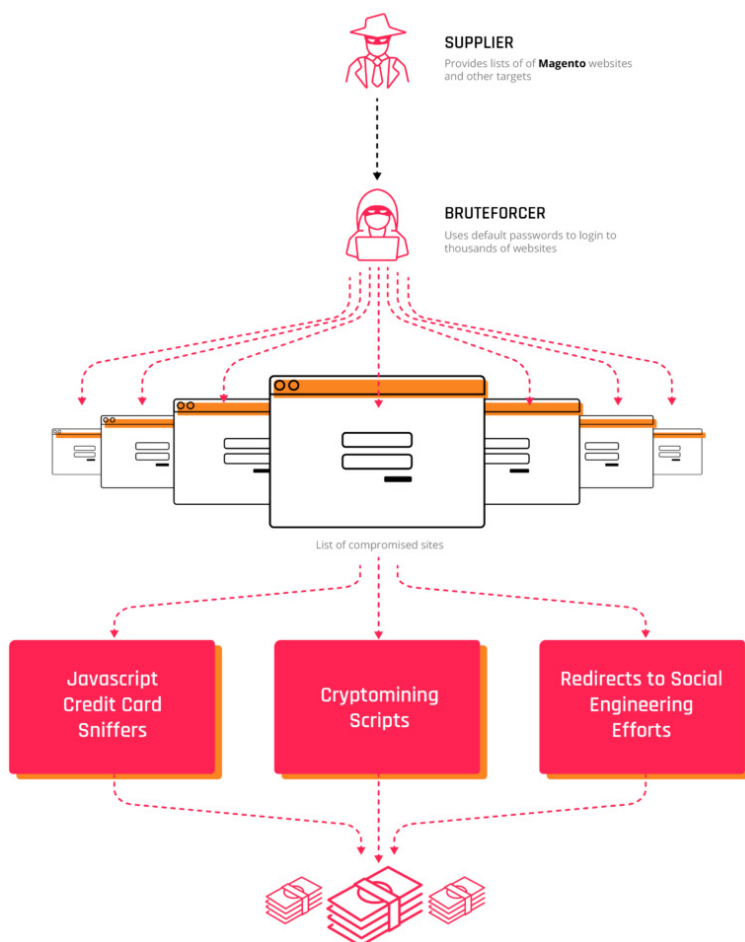
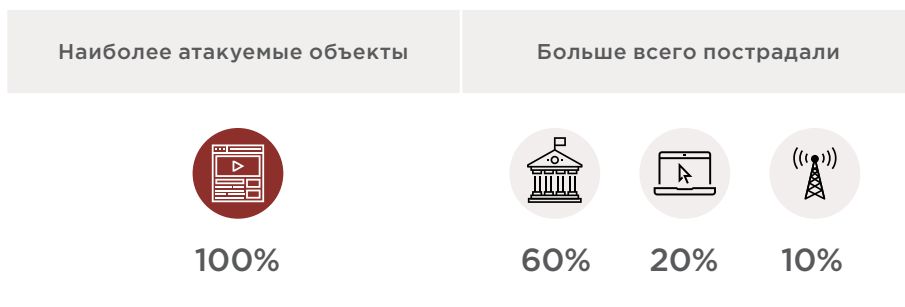
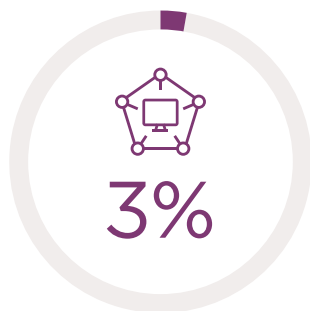


Рисунок 13. Схема атаки от специалистов компании Flashpoint



Кроме того, именно слабые пароли, подобранные злоумышленниками, зачастую оказываются исходным вектором проникновения в инфраструктуру компании. Так, в одном из инцидентов, расследование которого PT ESC проводил в конце 2017 года, преступникам удалось проникнуть во внутреннюю сеть компании благодаря успешному подбору пароля к доступному из интернета RDP-сервису на одном из серверов жертвы. В ходе атаки злоумышленники скомпрометировали ряд серверов и в течение нескольких дней контролировали внутренние ресурсы компании, оставаясь незамеченными. Инцидент был обнаружен лишь когда преступники зашифровали данные на нескольких серверах (что послужило причиной отказа некоторых систем) и потребовали выкуп за расшифровку. Стоит отметить, что в ходе подобных атак почтовый сервер также оказывается скомпрометирован, а значит, злоумышленники могут использовать честное имя компании-жертвы в фишинговых рассылках для клиентов и контрагентов. Этот инцидент в очередной раз показывает серьезность проблемы использования RDP и других сетевых интерфейсов, доступных из интернета, поскольку именно через них злоумышленник может получить доступ во внутреннюю сеть организации.

