



POSITIVE TECHNOLOGIES

Актуальные киберугрозы

I квартал 2019 года

Содержание

Обозначения	3
Тренды и прогнозы.....	4
Сводная статистика.....	5
Динамика атак.....	8
Методы атак.....	9
Использование вредоносного ПО.....	9
Социальная инженерия.....	11
Хакинг.....	12
Эксплуатация веб-уязвимостей.....	13
Подбор учетных данных.....	14
Категории жертв.....	14
Государственные организации.....	14
Медицинские учреждения.....	17
Промышленные компании.....	18
Финансовые организации.....	20
Онлайн-сервисы.....	22
Как защититься организации.....	24
Как вендору защитить свои продукты.....	26
Как защититься обычному пользователю.....	26
Об исследовании.....	27

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

Категории жертв



Финансовая отрасль



Государственные
учреждения



Медицинские учреждения



Наука и образование



Промышленные компании



Оборонные предприятия



Онлайн-сервисы



Сфера услуг



Транспорт



IT-компании



Торговля



Частные лица



Телекоммуникационные
компании



Блокчейн-проекты



Другие сферы

Тренды и прогнозы

Компания Positive Technologies продолжает следить за актуальными угрозами информационной безопасности. Специалисты во всем мире ведут непрерывную борьбу с киберпреступностью, и это, как и прежде, вынуждает злоумышленников совершенствовать свои инструменты. В начале года кибератаки стали испытанием для многих организаций различных сфер экономики.

Подводя итоги I квартала 2019 года, мы отмечаем следующие тенденции:

- Количество уникальных киберинцидентов продолжило расти и на 11% превысило показатели аналогичного периода в 2018 году.
- Становится больше вредоносного ПО, которое сочетает в себе функции троянов нескольких типов. Гибкая модульная архитектура делает его универсальным. К примеру, зловред может демонстрировать рекламу и одновременно с этим воровать пользовательские данные.
- Продолжает уменьшаться доля скрытого майнинга (7% против 9% в IV квартале 2018 года). Хакеры начали модернизировать майнеры до уровня многофункциональных троянов. Попав в систему с низкими вычислительными ресурсами, где майнинг малоэффективен, такой троян активирует функции шпионского ПО и ворует данные.
- Растет число заражений шифровальщиками (24% против 9% в IV квартале 2018 года). Довольно часто данный тип вредоносного ПО используется в комбинации с фишингом, причем злоумышленники изобретают новые способы обмануть пользователей и побудить их заплатить выкуп.
- Медицинские учреждения — самые распространенные жертвы троянов-шифровальщиков. Возможно, руководство организаций здравоохранения охотнее соглашается заплатить выкуп, нежели другие компании, ведь на кону оказываются жизни и здоровье людей.
- Кибератаки на государство главным образом направлены либо на кражу данных, для чего злоумышленники используют уникальное шпионское ПО собственной разработки, либо на взлом правительственных веб-ресурсов с целью заразить их посетителей вредоносным ПО.
- Вредоносное ПО — главная угроза для крупных промышленных компаний. Атакуя сферу промышленности, злоумышленники чаще всего заинтересованы в коммерческой тайне. В связи с этим нельзя исключать, что атаки шифровальщиков на промышленность направлены на сокрытие следов более ранних инцидентов.
- Многомиллионные утечки учетных записей ставят под угрозу онлайн-сервисы. Злоумышленники охотно используют данные, которые оказались в открытом доступе, для атак типа credentials stuffing.
- Атаки на веб-сайты с внедрением вредоносного JavaScript-кода (JS-снифферов), который ворует данные банковских карт, ставят под угрозу пользователей интернет-магазинов и онлайн-сервисов с функцией оплаты услуг.

Мы прогнозируем, что во II квартале угрозы будут только расти. Вредоносное ПО в сочетании с методами социальной инженерии останется основным оружием киберпреступников.

Не секрет, что криптовалюта востребована в преступном мире. Однако сложность майнинга постоянно растет, и хакеры вынуждены искать альтернативные способы ее добычи. В связи с этим мы считаем, что доля троянов-вымогателей будет высокой, пока есть те, кто готов заплатить выкуп.

Сводная статистика

В I квартале 2019 года рост доли атак, направленных на получение данных, продолжается. Теперь более половины хакерских атак совершаются с целью хищения информации. Злоумышленники заинтересованы в самых разнообразных данных — от личной переписки до коммерческой тайны. Но по-прежнему наиболее высоко ценятся учетные данные, персональные данные и данные платежных карт.

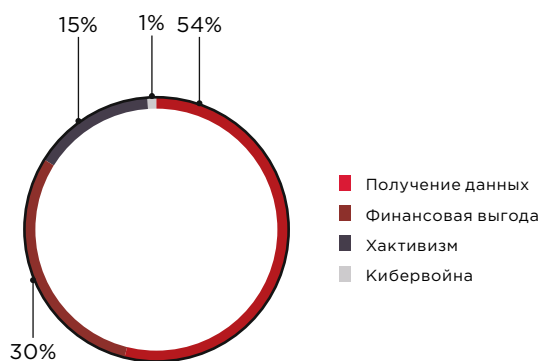


Рисунок 1. Мотивы злоумышленников



Рисунок 2. Типы украденных данных

В I квартале 2019 года доля целенаправленных атак снизилась по сравнению с IV кварталом 2018 года и составила 47% против 62%. Это связано с увеличением доли атак, которые не привязаны к конкретной отрасли; в основном речь идет о массовых вредоносных кампаниях. Доля киберинцидентов, в результате которых пострадали частные лица, практически не изменилась (21% против 22% в IV квартале 2018 года). Среди юридических лиц наиболее часто злоумышленники атакуют государственные организации, медицинские учреждения, промышленные компании, банки и другие организации финансовой сферы. Мы рассмотрим атаки на эти отрасли подробнее. Кроме того, в I квартале 2019 года выросло число атак на онлайн-сервисы. Далее мы попытаемся разобраться в причинах повышенного интереса к ним со стороны злоумышленников.

