



POSITIVE TECHNOLOGIES

Актуальные киберугрозы

IV 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	11
Эксплуатация веб-уязвимостей	11
Подбор учетных данных	12
DDoS	13
Категории жертв	14
Государственные организации	14
Медицинские учреждения	16
Финансовая отрасль	17
IT-компании	20
Частные лица	21
Как защититься организации	22
Как вендору защитить свои продукты	23
Как защититься обычному пользователю	24



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 исследований, а также данных авторитетных источников.

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

- Количество уникальных киберинцидентов на 11% превысило показатели аналогичного периода в 2017 году и на 7% — показатели III квартала 2018 года.
- Как и в предыдущие периоды, почти в каждой третьей утечке фигурируют персональные данные пользователей. Вполне вероятно, что этот показатель будет расти в 2019 году. По мнению наших экспертов, это может быть связано с General Data Protection Regulation (GDPR)¹ — законом, устанавливающим правила защиты персональных данных граждан ЕС. Компании, которые ранее умалчивали об инцидентах, после известий о первых штрафах и предупреждениях (например, в размере 20 млн евро²) станут, вероятно, охотнее уведомлять клиентов о кибератаках.
- Злоумышленники активно встраивают вредоносные скрипты в код уязвимых веб-ресурсов для кражи данных банковских карт со страниц оплаты. Наибольшую угрозу такие атаки несут государственным сайтам, принимающим оплату за муниципальные услуги, поскольку они наименее защищены.
- Слабость защиты сетевого периметра компаний была продемонстрирована в ходе довольно простой атаки на подбор учетных данных для подключения к удаленному компьютеру по протоколу RDP. Интересно, что жертвами хакера стали сразу десятки организаций из разных отраслей экономики. Это позволяет сделать вывод, что сегодня существует общая проблема недостаточно серьезного внимания компаний к администрированию и контролю защищенности сетевого периметра.
- Публикация статей исследователей ИБ, раскрывающих подробности уязвимостей нулевого дня, является проблемой современного киберпространства. Несмотря на то, что данные становятся публичными только после выпуска обновлений, закрывающих описанные уязвимости, пользователи не успевают их установить, а злоумышленники уже атакуют, используя опубликованные данные и даже готовые эксплойты.

¹ ec.europa.eu/info/law/law-topic/data-protection_en

² theinquirer.net/inquirer/news/3063193/ico-slaps-aggregateiq-with-first-official-gdpr-notice



Сводная статистика

В IV квартале 2018 года 48% атак были направлены на получение данных. Интересно, что в ходе половины из них злоумышленники использовали вредоносное ПО. Доля инцидентов, принесших преступникам финансовую выгоду, выросла на 6% по сравнению с прошлым кварталом. Если сравнивать с показателями 2017 года, то мы видим, что кража информации стала встречаться чаще, чем непосредственное получение денежных средств. К сожалению, многие люди больше заботятся о сохранности финансов, забывая о том, что персональные и учетные данные, данные банковских карт, медицинская информация, оказавшиеся в руках злоумышленников, могут в дальнейшем привести и к финансовым потерям.

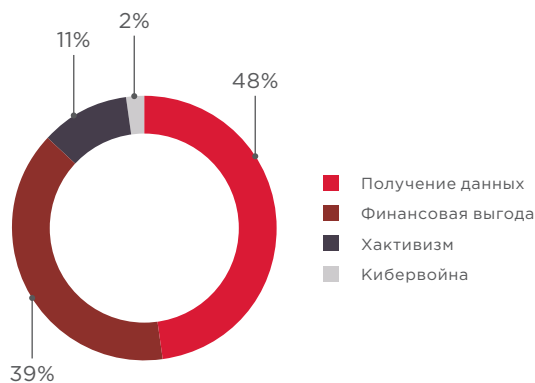


Рисунок 1. Мотивы злоумышленников

В IV квартале 2018 года злоумышленников в первую очередь (28% атак) интересовали учетные данные (логины, пароли) для доступа к различным сервисам и системам, в том числе к электронной почте сотрудников компаний. Примечательно, что для получения учетных данных злоумышленникам в большинстве случаев не приходится применять специализированное ПО, поскольку люди продолжают использовать даты своего рождения, клички собак и т. п. в качестве парольной информации. В 27% случаев были украдены персональные данные, а в 16% — данные платежных карт. Под конец года злоумышленники стали все чаще внедрять на сайты вредоносные скрипты для кражи вводимой пользователями информации.

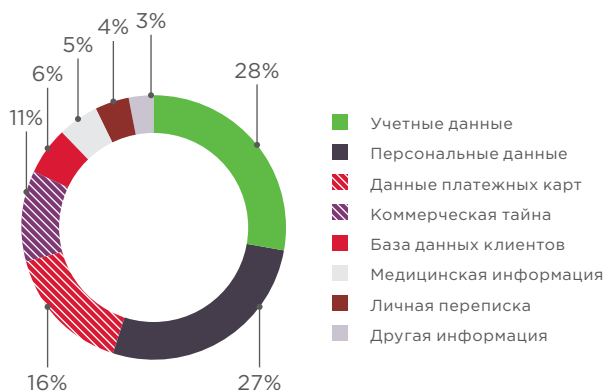


Рисунок 2. Типы украденных данных



В IV квартале 2018 года доля целенаправленных атак продолжила расти и составила 62%. Мы видим, что злоумышленники все чаще используют индивидуальный подход для атак на организации, а частные лица страдают от масштабных заражений вредоносным ПО. Далее мы остановимся подробнее на атаках, направленных на частных лиц, государственные и медицинские учреждения, финансовую отрасль и IT-компании, — поскольку именно в них чаще всего заинтересованы киберпреступники.