DDoS



В последний день зимы была зафиксирована самая мощная в истории DDoS-атака. Целью злоумышленников стал веб-сервис [GitHub](#), предоставляющий хостинг для IT-проектов. Мощность атаки достигла 1,35 терабита в секунду. Отразить атаку на GitHub помогли центры Akamai Prolexic. Серверы посредника маршрутизировали входящий и исходящий трафик с GitHub, и спустя восемь минут вредоносные пакеты были отсеяны и сайт вернулся к нормальной работе.

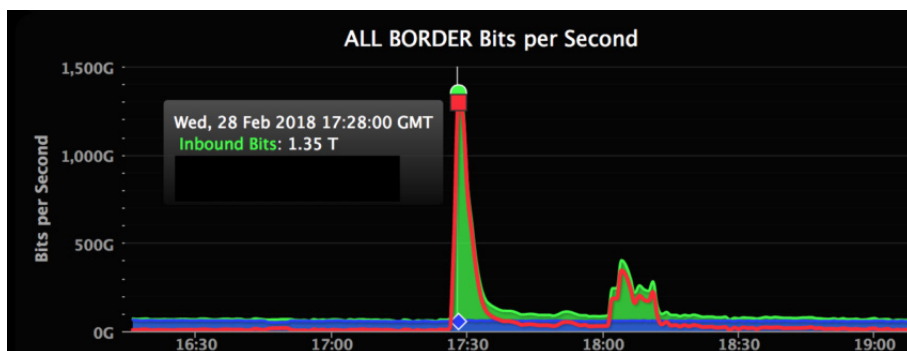


Рисунок 14. DDoS-атака на GitHub

Политические события часто провоцируют кибератаки. Так, в день выборов президента Российской Федерации [DDoS-атаке подвергся](#) сайт Центральной избирательной комиссии. А во время проведения финального голосования за названия новейших вооружений [был атакован](#) сайт Министерства обороны РФ.



Категории жертв

Далее мы подробнее остановимся на анализе атак на отдельные отрасли, которые в течение I квартала 2018 года чаще других становились целью злоумышленников.

Государственные учреждения



Пострадали более
500 тыс. человек

Ущерб более
1 млн долл. США



Рисунок 15. Методы атак на государственные учреждения

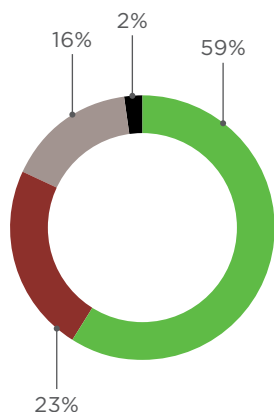
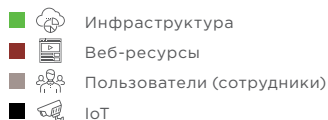