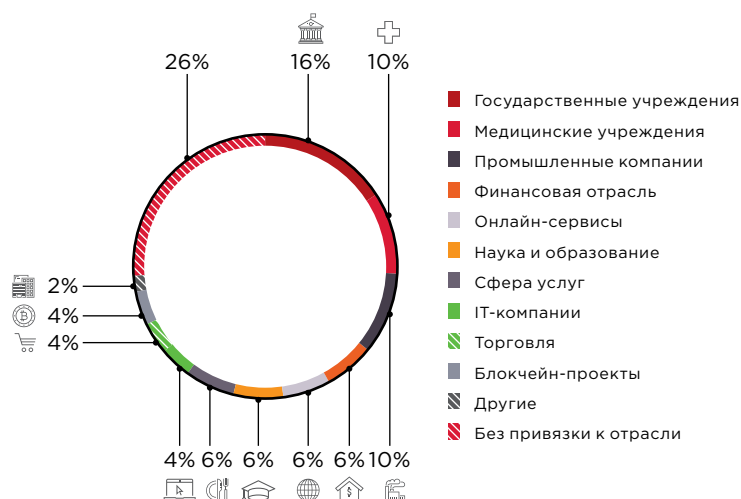


Рисунок 3. Категории жертв среди юридических лиц

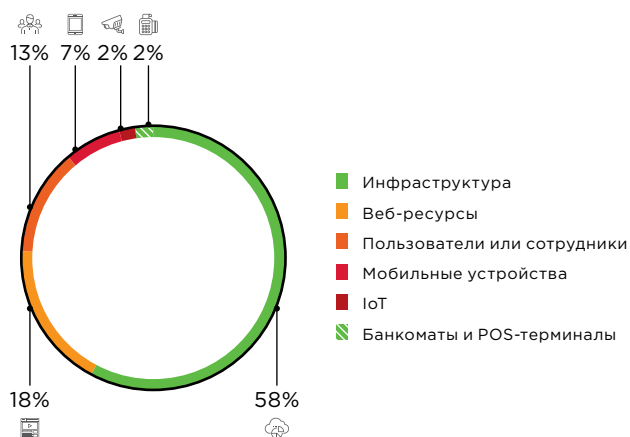


Рисунок 4. Объекты атак

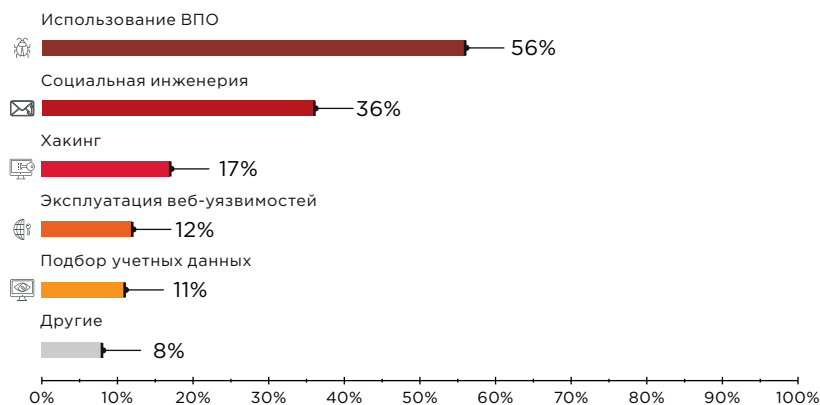


Рисунок 5. Методы атак

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	Наука и образование	Торговля	Частные лица	Блокчейн-проекты	Другие	Без привязки к отрасли
Всего атак		45	17	28	28	16	16	11	17	10	74	10	5	70
Объект	Инфраструктура	29	14	27	17	7	7	10	10	2	17	6	2	53
	Веб-ресурсы	13	2		8	9	3	1	5	5	8	2	3	5
	Пользователи	2	1	1	3		1		2	1	28	2		4
	Мобильные устройства	1									18			4
	Банкоматы и POS-терминалы						5			2				
	IoT										3			4
Метод	Использование ВПО	20	11	22	13	2	10	6	5	5	40	3	1	56
	Социальная инженерия	10	10	20	9			1	4	2	42	3		25
	Подбор учетных данных		1		7	4	3	5	5		5	2	2	5
	Хакинг	7	2	6	2	3	2	2	4		5	5	1	20
	Эксплуатация веб-уязвимостей	13				5	1	2	2	6	3		2	7
	Другие	10	2			4		2	1		4			5
Мотив	Финансовая выгода	8	4	3	9		3	3	5	2	33	4	2	29
	Получение данных	18	10	24	19	9	12	7	8	7	33	6	2	32
	Хактивизм	18	3			7	1	1	4	1	8		1	9
	Кибервойна	1		1										
		<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>												
Градации цвета показана доля атак внутри одной отрасли		0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%		

Динамика атак

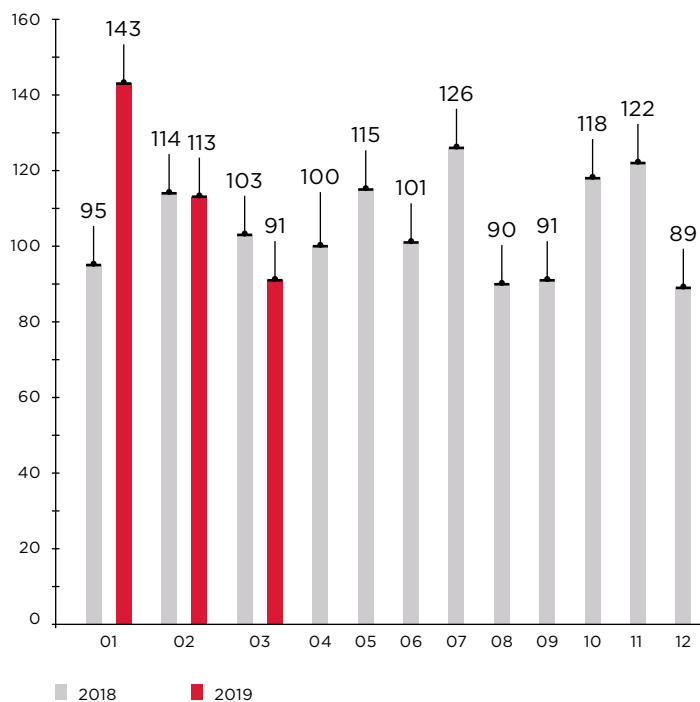


Рисунок 6. Количество инцидентов в 2018 и 2019 годах (по месяцам)

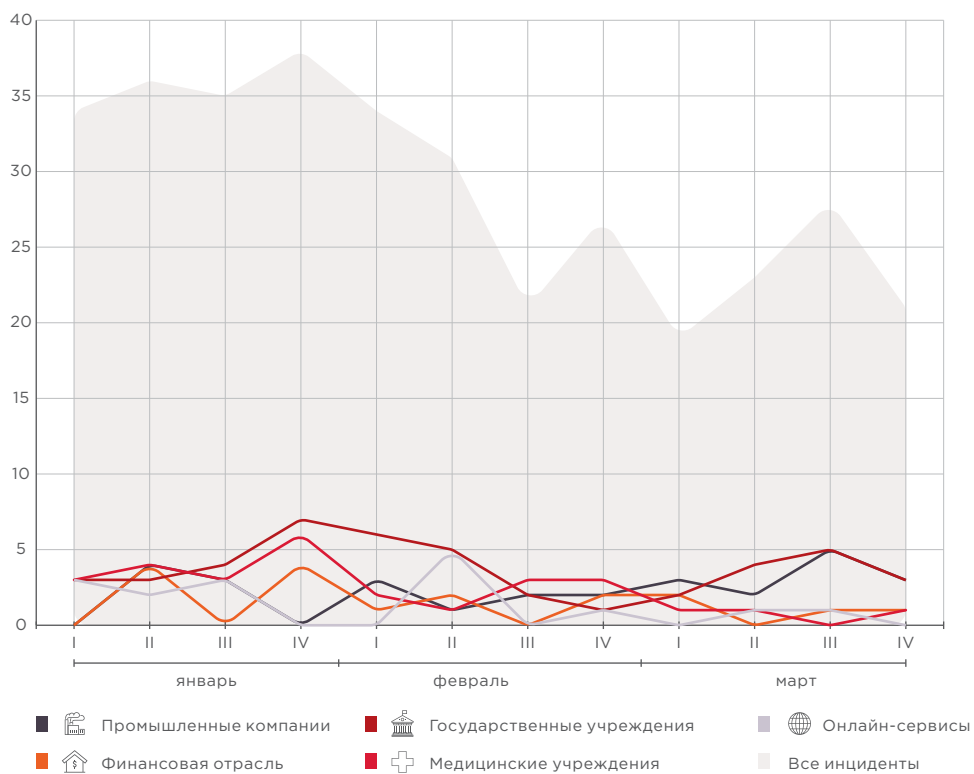


Рисунок 7. Количество инцидентов в I квартале 2019 года (по неделям)

Методы атак

Остановимся подробнее на каждом методе и укажем, какие объекты и отрасли больше других страдали от этих категорий атак.