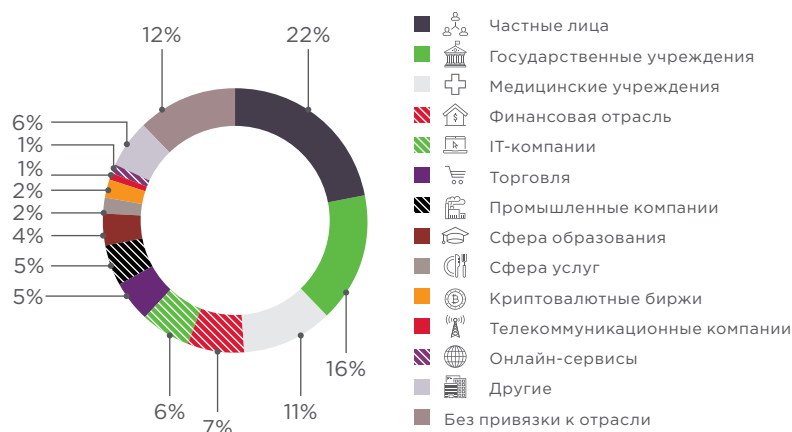


Рисунок 3. Категории жертв

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

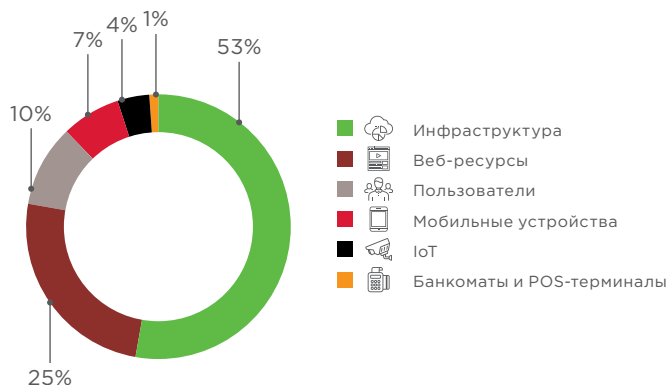


Рисунок 4. Объекты атак

Доля атак, нацеленных на инфраструктуру, в IV квартале 2018 года выросла по сравнению с аналогичным периодом прошлого года и составила 53% против 46% в 2017, доля атак на веб-ресурсы также немного подросла и составила 25%, а вот доли атак на пользователей и мобильные устройства снизились до 10% и 7% соответственно.

Рейтинг наиболее часто применяемых методов атак в течение года остается неизменным. В IV квартале 2018 года немного снизилась доля атак, в которых злоумышленники использовали вредоносное ПО (55% вместо 56% в III квартале). На 6% по сравнению с предыдущим периодом снизилась доля атак с использованием методов социальной инженерии. На 3% выросла доля атак, в ходе которых злоумышленники использовали уязвимости в веб-приложениях (и составила 20%), и на 4% — в которых были подобраны учетные данные (17%). Далее мы подробнее остановимся на каждом методе и укажем, какие объекты и отрасли больше всего пострадали от этих категорий атак.

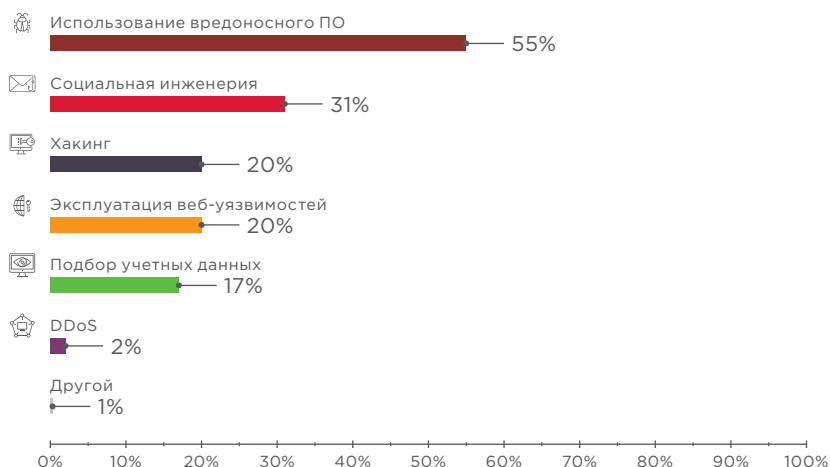


Рисунок 5. Методы атак

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	Сфера образования	Торговля	Телекоммуникационные компании	Частные лица	Криптовалютные биржи	Другие	Без привязки к отрасли
Всего атак		53	23	15	35	2	8	20	13	16	2	73	7	22	40
Объект	Инфраструктура	35	18	13	23		1	9	8	3	2	25	2	13	23
	Веб-ресурсы	13	3	2	6	2	5	9	1	12		10	5	7	6
	Пользователи	5			5		1	2	4	1		14		2	
	Мобильные устройства											22			
	Банкоматы и POS-терминалы		2				1								
	IoT				1							2			11
Метод	Атаки с использованием ВПО	29	14	12	15		4	7	5	6		53	1	6	30
	Социальная инженерия	19	12	5	7		1	1	8	1		34	1	5	8
	Подбор учетных данных	11	4	1	13		2	2	2	2		8		7	5
	Хакинг	8	10	1	5			6		2	2	4	6	5	18
	Эксплуатация веб-уязвимостей	11	2	3	4	2	5	5	1	10		8	1	7	6
	DDoS	1						4							2
	Другой											2			1
Мотив	Финансовая выгода	8	11		7		4	5	6	5	1	46	7	10	19
	Получение данных	37	12	14	26	2	3	6	6	10	1	21		8	13
	Хактивизм	6			2		1	9	1	1		5		4	7
	Кибервойна	2		1								1			1
Интенсивность цвета показывает долю атак в рамках одной отрасли		<div><div></div></div>													
		0%	10%	20%	30%	40%	100%								



Динамика атак

Количество уникальных киберинцидентов в IV квартале 2018 года на 11% превысило показатели аналогичного периода в 2017 году и на 7% — показатели предыдущего, III квартала.

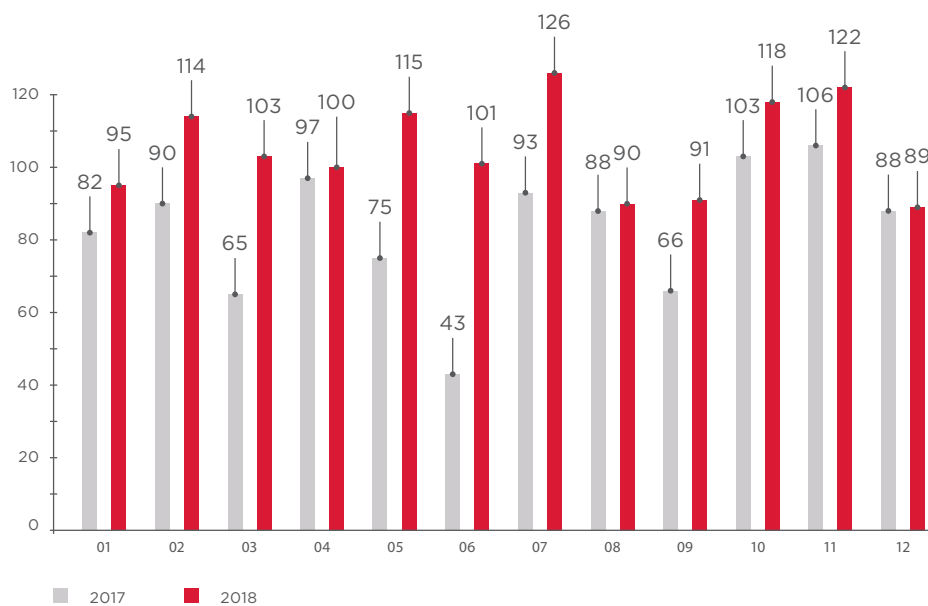


Рисунок 6. Количество инцидентов в 2017 и 2018 годах (по месяцам)