Рисунок 16. Объекты атак

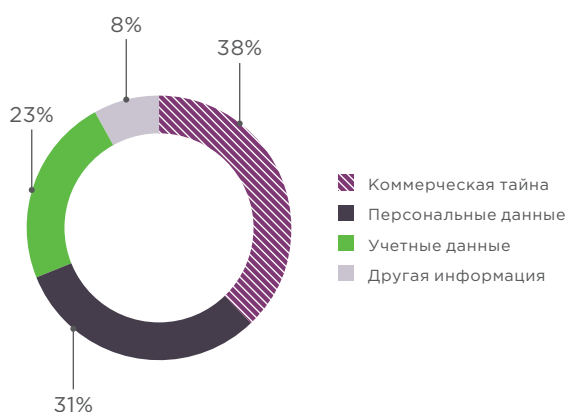


Рисунок 17. Украденные данные

Большинство атак на государственные учреждения в I квартале 2018 года проводились с использованием вредоносного ПО. Примечательно, что при этом 38% троянов представляли собой шпионское ПО, а еще 28% — программы для удаленного управления (RAT). В большинстве случаев эти типы ВПО оказывались в инфраструктуре государственных организаций через фишинговые рассылки по электронной почте. Например, в марте 2018 года специалисты PT ESC зафиксировали фишинговую рассылку APT-трояна в адрес госструктур. Злоумышленники использовали шпионское ПО — SANNY. Это ВПО, известное с 2012 года, было модифицировано и умело обходило User Account Control, компонент ОС Windows, защищающий от несанкционированного использования компьютера. Для каждой целевой компании злоумышленники формировали отдельный документ, содержащий макрос. Еще одна группировка, привлекавшая внимание сотрудников Positive Technologies, — ICEFOG аналогично действовала на территории СНГ, рассылая фишинговые документы с трояном Fucobha. Для загрузки ВПО в документах использовалась уязвимость CVE-2017-11882 в Office Equation Editor.



Углубление евразийской геополитики Китая и интересы безопасности России: транспортный аспект.

Тип проекта: а
Область знания: 07
Код классификатора РГНФ: 07-140
Код ГРНТИ: 73.01.17
Приоритетное направление развития науки, технологий и техники в Российской Федерации, критическая технология
7. Транспортные и космические системы.

Фамилия, имя, отчество руководителя проекта:
Аристова Людмила Борисовна Телефон руководителя проекта:
+79888269051
Объем финансирования проекта
на 2017 г.: 500 000 (пятьсот тысяч) рублей Год начала проекта 2018
Год окончания проекта 2019
Фамилии, имена, отчества основных исполнителей Семенова Н.К.

Название проекта
Углубление евразийской геополитики Китая и интересы безопасности России: транспортный аспект.
Тип проекта
а - проект проведения научных исследований, выполняемый научным коллективом или отдельным ученым
Область знания 07
Код классификатора 07-140
Дополнительные коды классификатора (при наличии приводятся дополнительные коды классификатора, к которым может быть отнесен проект) 07-110

Ключевые слова (приводится не более 15 слов)
Экономический пояс Шелкового пути, интересы безопасности РФ, Евразийский экономический союз, интеграция нового уровня, перспективы, риски

POSTAL ADDRESS - ADRESSE POSTALE: <redacted>
CABLE ADDRESS - ADRESSE TELEGRAPHIQUE: <redacted>
REFERENCE: <redacted> 8 December 2017
Dear <redacted>
On behalf of the Security Council Committee established pursuant to resolution 1718 (2006), I have the honour to refer to your letter dated 27 October 2017 on the unintended consequences of sanctions on humanitarian operations in the Democratic People's Republic of Korea (DPRK).

Рисунок 18. Вредоносные документы

Фишинговые документы, рассылаемые в ходе подобных атак, преимущественно используют известные уязвимости. И если компания вовремя обновляет используемое ПО, то случайное открытие сотрудником файла из электронной почты не приведет к компрометации внутренних ресурсов.