Использование вредоносного ПО

С начала года мы отмечаем случаи заражений многофункциональными троянами — модульным вредоносным ПО, способным совмещать функции зловредов различных типов. Так, например, троян DanaBot имеет компоненты для удаленного управления, снабжен функциями банковского трояна, а также может похищать пароли от ряда приложений.



Больше всего пострадали

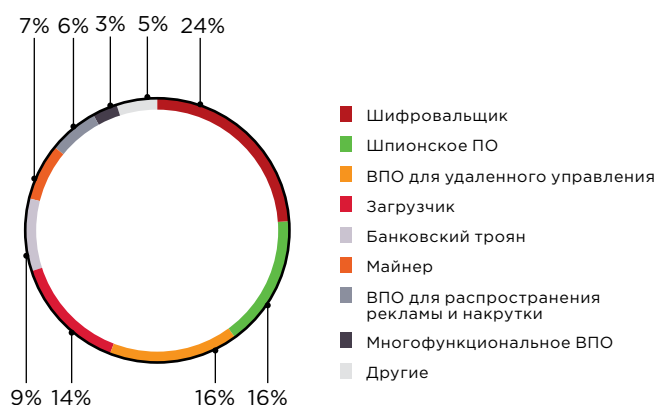
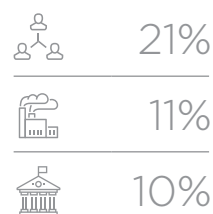


Рисунок 8. Типы ВПО

Фишинговые рассылки по-прежнему остаются эффективным способом доставки вредоносного ПО, однако электронная почта — далеко не единственный канал распространения зловредов. Например, пользователи активно загружают файлы с торрент-трекеров, а значит — риск заражения вредоносами здесь увеличивается в разы. Так, под видом фильма злоумышленники распространяли ПО для подмены адресов биткойн- и Ethereum-кошельков в момент вставки информации из буфера обмена. Другой ресурс, где пользователи активно скачивают программы, — официальные магазины приложений. В числе выявленных зловредов здесь лидируют программы с навязчивой рекламой^{1, 2}. Но встречаются и более опасные вредоносы, например шпионские трояны MobSTSPY и Exodus, банковские трояны Anubis и Gustuff. Последний хакеры приобретают как сервис по подписке (malware as a service) за 800 долл. США в месяц.

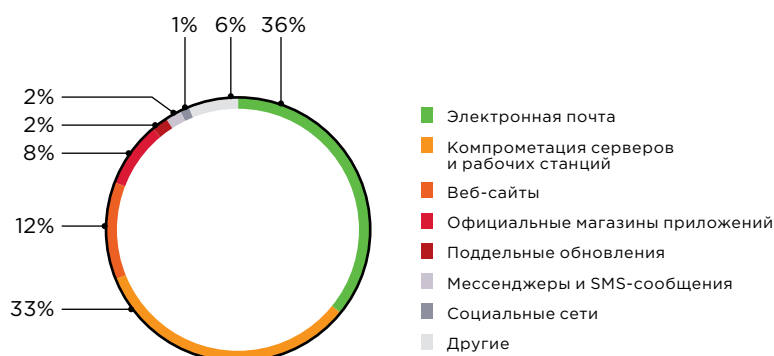


Рисунок 9. Способы распространения ВПО

1 blog.trendmicro.com/trendlabs-security-intelligence/adware-disguised-as-game-tv-remote-control-apps-infect-9-million-google-play-users/

2 research.checkpoint.com/simbad-a-rogue-adware-campaign-on-google-play/

Уровень скрытого майнинга снижается. Год назад, в начале 2018 года, доля майнеров достигала 23%, в IV квартале составляла 9%. В I квартале 2019 года доля криптоджекинга составила лишь 7%. Снижение рентабельности майнинга побуждает киберпреступников модифицировать майнеры, расширяя их возможности до уровня многофункциональных троянов. Например, новый троян CookieMiner не только устанавливает на компьютеры жертв скрытый майнер, но и выполняет роль инфостилера: крадет учетные записи и данные банковских карт.

Атаки с использованием троянов-вымогателей, напротив, снова набирают обороты. По сравнению с последним кварталом 2018 года наблюдается увеличение доли заражений ими с 9% до 24%. В то же время, судя по всему, доходы злоумышленников от «классических» шифровальщиков снижаются. Вероятно, в этом есть заслуга специалистов в области кибербезопасности, которые активно призывают пользователей не платить выкуп за восстановление файлов. Как бы то ни было, злоумышленники ищут новые хитроумные способы воздействия на своих жертв. Например, CryptoMix обещает жертвам направить выкуп на благотворительность в пользу больных детей. Еще одна вредоносная атака затронула пользователей, которые по тем или иным причинам не готовы заплатить выкуп в криптовалюте. Новый вариант шифровальщика предлагает способ оплаты якобы через сервис PayPal. Если пользователь решает воспользоваться этим способом, он перенаправляется на поддельную форму оплаты. Все введенные на фишинговой странице учетные данные и платежная информация попадают в руки злоумышленников, которые затем выводят деньги со счетов жертв или могут продать украденные данные в дарквебе.

В I квартале эксперты PT ESC зафиксировали массовую фишинговую рассылку якобы от лица крупных российских компаний. В качестве приложения к письму использовались либо ZIP-архив со сценарием на языке JavaScript, либо PDF-файл со встроенной ссылкой. В обоих вариантах на компьютер жертв загружался шифровальщик Shade (известен с 2014 года, прежнее название — Trolldesh). Вредоносное ПО удаляет теньные копии, шифрует файлы и добавляет к ним расширение .crypted000007, после чего файлы не поддаются восстановлению. Примечательно, что электронные письма отправлялись со взломанных IoT-устройств, в частности с роутеров.

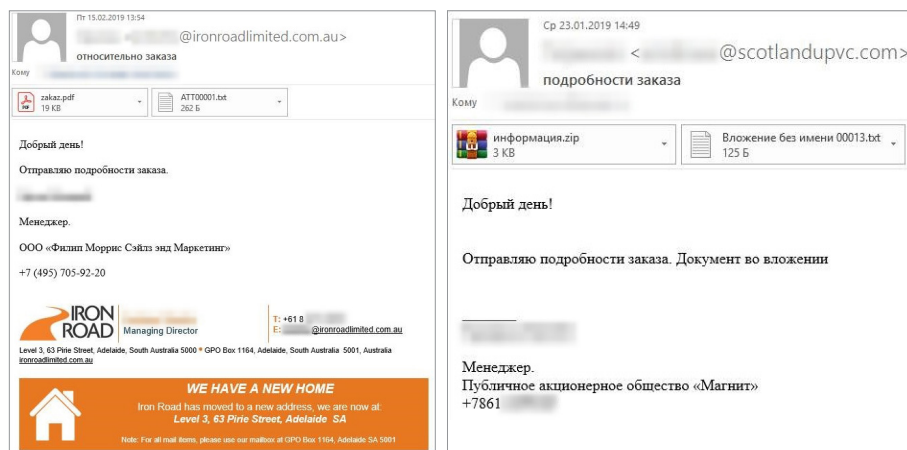


Рисунок 10. Примеры фишинговых писем, распространяющих шифровальщик Shade

Социальная инженерия

Активное использование социальной инженерии для распространения вредоносного ПО продолжается. В марте специалисты PT ESC зафиксировали массовую рассылку писем с текстовым документом на тему предстоящих выборов президента Украины. Документ содержал макрос, который раскодировал скрытый в метаданных скрипт PowerShell Empire, предназначенный для скачивания вредоносного ПО на компьютер жертвы.