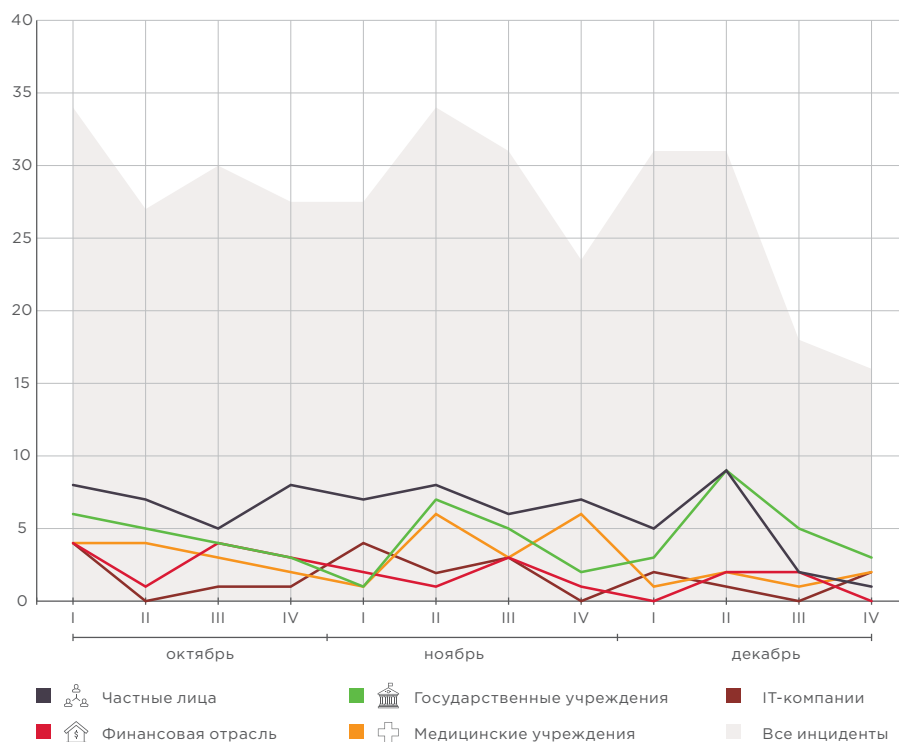


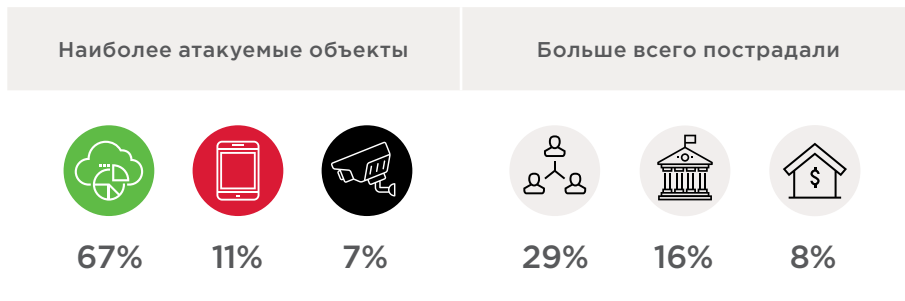
Рисунок 7. Количество инцидентов в IV квартале 2018 года (по неделям)



Методы атак

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

Использование вредоносного ПО



Для сбора информации с компьютеров и смартфонов жертв злоумышленники продолжают использовать шпионское ПО (29% случаев) и ВПО для удаленного управления (25%). Резкое увеличение количества заражений шифровальщиками, которое мы наблюдали в III квартале, в IV квартале вернулось к прежним значениям и составило 9% всех заражений.

В 39% случаев заражение происходило путем предварительной компрометации серверов и рабочих станций. Так, шифровальщик JungleSec³ поражал компьютеры через незащищенные интерфейсы IPMI (Intelligent Platform Management Interface), например использующие учетные данные по умолчанию. В 29% атак с использованием ВПО вредоносное вложение отправлялось жертве по электронной почте, а в 16% случаев загрузка ВПО происходила при посещении зараженного сайта.

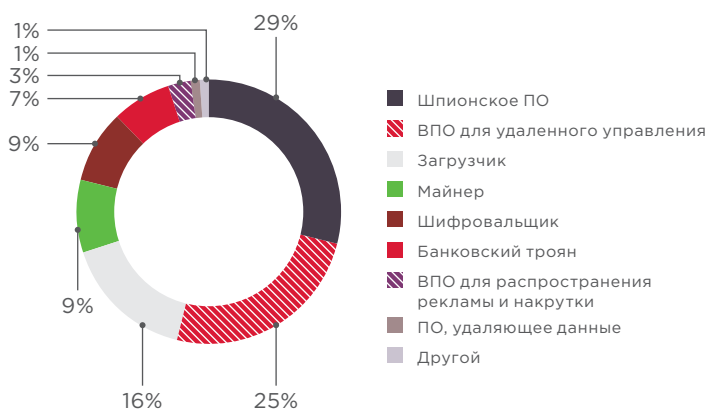


Рисунок 8. Типы вредоносного ПО

³ bleepingcomputer.com/news/security/junglesec-ransomware-infects-victims-through-ipmi-remote-interfaces/

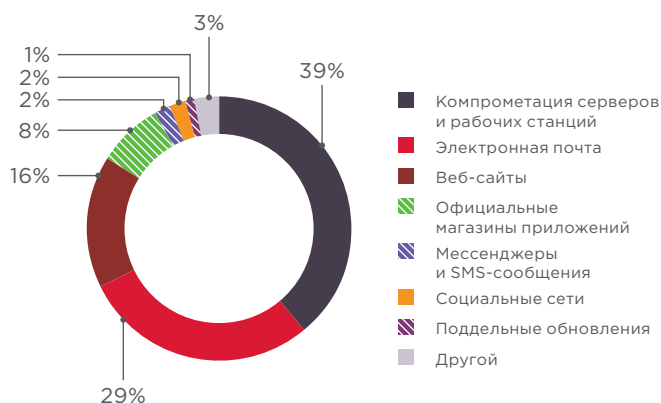


Рисунок 9. Способы распространения ВПО

Специалисты по безопасности регулярно сообщают о ВПО, найденном в официальных магазинах мобильных приложений. К примеру, в ноябре стало известно о поддельных криптокошельках в магазине Google Play⁴. Есть и другие примеры, когда вредоносное ПО распространяется через доверенные ресурсы. В октябре было обнаружено 12 поддельных библиотек в репозитории PyPI — Python Package Index⁵, имитирующих различные популярные пакеты и имеющих схожие имена (например, diango, djago, dajngo вместо Django). В 2017 году специалисты из Национальной службы безопасности Словакии уже находили вредоносные библиотеки в репозитории Python, однако, как мы видим, ситуация не изменилась, и проверок безопасности, которые бы не позволили загрузить вредоносные пакеты в каталог, не появилось.