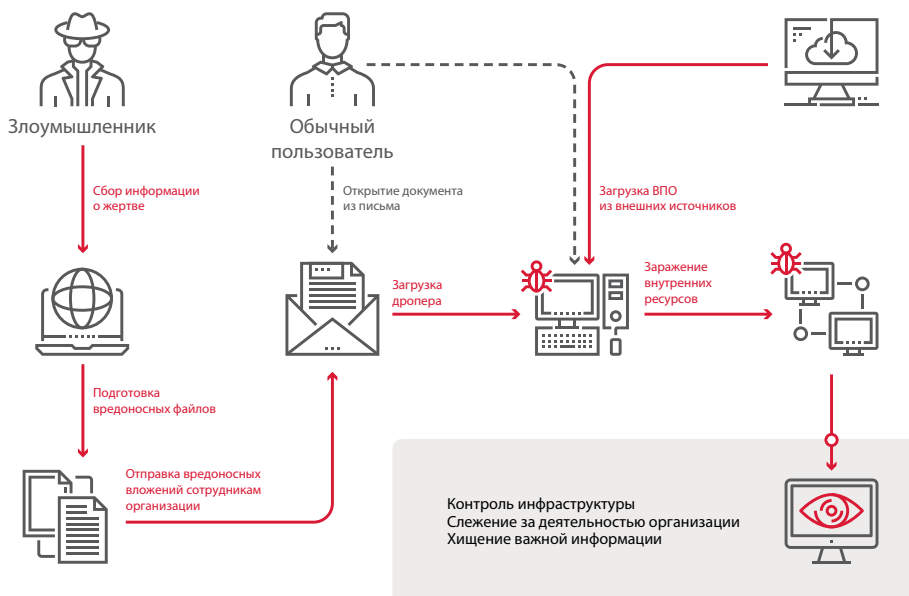


Рисунок 19. Типовая схема шпионской кампании



Пострадали более
3 млн человек

Медицинские учреждения

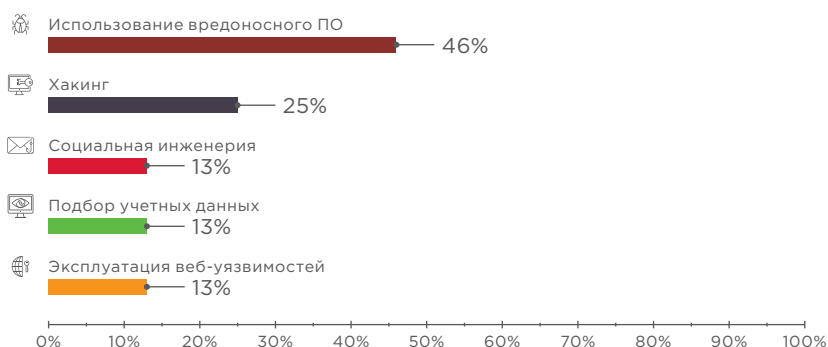


Рисунок 20. Методы атак на медицинские учреждения

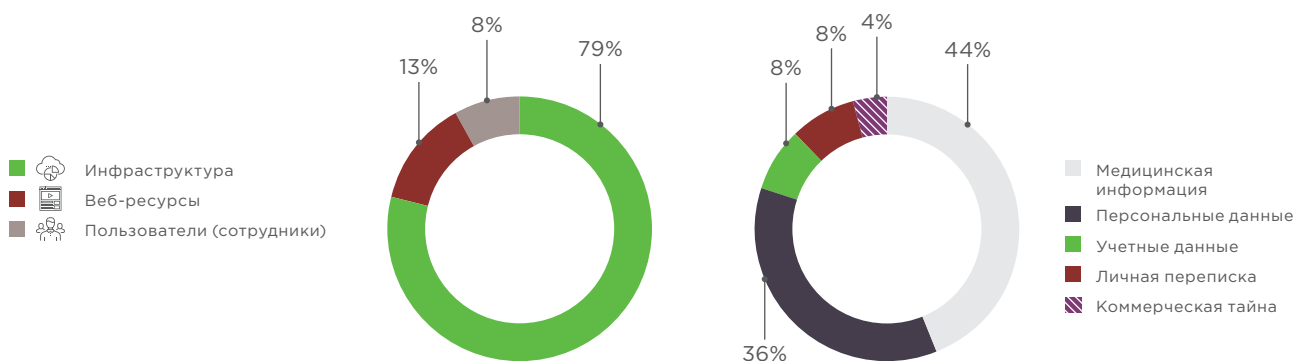


Рисунок 21. Объекты атак

Рисунок 22. Украденные данные

В ходе большинства (65%) атак на медицинские учреждения злоумышленники стремились получить доступ к чувствительной информации — преимущественно медицинским и персональным данным (44% и 36% соответственно). Но бывают ситуации, когда целью злоумышленников является ограничение доступа к этим данным. Так, в январе 2018 года американская клиника Hancock Health стала жертвой вредоносной кампании [SamSam](#). Злоумышленники с помощью вредоносного ПО зашифровали файловую систему организации и требовали выкуп за расшифровку. Этот инцидент существенно нарушил работу больницы, сотрудникам которой пришлось вносить данные в медицинские карты пациентов вручную. Несмотря на имеющиеся резервные копии, компания оценила, что восстановление всех систем займет слишком много времени, и заплатила вымогателям 55 тыс. долл. США.