Помимо политических событий, другим инфоповодом для фишинговых рассылок часто становятся отраслевые конференции. Так, обнаруженный нашими экспертами документ — приглашение на научную конференцию — содержал эксплойт для уязвимости [CVE-2018-0802](#) и ВПО для удаленного управления.



Больше всего
пострадали

 33%

 16%

 8%



Рисунок 11. Приглашение на конференцию, содержащее вредоносный код

Еще одна популярная тема для фишинговых рассылок — просьба подтвердить учетную запись. Присылая подобные письма владельцам популярных аккаунтов в Instagram, злоумышленники вынуждали жертв вводить персональные и учетные данные в поддельные формы, в результате чего вся информация попадала в руки киберпреступников. Другой пример — февральская фишинговая рассылка клиентам банка TD Bank якобы с просьбой подтвердить статус аккаунта. В качестве нагрузки в письме доставлялся банковский троян TrickBot. В обоих случаях электронные адреса, с которых приходили вредоносные сообщения о необходимости подтвердить статус, были очень похожи на оригинальные адреса компаний.

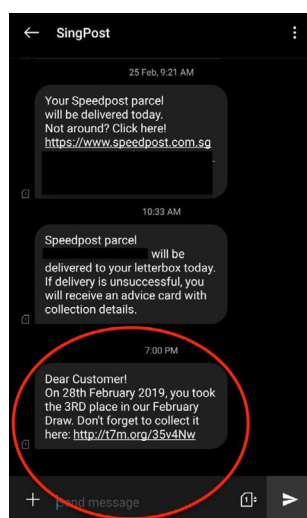


Рисунок 12. Поддельное SMS-сообщение с вредоносной ссылкой

Опытные интернет-пользователи знают, что одна или несколько перепутанных букв в адресе говорят об опасности и вероятной фишинговой атаке. Но что, если в имени отправителя указан верный домен? Абсолютно ли безопасно открывать вложения из таких писем? Как показывает практика, нет. Хакеры часто используют взломанные ресурсы или уязвимости в почтовых сервисах для вредоносных рассылок от имени компании-жертвы (так называемые brand impersonation attacks). Например, используя небезопасную конфигурацию сервера SMTP, хакеры распространяли вредоносное ПО от имени компании DHL. Адрес, с которого приходили письма, имел вид support@dhl.com, что несомненно повышало доверие жертв — получателей писем.

SingPost — еще один логистический оператор, имя которого было задействовано в хитроумной фишинговой атаке. Злоумышленникам удалось разослать вредоносную ссылку на телефоны пользователей якобы от SingPost. Поддельное SMS-сообщение попадало в цепочку легитимных сообщений, которые компания ранее присылала своим клиентам, что несомненно снижало бдительность пользователей, как и в случае с DHL.

Хакинг

Известные уязвимости и уязвимости нулевого дня в программном обеспечении активно эксплуатируются злоумышленниками в различных целях. Например, готовые эксплойты часто используют для доставки на оборудование скрытых майнеров. В I квартале 2019 года для установки майнеров хакеры использовали, к примеру, бреши в защите кластеров с устаревшими версиями Elasticsearch (CVE-2014-3120, CVE-2015-1427), эксплуатировали уязвимости CVE-2019-6340 в CMS Drupal и CVE-2019-5736 в контейнерах Docker. Еще одна цель, которую преследуют злоумышленники, — повышение привилегий в системе, ведь права администратора дают простор действиям хакеров. Например, уязвимость нулевого дня в плагине Easy WP SMTP для CMS WordPress позволяет злоумышленникам создавать административные аккаунты, менять параметры SMTP-сервера и перенаправлять трафик. Брешь может использоваться для организации фишинговых атак от лица компании-жертвы, чей сайт оказался взломан. Пример такой атаки мы рассмотрели выше, когда говорили о социальной инженерии. Еще в одном сценарии атак для повышения привилегий злоумышленники эксплуатировали сразу две уязвимости нулевого дня — в браузере Google Chrome и в Windows 7. Специалисты компании Google выявили эти атаки в конце февраля.

В феврале также стало известно, что эксперты в области кибербезопасности обнаружили уязвимости в WinRAR, которые на тот момент присутствовали в программе уже около 19 лет. Бреши открывают злоумышленникам новые возможности для заражения жертв вредоносным ПО. Спустя меньше месяца после известия о проблеме в WinRAR специалисты насчитали порядка сотни эксплойтов для выявленных уязвимостей. Причина такого интереса со стороны хакеров кроется в повсеместном использовании архиватора, начиная с обычных

17%

Больше всего пострадали

12%



10%



8%



пользователей и заканчивая крупными компаниями. По оценке экспертов, найденная брешь угрожает 500 млн пользователей. Разработчики уже устранили проблемы и выпустили новую версию ПО, но угроза по-прежнему актуальна из-за отсутствия в WinRAR механизма автоматического обновления.

Эксплуатация веб-уязвимостей

Начало года ознаменовалось массовыми атаками группировки MageCart, которая известна так называемыми веб-скиммерами — наборами скриптов для кражи данных платежных карт с веб-сайтов. Мы уже рассказывали об этих атаках в нашем [отчете](#) за IV квартал прошлого года. В январе 2019 года специалисты [зафиксировали](#) новую волну атак MageCart. Заражены оказались сразу 277 сайтов электронной коммерции. Такого масштаба злоумышленники достигли за счет метода supply chain attack: они компрометируют одну компанию с целью атак на другую. Так, хакеры из MageCart внедрили вредоносный код в JavaScript-библиотеку, которую использовало рекламное агентство Adverline. В результате сайты всех компаний-клиентов, которые размещали на своих сайтах рекламу через это агентство, оказались заражены. Аналогичную атаку, только более крупного масштаба, зафиксировали специалисты The Media Trust. Им удалось [установить](#), что скомпрометированы несколько десятков вендоров рекламы, в результате чего в зоне риска оказались 49 сайтов с высокой посещаемостью.

Однако кража данных — не единственная цель, которую преследуют злоумышленники, взламывая сайты. Атака на сайт — один из эффективных способов привлечь внимание к той или иной проблеме. Например, веб-ресурсы правительственных учреждений часто подвергаются атакам из-за значимых событий, вызвавших общественный резонанс. Так, после террористического акта в Пулваме 14 февраля 2019 года хакеры [взломали](#) сотни государственных веб-ресурсов Пакистана.

Еще одним поводом для привлечения общественного внимания могут стать обнаруженные проблемы в безопасности. Сайт компании Luas был [взломан](#) злоумышленниками из-за того, что владельцы веб-ресурса долгое время молчали в ответ на сообщения анонимного хакера о наличии брешей в системе защиты. Вероятно, игнорирование проблемы со стороны разработчиков стало поводом и для XSS-атаки на пользователей популярной российской соцсети «ВКонтакте» в феврале 2019 года.