Социальная инженерия



Социальная инженерия в IV квартале использовалась практически в каждой третьей атаке. Фишинг в адрес сотрудников компании-жертвы стал уже отработанной схемой злоумышленников в рамках целенаправленных атак.

В ноябре специалисты PT ESC обнаружили вредоносное вложение электронной почты формата Publisher с названием «Приглашение 29–30 ноября 2018.pub»⁶, которое позволяло злоумышленнику захватывать изображение с веб-камер, записывать звук по команде или при обнаружении окна Skype, запускать PowerShell-скрипты, делать скриншоты экрана, копировать файлы с медиаустройств. Для этого жертве необходимо было включить скрипт Microsoft Publisher при открытии документа. Злоумышленники ловко привлекли внимание читателей размытым изображением, на котором проглядывал герб — так, что документ должен был вызывать доверие и желание с ним ознакомиться, включив необходимый скрипт. В файл был встроен код JavaScript, который раскодировал PDF и EXE из Base64 и исполнял их, а жертва тем временем видела на экране документ-заглушку. Таким образом на компьютере незаметно для пользователя устанавливалось ВПО для удаленного управления Treasure Hunter, которое собирало информацию о системе, отправляло ее на удаленный командный сервер и принимало команды с него.

4 lukasstefanko.com/2018/11/fake-cryptocurrency-wallets-found-on-play-store.html

5 zdnet.com/article/twelve-malicious-python-libraries-found-and-removed-from-pypi/

6 habr.com/company/pt/blog/432172/

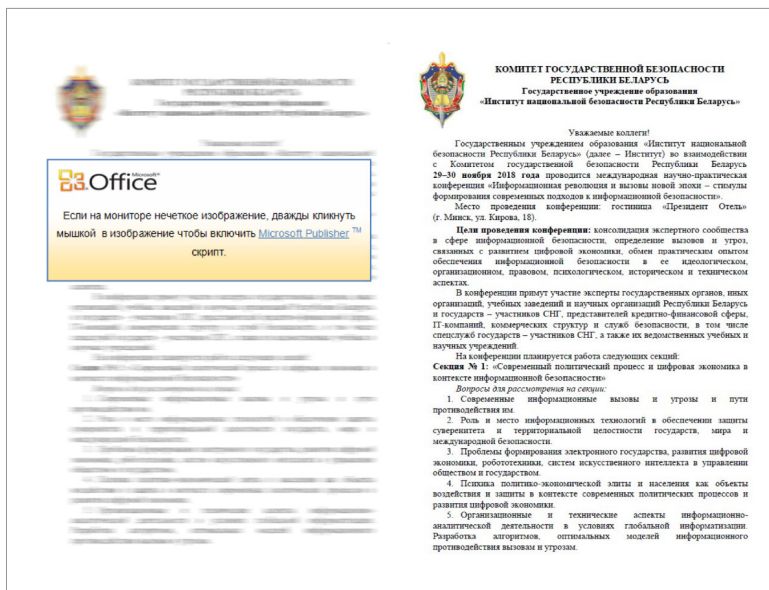


Рисунок 10. Документ-заглушка для ВПО Treasure Hunter RAT

Электронные письма часто рассылаются в маркетинговых целях и содержат кнопки-приглашения для перехода на сайт. Мы напоминаем, что перед нажатием на такую кнопку в письме необходимо обратить внимание на имя адресанта, а также на ссылку, куда будет осуществлен переход после нажатия. Так, например, клиенты Spotify в ноябре стали жертвами фишинговой кампании⁷. Злоумышленники заманивали пользователей на поддельный сайт и просили ввести учетные данные.

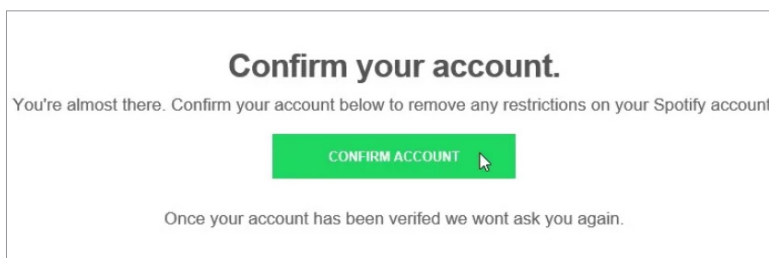


Рисунок 11. Текст фишингового письма

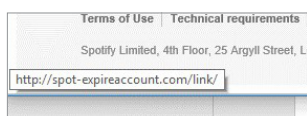


Рисунок 12. Адрес, на который перенаправлялся пользователь из письма

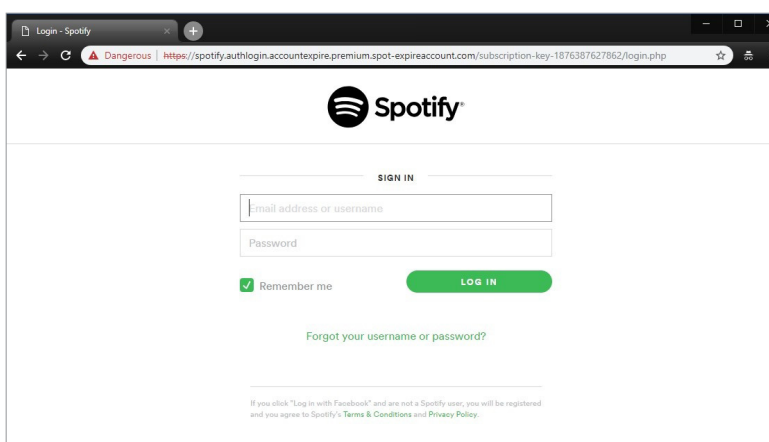
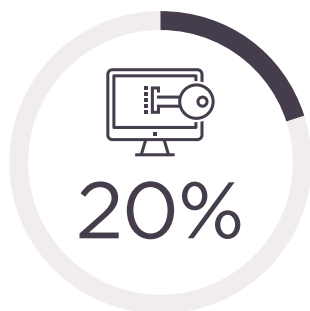


Рисунок 13. Фишинговый сайт, на который попадал пользователь, перейдя по ссылке

⁷ blog.appriver.com/spotify-phishing-campaign-making-rounds



Хакинг



Наиболее атакуемые объекты



69%



15%



10%



15%



12%



9%

Больше всего пострадали

Хакинг — это метод атак с использованием уязвимостей в ПО, службах, ошибок в механизмах защиты и других недостатков атакуемых систем без применения социальной инженерии и вредоносного ПО — и без учета веб-атак, которые мы выделили в отдельную категорию. В последние пару лет злоумышленники стали активно проверять на прочность блокчейн-платформы. В первом полугодии мы уже отмечали атаки типа «51%» на криптовалюты, в ходе которых преступники завладевают «контрольным пакетом» генерирующих мощностей сети (хешрейта) и получают возможность проводить двойное списание средств (double spending). В ходе такой атаки на криптовалюту Vertcoin⁸ в ноябре злоумышленникам удалось совершить не менее 15 двойных списаний монет на общую сумму более 100 тыс. долл. США.