Примечательно, что именно больницы многие эксперты считают отличной мишенью для вымогателей. Ведь от корректной работы медицинских IT-систем зависит самое ценное — жизни и здоровье людей, а значит, администрация легко пойдет на поводу у преступников.

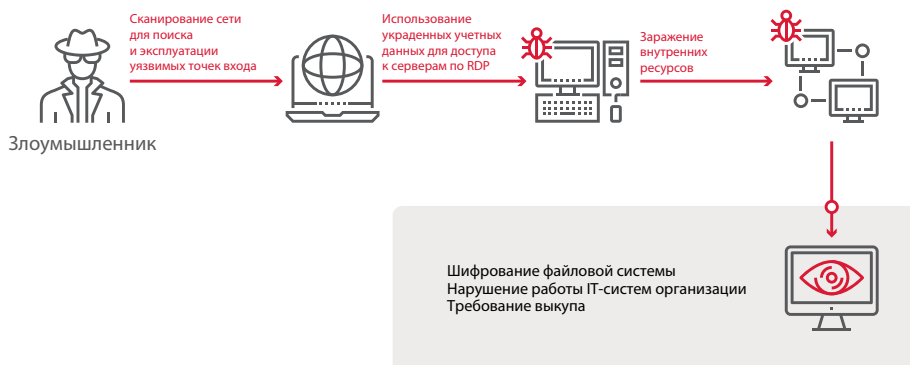


Рисунок 23. Схема вредоносной кампании SamSam



Финансовая отрасль



Ущерб более
83 млн долл. США

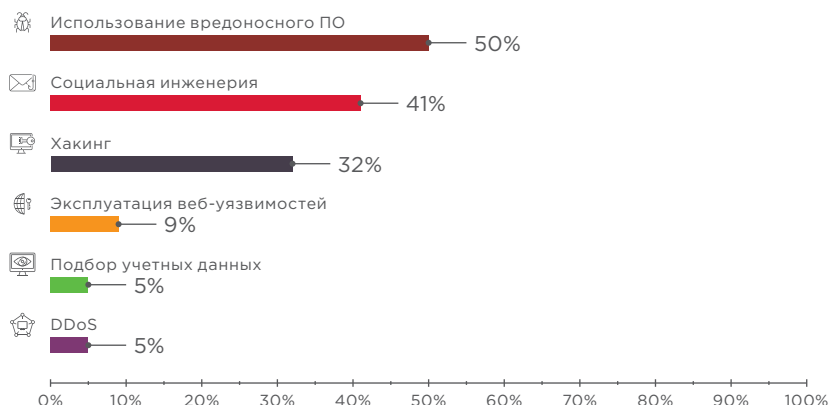


Рисунок 24. Методы атак на финансовую отрасль

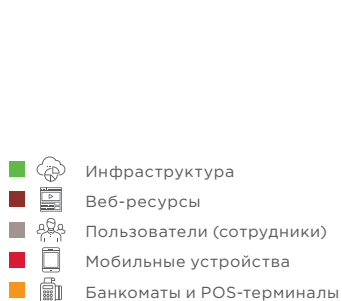


Рисунок 25. Объекты атак

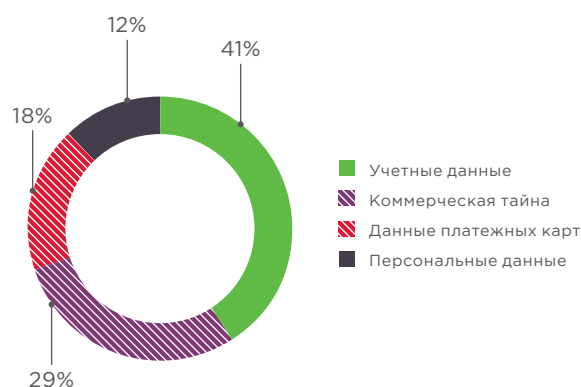


Рисунок 26. Украденные данные

Атаки на компании финансовой отрасли традиционно наносят наибольший ущерб. Шестьдесят четыре процента кибератак были совершены в целях получения финансовой выгоды, остальные 36% — для получения информации, преимущественно учетных данных (например, от внутренних банковских систем) и банковской информации (например, сведений о личных счетах клиентов).