Атаки XSS угрожают также пользователям сайтов под управлением WordPress. Уязвимость в плагине Abandoned Cart позволяет злоумышленникам создавать [бэкдор](#) — аккаунт с правами администратора. По данным экспертов, выявленная брешь была проэксплуатирована злоумышленниками не менее пяти тысяч раз. Еще одна [уязвимость](#), на этот раз в плагине Social Warfare, позволяет перенаправлять пользователей на сайты, подконтрольные злоумышленникам. К слову, согласно нашему [исследованию](#), XSS-атаки по-прежнему остаются распространенным риском для пользователей веб-приложений.



12%

Больше всего
пострадали



31%



14%



12%



Больше всего
пострадали



Подбор учетных данных

Один из источников дохода хакеров — это продажа учетных данных в дарквебе. Чем больше логинов и паролей удастся похитить киберпреступнику, тем выше его доход, поэтому атаки с подбором паролей нередко носят массовый характер. Специалисты отмечают рост числа атак, направленных на подбор учетных данных в облачных сервисах Office 365 и G Suite. Злоумышленники используют уязвимости в старых версиях протокола IMAP, которые позволяют им существенно повысить скорость перебора паролей.

Признаки подбора учетных данных есть и среди следов атаки на компанию Citrix. В результате киберинцидента были похищены документы, содержащие коммерческую тайну. Эксперты склоняются к версии, что злоумышленники использовали технику password spraying. Она предполагает опробование одного или нескольких паролей для целого списка логинов. При таком подходе, в отличие от перебора паролей, удастся избежать блокировки учетных записей из-за многократных попыток аутентификации.



В марте 2019 года консорциум W3C и FIDO Alliance официально признали стандарт беспарольной аутентификации WebAuthn. Ожидается, что с переходом на новую технологию перебор паролей и password spraying потеряют свою актуальность. Однако внедрение нового стандарта потребует времени

Категории жертв

Государственные организации

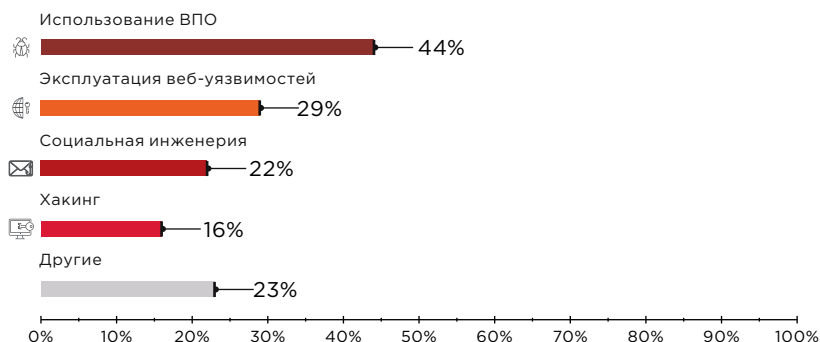


Рисунок 13. Методы атак на государственные организации в Q1 2019

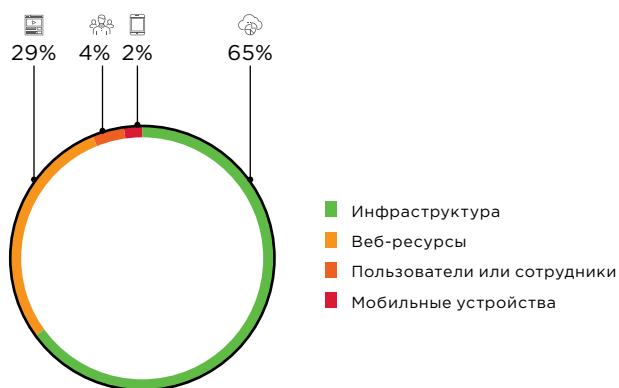


Рисунок 14. Объекты атак

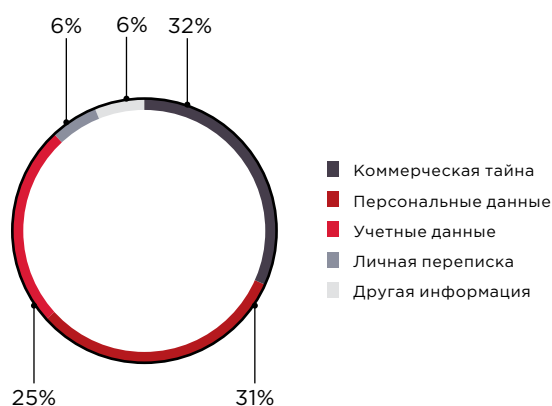


Рисунок 15. Украденные данные

Начало года выдалось неспокойным для правительственных организаций многих стран. Начавшаяся в конце прошлого года сложная, но хорошо спланированная кампания по кибершпионажу [DNSpionage](#) получила развитие в январе и феврале 2019 года. Действия киберпреступников были направлены на кражу учетных данных электронной почты и других правительственных ресурсов. Атака представляет собой классический вариант *supply chain attack*. Преступной группировке удалось скомпрометировать учетные записи двух крупных DNS-провайдеров. Но их конечной целью были не они, а государственные организации на Ближнем Востоке. Получив доступ к серверам провайдеров, хакеры использовали атаку *DNS hijacking*, суть которой заключается в модификации записей DNS, чтобы весь трафик почты и виртуальных частных сетей перенаправлялся на подконтрольный злоумышленникам сервер. Кампания имела столь серьезный масштаб, что Министерство внутренней безопасности США было вынуждено в срочном порядке выпустить [предписание](#) о мерах безопасности для всех федеральных агентств.

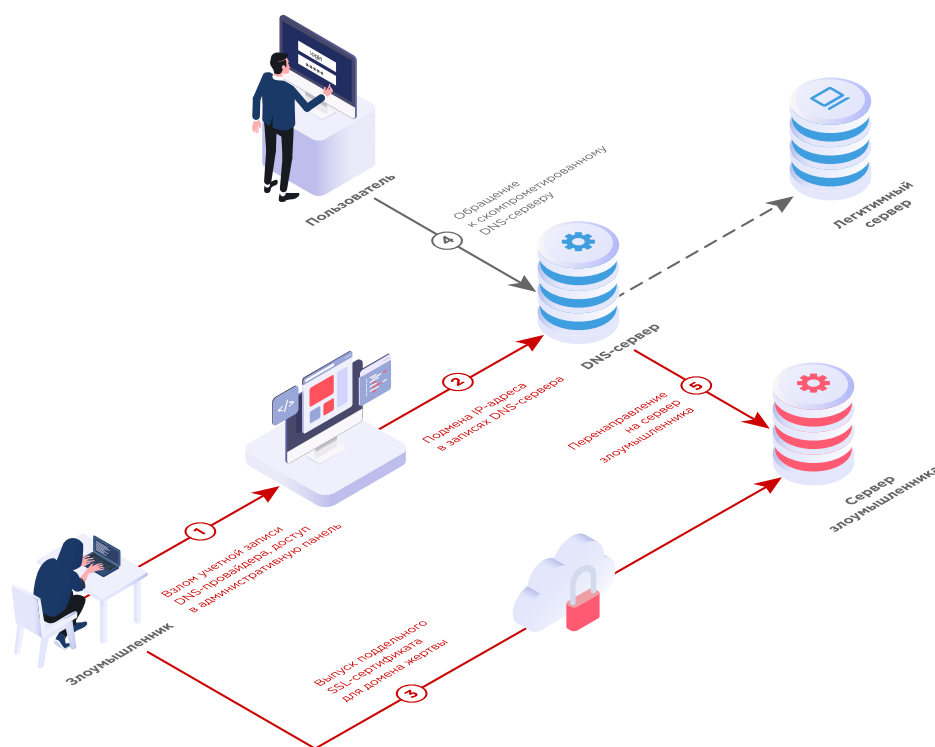


Рисунок 16. Схема атаки DNS hijacking

Другим громким событием начала января стало известие о возобновлении активности АРТ-группировки DarkHydrus. Хакеры атакуют государственные учреждения, преимущественно на Ближнем Востоке, и распространяют обновленный вариант трояна RogueRobin (собственная разработка группировки). В новой версии ВПО добавлен альтернативный канал связи с командным сервером: теперь для управления используется API «Google Диска».