Уязвимость во фреймворке ThinkPHP, позволяющая удаленно выполнить произвольный код на сервере, поставила под угрозу более 45 000 китайских сайтов⁹. Спустя всего сутки после публикации информации о выявленной уязвимости и PoC-эксплойта сразу несколько хакерских групп начали поиск уязвимых ресурсов и попытки использовать этот недостаток.

Эксплуатация веб-уязвимостей



Наиболее атакуемые объекты



92%



8%



17%



15%



12%

Больше всего пострадали

Четвертый квартал 2018 года выделился большим количеством кибератак, в ходе которых злоумышленники внедряли в код уязвимых сайтов вредоносные скрипты. Например, группировка MageCart (под этим названием фигурируют семь различных группировок со схожим почерком¹⁰) ищет уязвимые интернет-магазины и через недостатки в CMS или ее плагинах внедряет вредоносный JavaScript-код на страницы оплаты. Таким образом были похищены вводимые пользователями данные (номера банковских карт, имена, адреса и т. п.) в интернет-магазинах OppoSuits¹¹, Infowars¹², Umbro Brasil¹³. Как правило, преступники, добывающие данные банковских карт, не занимаются получением денег с них, а продают информацию на теневом рынке¹⁴.

8 medium.com/coinmonks/vertcoin-vtc-is-currently-being-51-attacked-53ab633c08a4

9 zdnet.com/article/chinese-websites-have-been-under-attack-for-a-week-via-a-new-php-framework-bug/

10 riskiq.com/research/inside-magecart/

11 itwire.com/security/85506-clothing-company-opposuits-hit-by-magecart-attack.html

12 zdnet.com/article/card-skimming-malware-removed-from-infowars-online-store/

13 blog.malwarebytes.com/threat-analysis/2018/11/web-skimmers-compete-umbro-brasil-hack/

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

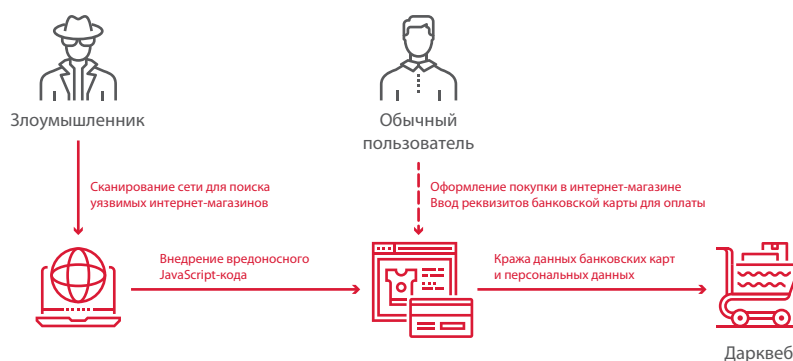
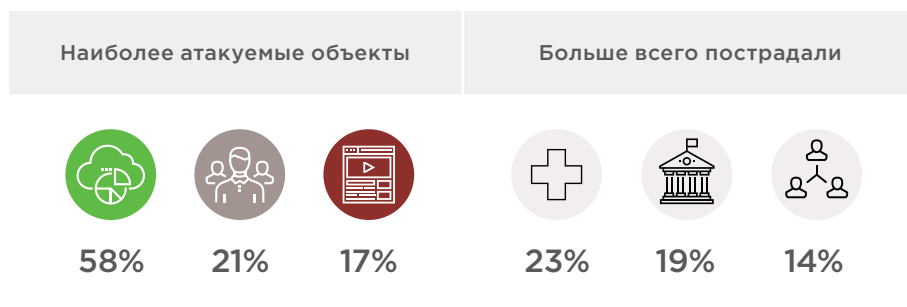
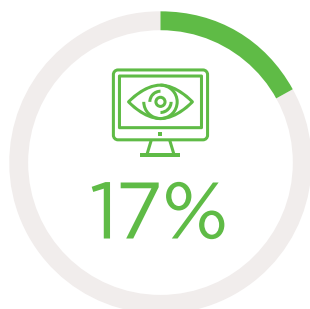


Рисунок 14. Схема действий группировки MageCart

Специалисты ESET в ноябре рассказали о группировке OceanLotus, скомпрометировавшей 21 сайт для проведения атак watering hole¹⁵. Суть подобных атак состоит в том, что злоумышленники заражают вредоносным ПО сайты, часто посещаемые их потенциальными жертвами. Это могут быть сайты компаний-партнеров или подрядчиков, общественных организаций и даже правительственных учреждений. Стоит кому-то зайти на такой сайт, как злоумышленники получают доступ к данным на компьютере жертвы, сообщениям электронной почты, любой важной информации, такой как учетные записи и пароли. Среди скомпрометированных OceanLotus оказались сайт министерства иностранных дел Камбоджи, министерства обороны Камбоджи, а также ряд новостных веб-ресурсов Вьетнама.

Подбор учетных данных



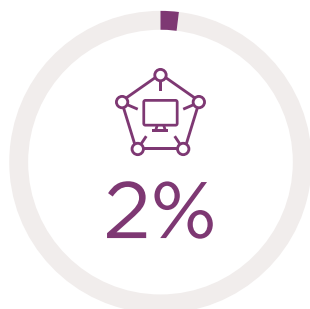
Практика показывает, что подбор паролей часто является исходным вектором компрометации инфраструктуры компаний. Так, в одном из инцидентов, расследованных специалистами PT ESC в конце 2018 года, злоумышленник скомпрометировал сервер жертвы методом перебора паролей по протоколу RDP и затем начал исследование внутренней сети. Преступник вывел из строя серверы путем шифрования системных файлов, а затем потребовал выкуп за расшифровку информации. Таким образом использование словарных паролей, отсутствие двухфакторной аутентификации и недостаточный уровень защищенности ресурсов позволили злоумышленнику получить доступ к внутренней сети жертвы. В рамках данного инцидента преступника интересовала финансовая выгода, но он обладал достаточными возможностями для шпионажа, атак на контрагентов компании и других более сложных атак. Впоследствии было выявлено, что хакер провел аналогичные атаки на периметр сети порядка 30 компаний из различных отраслей экономики. Около половины атак оказались успешны благодаря тому, что для учетной записи администратора ОС использовались крайне слабые пароли (123456, Pass123123, Qwerty12345, 123qweASD и т. п.), а RDP-порты на компьютерах и серверах оказались открыты для подключения из интернета. Подобную атаку может осуществить любой нарушитель, даже имеющий низкую квалификацию, поэтому крайне важно следить за безопасностью периметра компании и проводить инвентаризацию доступных для подключения ресурсов.