В I квартале 2018 года внимание общественности привлекли атаки на банкоматы США с использованием вредоносного ПО («джекпоттинг»), принесшие преступникам более 1 млн долл. США. Злоумышленники использовали униформу сотрудников компаний, обслуживающих банковское оборудование, портативный компьютер, эндоскоп и мобильное устройство, с помощью которых подключались к банкомату. Они устанавливали специализированное вредоносное ПО (такое как *Ploutus-D*), которое позволяло управлять банкоматом и получить весь запас наличных¹. Кроме того, в I квартале специалисты PT ESC продолжали фиксировать вредоносные рассылки группировки Cobalt в адрес банков; теперь использовался новый компоновщик документов с ThreatKit с январской уязвимостью [CVE-2018-0802](#).

¹ Подробное исследование логических атак на банкоматы с использованием данного класса вредоносного ПО представлено в отчете Positive Technologies «Атаки на банкоматы на примере GREENDISPENSER: организация и технологии».



Образование



Пострадали более
14 млн человек

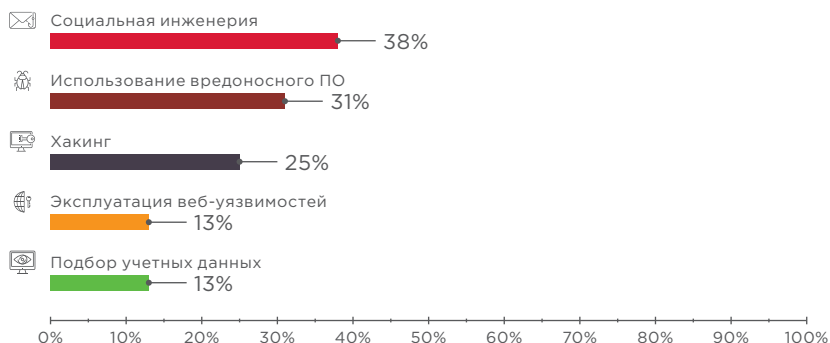


Рисунок 27. Методы атак на образовательные учреждения

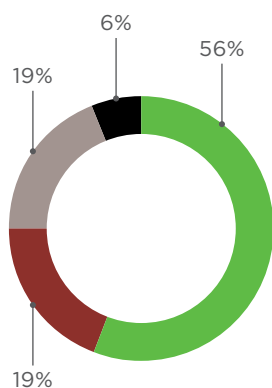
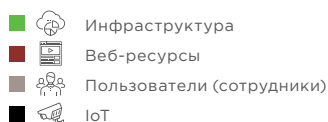


Рисунок 28. Объекты атак



Рисунок 29. Украденные данные

В атаках на образовательные учреждения злоумышленники чаще всего стремятся получить доступ к данным. Так, в 75% атак был получен доступ к персональным данным учащихся или сотрудников, интеллектуальной собственности, учетным данным от образовательных информационных систем. Отметим, что многие университеты проводят серьезные научные исследования, которые затем используются в военной, промышленной и других сферах, и эти наработки могут быть целью атак.

Так, в феврале Министерство юстиции США завело уголовное дело против девяти уроженцев Ирана, участвовавших в атаках на 320 университетов в 22 странах для хищения научной документации и данных об исследованиях. Злоумышленники в ходе фишинговых кампаний получали учетные данные от электронной почты профессоров и от компьютерных систем университетов. Похищенная информация распространялась через сервисы Megaraper.ir и Gigaraper.ir, позволяющие бесплатно получать доступ к различным научным работам, а также могла передаваться иранскому правительству.