Как и раньше, злоумышленники продолжают взламывать веб-ресурсы государственных организаций и размещать на них вредоносное ПО, зная, что взломанные веб-сайты имеют высокую посещаемость. Так, на сайте посольства Бангладеш в Каире злоумышленники разместили ссылки на вредоносные документы в формате Word, доставляющие загрузчик Godzilla.

Заражению вредоносным ПО подвергся и правительственный сайт Пакистана. На этот раз жертвой стал онлайн-ресурс, на котором пользователи могли оставить заявку на получение гражданства или проверить ее статус. Шпионское ПО — JavaScript-фреймворк Scanbox — собирало все введенные на сайте данные пользователей и перенаправляло их киберпреступникам.

В I квартале 2019 года мы отмечаем большое число атак на государственные учреждения с использованием шифровальщиков. В большинстве случаев файлы удастся восстановить из резервных копий, однако правительство округа Джексон в американском штате Джорджия все же приняло решение заплатить выкуп в размере 400 тысяч долл. США, чтобы восстановить ИТ-инфраструктуру.

Медицинские учреждения

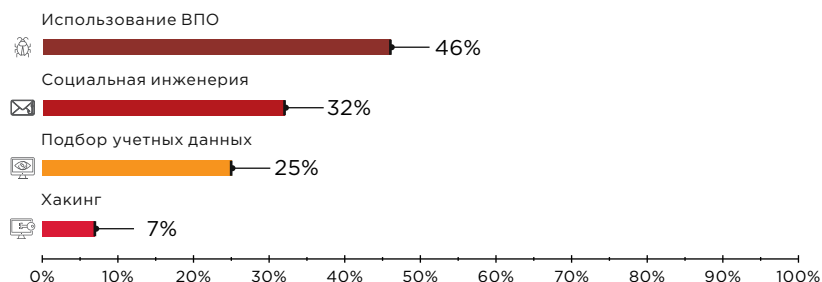


Рисунок 17. Методы атак на медицинские учреждения в Q1 2019

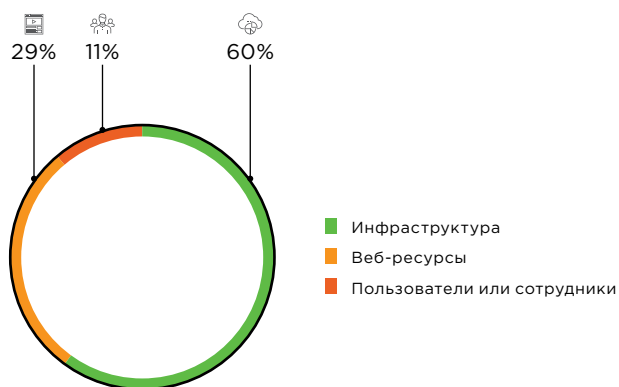


Рисунок 18. Объекты атак

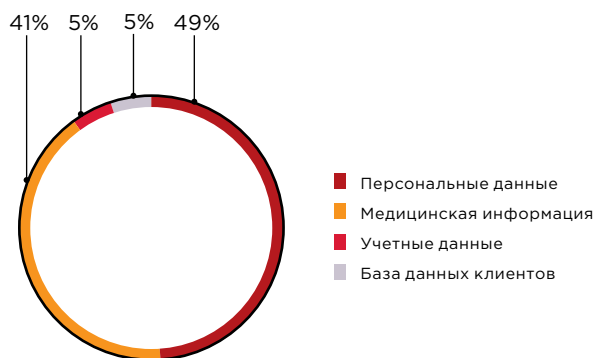


Рисунок 19. Украденные данные

Основными методами атак на медицинские учреждения по-прежнему остаются заражение вредоносным ПО и взлом учетных записей сотрудников. Так, электронная почта сотрудников центра Verity Medical Foundation подвергалась взлому три раза в течение нескольких месяцев.

Сфера здравоохранения, пожалуй, чаще других страдает от атак шифровальщиков. С одной стороны, не секрет, что зачастую в медицинских организациях наблюдается дефицит бюджета на информационную безопасность, а значит — система защиты может оказаться ненадежной, что делает медицинские учреждения легкой добычей для хакеров.

С другой стороны, здравоохранительные организации хранят и обрабатывают большое количество персональных данных, в том числе диагнозы пациентов. За утрату такой базы данных компаниям грозят внушительные штрафы, поэтому владельцы медицинских центров охотнее платят выкуп, чем компании из других отраслей. Так, администрация центра Columbia Surgical Specialists предпочла не рисковать данными пациентов и заплатила выкуп за восстановление файлов в размере 15 тыс. долл. США.

Промышленные компании

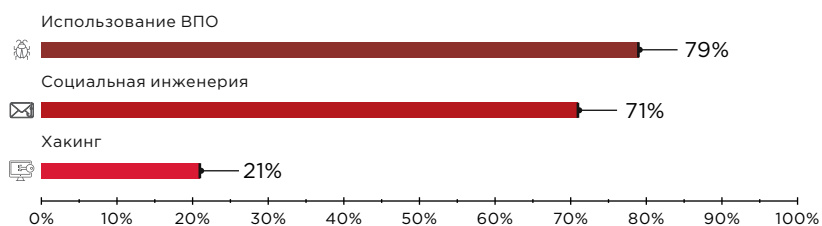


Рисунок 20. Методы атак на промышленные компании в Q1 2019

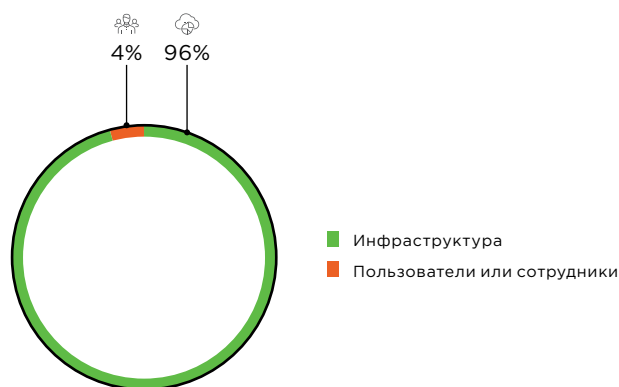


Рисунок 21. Объекты атак

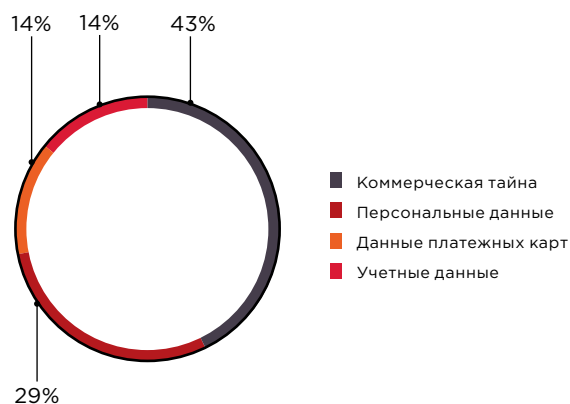


Рисунок 22. Украденные данные

С начала года эксперты РТ ESC регулярно фиксируют вредоносные фишинговые рассылки от вымышленных отправителей в адрес компаний нефтегазовой отрасли и других производственных организаций. Кампанию проводит группировка RTM, ее главная цель — кража денежных средств со счетов жертв. В феврале группировка перенесла свою инфраструктуру в сеть Tor. Ранее ее инфраструктура находилась внутри блокчейн-сети, и троян при запросе домена через блокчейн получал IP-адрес контрольного сервера.