¹⁵ wlvsecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/



Ботнеты не всегда используются для DDoS-атак. В декабре исследователи компании Defiant рассказали о необычном ботнете, состоящем из 20 000 сайтов¹⁶. Злоумышленники использовали веб-ресурсы под управлением WordPress для проведения брутфорс-атак на панели администраторов целевых сайтов, чтобы затем с их помощью проводить новые атаки. За месяц было зафиксировано более 5 миллионов таких попыток перебора учетных данных.

DDoS



Наиболее атакуемые объекты



72%



14%



14%



57%



14%

Больше всего пострадали

Доля DDoS-атак из квартала в квартал меняется незначительно. В октябре был обнаружен новый ботнет для DDoS-атак¹⁷. DemonBot состоит из уязвимых серверов Hadoop с неверно настроенным модулем YARN (Yet Another Resource Negotiator). Уязвимость позволяет добавить в кластер новое приложение, и таким образом злоумышленники устанавливают на серверы ВПО для организации DDoS-атак (UDP- и TCP-флуда). Стоит отметить, что эта уязвимость известна с 2016 года¹⁸, однако IT-специалисты нередко недооценивают важность обеспечения безопасности и не выполняют необходимую настройку при развертывании инфраструктуры.

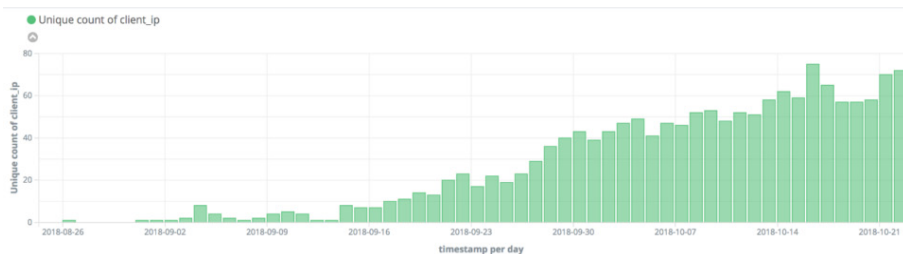


Рисунок 15. Число атакованных серверов Hadoop

Также в октябре была отмечена группировка хактивистов Anonymous, которая в этот раз нацелилась на государственные веб-ресурсы Габона, нарушив работу более 70 сайтов¹⁹.

¹⁶ wordfence.com/blog/2018/12/wordpress-botnet-attacking-wordpress/

¹⁷ blog.radware.com/security/2018/10/new-demonbot-discovered/

¹⁸ archive.hack.lu/2016/Wavestone-Hack.lu-2016-Hadoop-safari-Hunting-for-vulnerabilities-v1.0.pdf

¹⁹ news24.com/Africa/News/gabon-official-websites-hacked-anonymous-group-20181029



Категории жертв

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

Государственные организации



Ущерб более
50 тыс. долл. США



Рисунок 16. Методы атак на государственные организации в Q4 2018

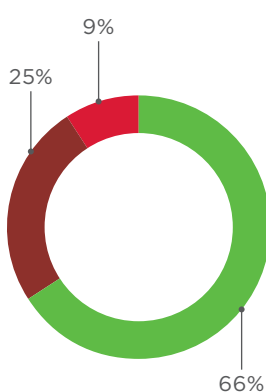
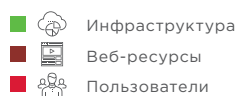


Рисунок 17. Объекты атак

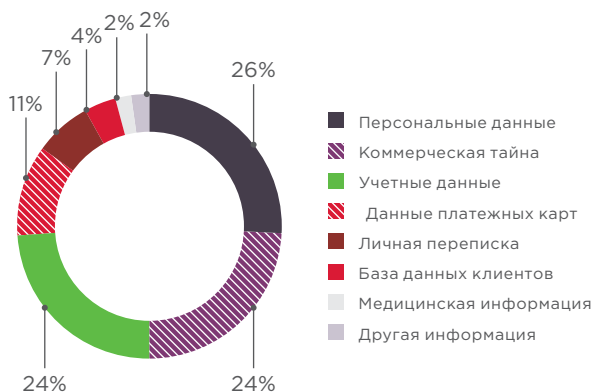


Рисунок 18. Украденные данные

Государства становятся цифровыми, государственные услуги переходят в сеть, оплату за них принимают по интернету. Многие задачи гражданам становится решать проще, но вместе с тем появляются новые риски и угрозы, связанные с киберпреступностью. С апреля 2017 года по декабрь 2018 года продолжались атаки на интернет-портал Click2Gov²⁰, принимающий платежи за парковку, коммунальные и другие муниципальные услуги в США. Всего было зафиксировано 20 подобных инцидентов, приведших к утечке не менее чем 111 860 платежных карт. Предполагается, что злоумышленники загружали на веб-серверы JSP-оболочку SJavaWebManage и в режиме отладки получали доступ к данным банковских карт в незашифрованном виде. Примечательно, что данные об уязвимостях в этом платежном сервисе и рекомендации по их устранению появились еще в 2017 году, но судя по тому, что кибератаки продолжались в течение полутора лет, организации, пользующиеся этой системой, не следили за новостями в сфере ИБ и не приняли необходимых мер защиты.