Рисунок 30. Фрагмент объявления ФБР о поиске киберпреступников



Частные лица



Ущерб более
9 млн долл. США

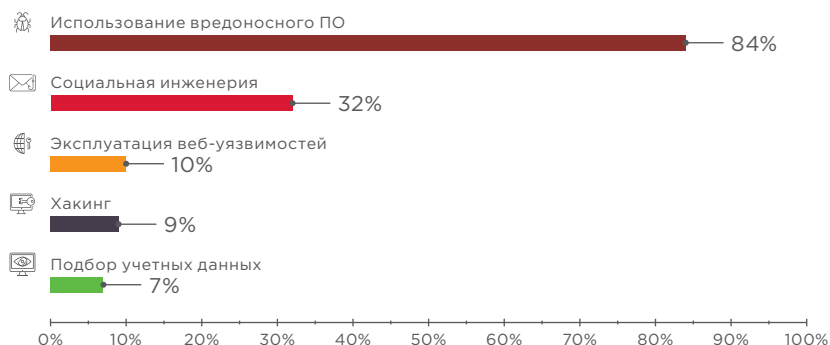


Рисунок 31. Методы атак на частных лиц

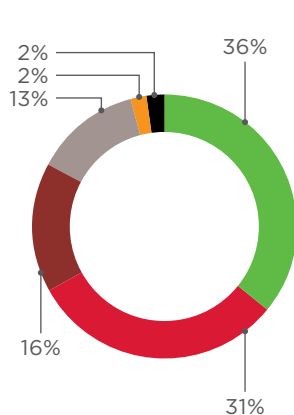
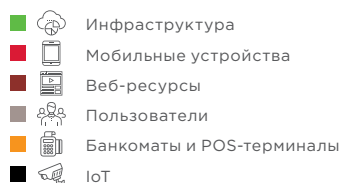


Рисунок 32. Объекты атак

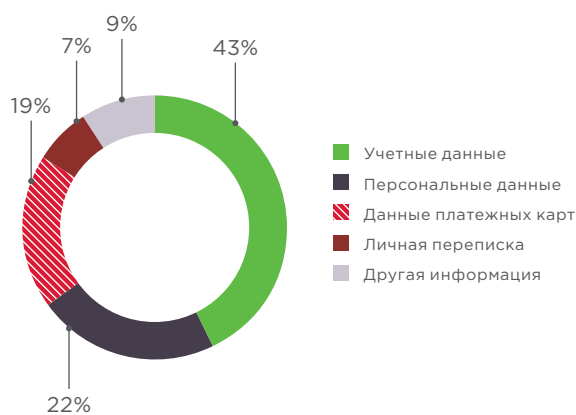


Рисунок 33. Украденные данные

В I квартале 2018 года 28% атак были нацелены на обычных людей. Примечательно, что в пяти из каждых шести киберинцидентов было использовано вредоносное ПО. Чаще других на устройства жертв попадало шпионское ПО (34% случаев заражения), майнеры криптовалюты (27%) и ВПО для распространения рекламы (18%). А самыми популярными путями заражения стали веб-ресурсы (33%) и официальные магазины мобильных приложений (25%).

Любители халявы все чаще становятся жертвами киберпреступников. Так, например, на пиратских сайтах распространялась книга о Дональде Трампе «Огонь и ярость», которая содержала вредоносное ПО, позволяющее злоумышленникам получить доступ к компьютеру жертвы. А русскоязычный торрент-сайт b-tor.ru вместе с легитимными файлами загружал на компьютер жертвы майнер криптовалюты Monero под названием XMRIg.

Поисковые сервисы все чаще становятся площадкой для распространения ссылок на фишинговые ресурсы, в частности из-за возможности размещения рекламы. Так, в марте злоумышленники разместили на сайте google.com ссылку на фишинговую страницу, замаскировав ее под платное объявление, которое якобы принадлежало Amazon. После перехода по ссылке пользователи оказывались на сайте, имитирующем страницу поддержки Apple или Windows, где появлялось всплывающее окно, предупреждающее о том, что компьютер был заражен вредоносным ПО, а личная информация, такая как учетные данные, данные кредитных карт, была похищена. Пользователю рекомендовалось связаться со специалистами, а затем перевести им деньги, чтобы не допустить утечки украденных данных. На самом же деле это оповещение принадлежало вымогателям, которые не получали никакого доступа к данным.

Как защититься организации

Используйте эффективные технические средства защиты:

- средства централизованного управления обновлениями для используемого ПО;
- антивирусы (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;
- специализированные сервисы анти-DDoS.

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 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 (защищенным хранилищем с функциями генерации новых паролей);
- не используйте один и тот же пароль для разных систем (для сайтов, электронной почты и др.);
- меняйте все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.

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 веб-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

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.