Рисунок 23. Фишинговые письма группировки RTM

Операторы нового шифровальщика LockerGoga нацелены на крупные инжиниринговые и промышленные компании. Громким событием января стало заражение французской компании Altran Technologies. А уже в марте стало известно об атаке на норвежскую металлургическую компанию Norsk Hydro, вызвавшей остановку производства. Как выяснилось позже, есть еще жертвы: от действий шифровальщика пострадали две американские компании химической отрасли. Специалисты по безопасности активно изучают нашумевший вредонос и уже сумели найти ошибку в его коде, которая позволяет выстроить защиту. Однако рано говорить о победе: зловард развивается очень быстро, на данный момент известно о 31 его разновидности.

Финансовые организации

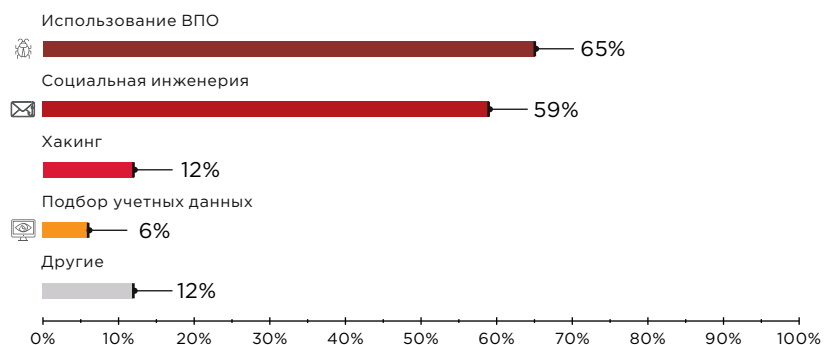


Рисунок 24. Методы атак на финансовые организации в Q1 2019



Рисунок 25. Объекты атак



Рисунок 26. Украденные данные

Группировка Silence продолжает атаковать банки. Первую в этом году массовую фишинговую рассылку специалисты PT ESC зафиксировали 16 января. Письма содержали якобы приглашения на профильную конференцию iFin-2019.

Тема: Форум iFin-2019
 Прикрепленные файлы: Письмо.html, Priglasenie.zip

Форум iFin-2019 – это центральное мероприятие в России, посвященное электронным финансам, которое проводится с 2001 года. На Форуме можно будет ознакомиться с самыми современными достижениями в области ДБО, интернет- и мобильного банкинга, финансовых маркетплейсов и экосистем, узнать о применении в дистанционном обслуживании инновационных технологий, включая демонстрации искусственного интеллекта в банковской сфере, биометрии, вычислений в оперативной памяти, облачных технологий, открытых API, новых средств информационной безопасности и многое другое. В деловой программе Форума – всестороннее обсуждение новейших технологий и практических примеров их использования, представленных ведущими банками и разработчиками.

Участие двух представителей от кредитных организаций – бесплатное (при условии предварительной регистрации). Поспешите зарегистрироваться. Заполните анкету в приложенном архиве и перешлите нам. Вы получите два бесплатных пригласительных и название Вашего банка будет размещено на официальном портале форума.

Рисунок 27. Фишинговое письмо группировки Silence с приглашением на конференцию

Помимо приглашений на конференцию группировка продолжила рассылку писем с заголовками, относящимися к рабочим вопросам, например сообщений об открытии корреспондентского счета. Подобные темы для рассылок мы отмечали и в октябре-декабре прошлого года, рассказывая о киберинцидентах IV квартала. В качестве полезной нагрузки вредоносный архив, прикрепленный к письму, содержал загрузчик, подписанный корректным сертификатом. Примечательно, что данный сертификат использовался также группировкой Cobalt.

Name	SEVA MEDICAL LTD
Status	Valid
Valid From	12:00 AM 12/13/2018
Valid To	11:59 PM 12/13/2019
Valid Usage	Code Signing
Algorithm	sha256RSA
Serial Number	75 52 22 15 40 63 35 72 56 87 AF 88 8D CD C8 0C

Рисунок 28. Сертификат для подписи вредоносного ПО

Группировка Cobalt не сдает позиции: ее атаки на финансовый сектор продолжают. В I квартале 2019 года злоумышленники используют ту же технику, что и в конце прошлого года. Как и прежде, полезная нагрузка в виде обфусцированного JavaScript-бэкдора доставляется внутри COM-DLL-Dropper.

В феврале специалисты PT ESC зафиксировали атаку с использованием Metasploit в связке с COM-DLL-Dropper. С контрольного сервера в память зараженного компьютера загружается Metasploit stager, который, в свою очередь, дает злоумышленникам удаленный доступ к компьютерам жертв, а также загружает необходимые модули Metasploit. Схожую атаку проводила в октябре и декабре прошлого года неизвестная группировка, о которой мы уже писали.

Кибератака на банк может закончиться простоем инфраструктуры, один день которого исчисляется десятками, а иногда и сотнями тысяч долл. США. В феврале мальтийский банк Bank of Valletta был вынужден прекратить свои операции в связи с кибератакой. Хакеры пытались похитить 13 млн евро, но атаку удалось вовремя локализовать и остановить.