²⁰ <https://geminiadvisory.io/hacked-click2gov-exposed-payment-data/>

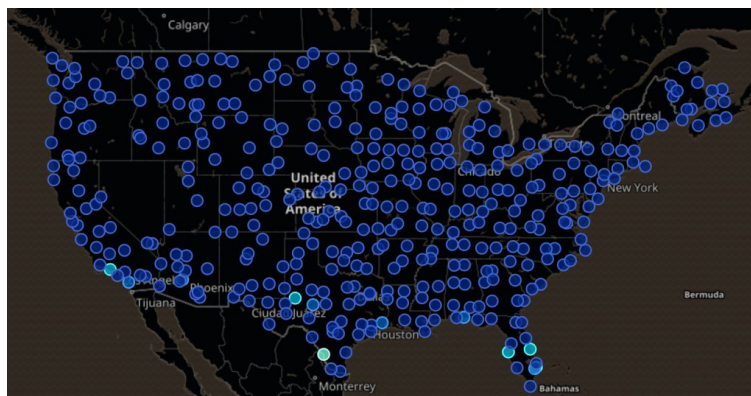


Рисунок 19. Местоположение жертв атаки на портал Click2Gov

Специалисты PT ESC в IV квартале 2018 года отметили активность двух группировок, Danti APT и SongXY, направленную против государственных организаций России и стран СНГ. В ноябре был обнаружен вредоносный документ группы Danti APT, активность которой последний раз наблюдалась в 2016 году. Интересно, что функции используемого ВПО за два года не изменились: троян собирал и отправлял на контрольный сервер данные об используемой инфраструктуре (информацию о процессоре, памяти, версии операционной системы, имя пользователя, данные о сети). Но в этот раз злоумышленники вместо CVE-2015-2545²¹ эксплуатировали другую уязвимость Microsoft Office — CVE-2017-11882²².

После достижения 5,9% роста в 2017 году ожидается, что восточноазиатская экономика будет устойчивым ростом в 5,7% и 5,6% в 2018 и 2019 годах, соответственно. При поддержке умеренного инфляционного давления, низких процентных ставок и здоровых условий на рынке труда личное потребление будет оставаться основным фактором экономического роста. Поскольку правительство приступает к строительству крупных инфраструктурных проектов, ожидается, что государственные инвестиции останутся сильными. Ожидается, что сильный рост экспорта в 2017 году замедлится, благоприятные условия внешнего спроса будут продолжать поддерживать региональные перспективы.

В докладе прогнозируется, что экономические перспективы Южной Азии остаются стабильными и оптимистичными, что обусловлено сильным личным потреблением и разумной макроэкономической политикой. Позитивный прогноз поможет постоянно улучшать показатели рынка труда и снижать уровень бедности. Позиция денежно-кредитной политики умеренно ослаблена, но фискальная политика все еще подчеркивает инвестиции в инфраструктуру. После достижения в 2017 году роста примерно на 6,3%, региональный рост ВВП в Южной Азии, как ожидается, ускорится до 6,5% и 6,7% в 2018 и 2019 годах, соответственно. Ожидается, что региональная инфляция будет оставаться стабильной и на относительно низком уровне. Экономические перспективы Индии остаются оптимистичными благодаря сильному личному потреблению, сильным государственным инвестициям и структурным реформам. Ожидается рост ВВП Индии с 6,7% в 2017 году до 7,2% в 2018 году и 7,4% в 2019 году. Однако слабая эффективность частных инвестиций остается ключевой макроэкономической проблемой.

Рисунок 20. Документ-заглушка, рассылаемый группировкой Danti APT по электронной почте

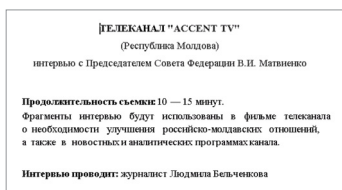


Рисунок 21. Документ-заглушка, рассылаемый группировкой SongXY по электронной почте

Также в ноябре эксперты PT ESC обнаружили вредоносный документ группировки SongXY. Во время своей последней активности, в 2017-м — начале 2018 годах, группа использовала документы Microsoft Office с макросами, а в этот раз она сменила загрузчик и использовала тот же эксплойт, что и у Danti APT, эксплуатирующий CVE-2017-11882. ВПО собирало информацию с зараженного компьютера и передавало ее злоумышленникам.

²¹ nvd.nist.gov/vuln/detail/CVE-2015-2545

²² nvd.nist.gov/vuln/detail/CVE-2017-11882



Пострадали более
3 млн человек

Медицинские учреждения

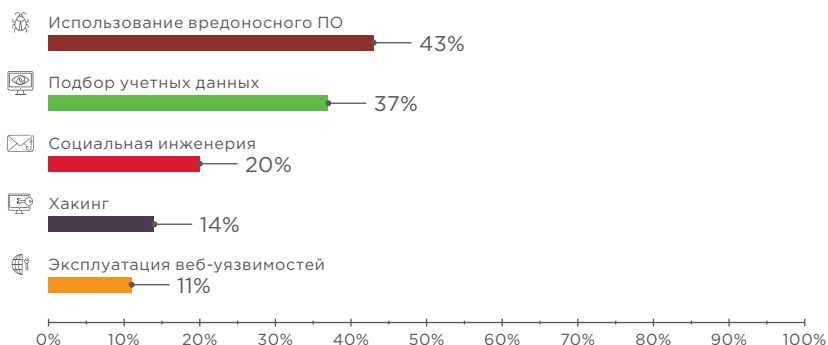


Рисунок 22. Методы атак на медицинские учреждения в Q4 2018

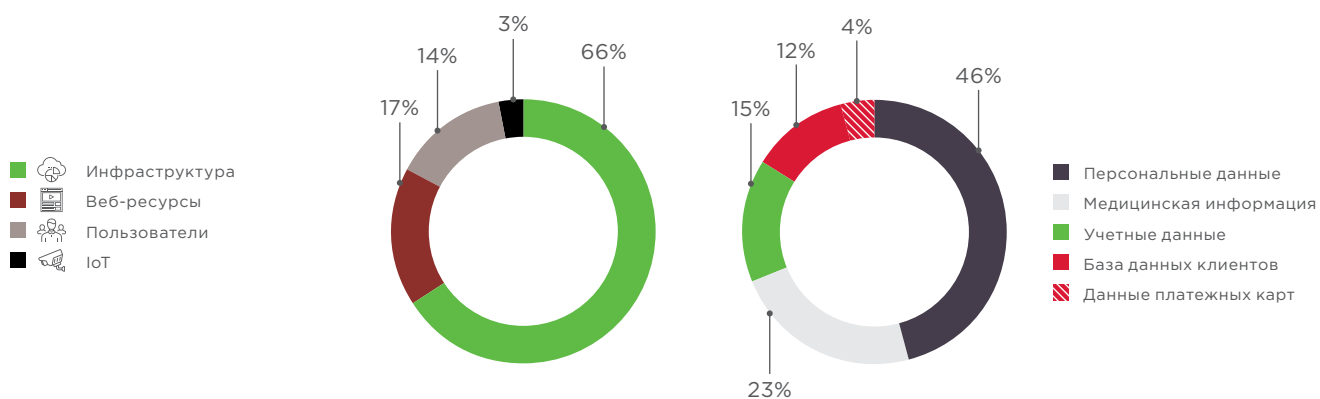


Рисунок 23. Объекты атак

Рисунок 24. Украденные данные

Тренд внедрения вредоносных скриптов в код уязвимых сайтов не обошел стороной и медицинские учреждения. Так, портал, принимающий оплату за медицинские услуги, подвергся атаке²³ и данные 5850 человек, которые вводили номера своих банковских карт для оплаты на сайте в период между 25 октября и 8 ноября, предположительно оказались в руках киберпреступников. Скорее всего, эта информация уже продается в дарквебе.