Онлайн-сервисы

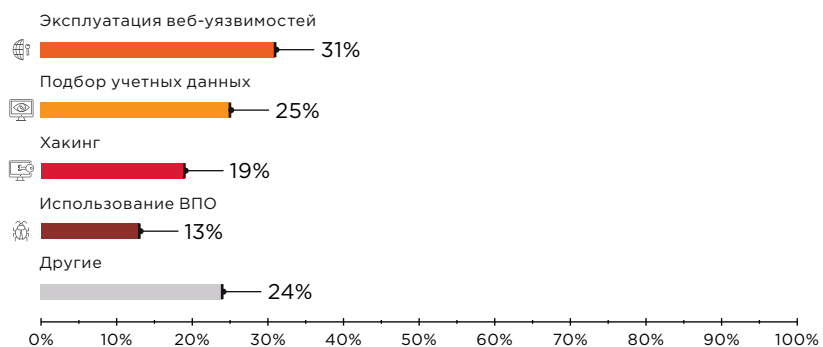


Рисунок 29. Методы атак на онлайн-сервисы в Q1 2019

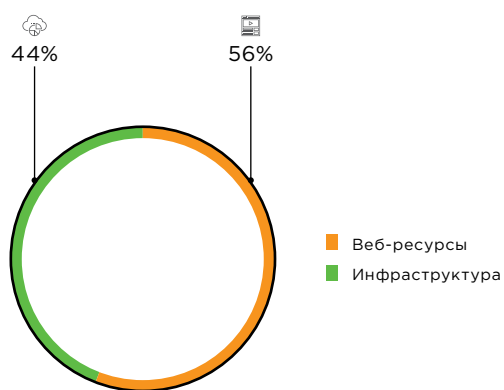


Рисунок 30. Объекты атак

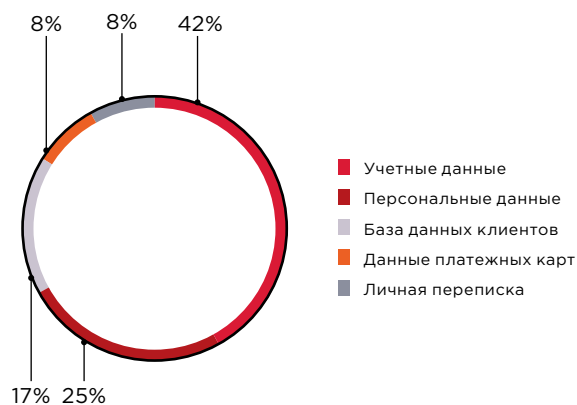


Рисунок 31. Украденные данные

Активные пользователи интернета ежедневно имеют дело с различными онлайн-сервисами: общаются в соцсетях, играют в игры, смотрят фильмы, покупают билеты, бронируют номера. Но эти сервисы привлекают внимание не только обычных пользователей, но и хакеров, ведь они содержат огромное количество пользовательских данных, в том числе персональных, которые можно выгодно продать.

Атаки типа *credentials stuffing*, когда злоумышленник пытается аутентифицироваться в системе с учетными данными пользователей других систем, на сегодняшний день являются одним из популярных методов взлома онлайн-сервисов. В январе администраторы Reddit заявили о попытках несанкционированного доступа к аккаунтам пользователей, в результате которых им пришлось сбросить пароли. Как говорят сами владельцы сервиса, злоумышленники, вероятно, пытались воспользоваться паролями из массовых утечек. Атаке *credentials stuffing* подвергся и видеохостинг DailyMotion. Возникает вопрос: где хакеры берут базы данных учетных записей для проведения таких атак? Например, в дарквебе. Так, на теневой площадке Dream Market были выставлены на продажу данные 620 млн пользователей 16 крупных сайтов, включая популярные онлайн-сервисы.

Однако не всегда целью злоумышленников становится кража информации. Почтовый сервис VEmail был полностью уничтожен в результате хакерской атаки в феврале 2019 года. Злоумышленники отформатировали диски на всех серверах, в результате чего оказались потеряны даже резервные копии. Вероятно, подобные действия связаны с высокой конкуренцией и активной борьбой за пользователей.

Как защититься организации

Используйте эффективные технические средства защиты

- Системы централизованного управления обновлениями и патчами для используемого ПО. Для правильной приоритизации планов по обновлениям необходимо учитывать сведения об актуальных угрозах безопасности.
- Системы антивирусной защиты со встроенной изолированной средой («песочницей») для динамической проверки файлов, способные выявлять и блокировать вредоносные файлы в корпоративной электронной почте до момента их открытия сотрудниками и другие вирусные угрозы. Наиболее эффективным будет использование антивирусного ПО, построенного на решениях одновременно нескольких производителей, способного обнаруживать скрытое присутствие вредоносных программ и позволяющего выявлять и блокировать вредоносную активность в различных потоках данных — в почтовом, сетевом и веб-трафике, в файловых хранилищах, на веб-порталах. Важно, чтобы выбранное решение позволяло проверять файлы не только в реальном времени, но и автоматически анализировало уже проверенные ранее, это позволит выявить не обнаруженные ранее угрозы при обновлении баз сигнатур.
- SIEM-решения — для своевременного выявления и эффективного реагирования на инциденты информационной безопасности. Это позволит своевременно выявлять злонамеренную активность, попытки взлома инфраструктуры, присутствие злоумышленника и принимать оперативные меры по нейтрализации угроз.
- Автоматизированные средства анализа защищенности и выявления уязвимостей в ПО.
- Межсетевые экраны уровня приложений (web application firewall) — в качестве превентивной меры защиты веб-ресурсов.
- Системы глубокого анализа сетевого трафика — для обнаружения сложных целевых атак как в реальном времени, так и в сохраненных копиях трафика. Применение такого решения позволит не только увидеть не обнаруженные ранее факты взлома, но и в режиме реального времени отслеживать сетевые атаки, в том числе запуск вредоносного ПО и хакерских инструментов, эксплуатацию уязвимостей ПО и атаки на контроллер домена. Такой подход позволит существенно снизить время скрытного присутствия нарушителя в инфраструктуре, и тем самым минимизировать риски утечки важных данных и нарушения работы бизнес-систем, снизить возможные финансовые потери от присутствия злоумышленников.
- Специализированные сервисы анти-DDoS.

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.

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.

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 инвентаризацию ресурсов, доступных для подключения из интернета; анализируйте защищенность таких ресурсов и устраняйте уязвимости в используемом ПО; хорошей практикой является постоянный мониторинг публикаций о новых уязвимостях: это позволяет оперативно выявлять такие уязвимости в ресурсах компании и своевременно их устранять;
- эффективно фильтруйте трафик для минимизации доступных внешнему злоумышленнику интерфейсов сетевых служб; особое внимание стоит уделять интерфейсам удаленного управления серверами и сетевым оборудованием;
- 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).

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 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.

Об исследовании

Данный отчет содержит информацию об актуальных угрозах информационной безопасности, основанную на собственной экспертизе компании Positive Technologies, результатах многочисленных расследований, а также на данных авторитетных источников.

В рамках аналитического исследования массовые инциденты (например, вирусные атаки, в ходе которых злоумышленники проводят многоадресные фишинговые рассылки) рассматриваются как одна уникальная угроза информационной безопасности. Каждое событие характеризуется следующими признаками:

- **Объект атаки** — объект деструктивного воздействия со стороны киберпреступников. Например, в случае атаки на сетевое оборудование, серверы или рабочие станции пользователей объектом является инфраструктура.
- **Мотив атаки** — первостепенная цель киберпреступников. Например, если в результате атаки похищены данные платежных карт, мотивом в этом случае является получение данных.
- **Методы атаки** — совокупность приемов, которые использовались для достижения цели. Например, злоумышленник может провести разведку, выявить доступные для подключения уязвимые сетевые службы, проэксплуатировать уязвимости и получить доступ к ресурсам или информацию; такой процесс мы называем хакингом. При этом подбор учетных данных и использование уязвимостей веб-приложений мы выделили в отдельные категории для большей детализации.
- **Категория жертв** — сфера деятельности атакованной организации (или частные лица, если в результате атаки пострадали люди независимо от места их работы). Так, к сфере услуг мы относим организации, которые предоставляют услуги на коммерческой основе (например, консалтинговые организации или гостиницы, рестораны). Категория «онлайн-сервисы» включает интернет-площадки, позволяющие пользователям решать их задачи онлайн (например, сайты-агрегаторы для покупки билетов, бронирования номеров в гостиницах, блоги, соцсети, мессенджеры и иные социальные медиаресурсы, видеохостинги, онлайн-игры). Масштабные кибератаки, преимущественно вредоносные эпидемии, которые не ограничиваются воздействием на какую-то одну отрасль, мы отнесли к категории «Без привязки к отрасли».

По нашей оценке, большинство кибератак не передается огласке из-за репутационных рисков, в связи с этим оценить точное число угроз не представляется возможным даже организациям, занимающимся расследованием инцидентов и анализом действий хакерских групп. Данное исследование проводится с целью обратить внимание организаций и граждан, интересующихся современным состоянием информационной безопасности, на наиболее актуальные мотивы и методы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз.

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.