В остальном атаки на медицинские учреждения в IV квартале не отличались оригинальностью. Киберпреступники продолжили компрометировать компьютеры сотрудников компаний (подбирая пароли к их учетным записям и рассылая вредоносное ПО по электронной почте) и таким образом получать доступ к медицинской информации и персональным данным пациентов.

²³ bnd.com/news/local/article223273720.html



Ущерб более
20 млн долл. США
Пострадали более
1 млн человек

Финансовая отрасль

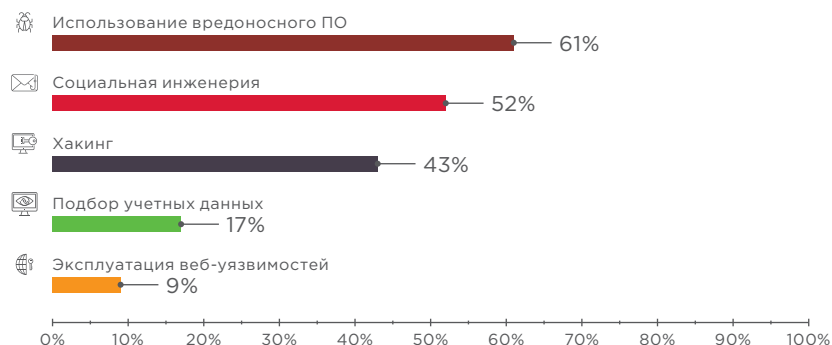


Рисунок 25. Методы атак на финансовую отрасль в Q4 2018

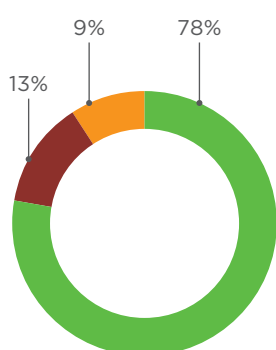
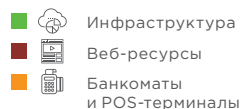


Рисунок 26. Объекты атак

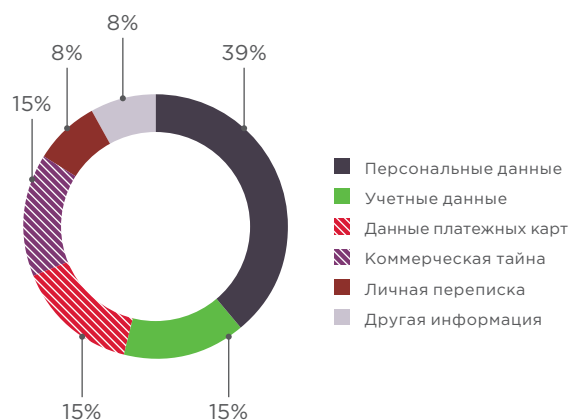


Рисунок 27. Украденные данные

В IV квартале специалисты PT ESC отметили активность трех групп, атакующих финансовые организации: уже знакомых Silence и Cobalt, а также новую группу, нацеленную на российские банки. Группа Silence провела две атаки в октябре и одну в конце декабря. В октябре жертвам рассылался вредоносный CHM-файл, упакованный в архив, имеющий очень низкий уровень обнаружения антивирусным ПО. Итоговым загрузчиком в этих атаках был silence-загрузчик, собирающий информацию о системе (systeminfo, ipconfig) и отправляющий ее на удаленный сервер вместе с серийным номером жесткого диска для уникальности. В декабре группа рассылала RTF-файл со встроенным, в виде OLE-объекта, CHM-файлом, а код итогового silence-загрузчика был существенно изменен.

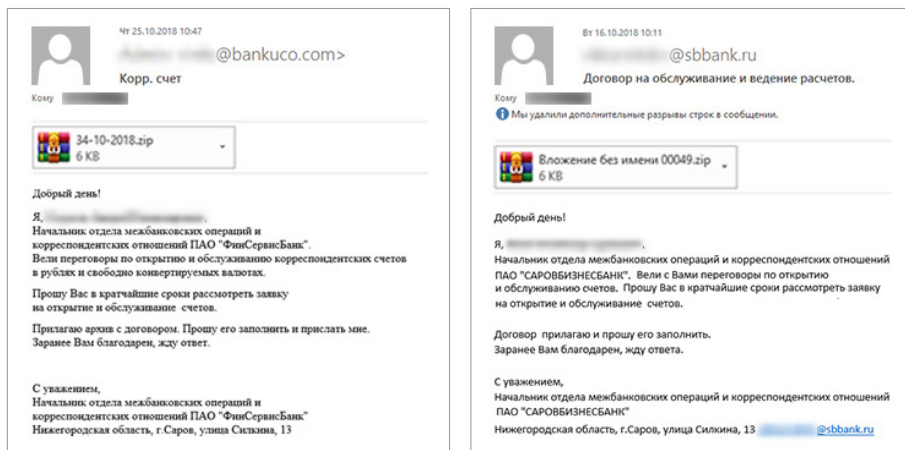


Рисунок 28. Октябрьские фишинговые рассылки Silence

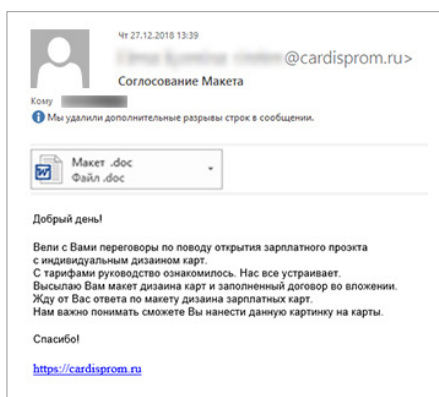


Рисунок 29. Декабрьская фишинговая рассылка Silence

За IV квартал было зафиксировано 11 атак группы Cobalt, некоторые из них проводились за пределами СНГ. Две фишинговые рассылки проводились от лица взломанных банков — Unistream и Kassa Nova в Казахстане. Остальные атаки были направлены на российские банки. Примечательно, что группировка вновь провела вредоносную рассылку в день публикации информации об уязвимости нулевого дня CVE-2018-15982²⁴ (как в 2017 году при появлении данных о CVE-2017-11882). Однако злоумышленники допустили ошибку, не упаковав полезную нагрузку в архив, и команды в шелл-коде (взятом из статьи об уязвимости) на распаковку архива не могли выполняться успешно.

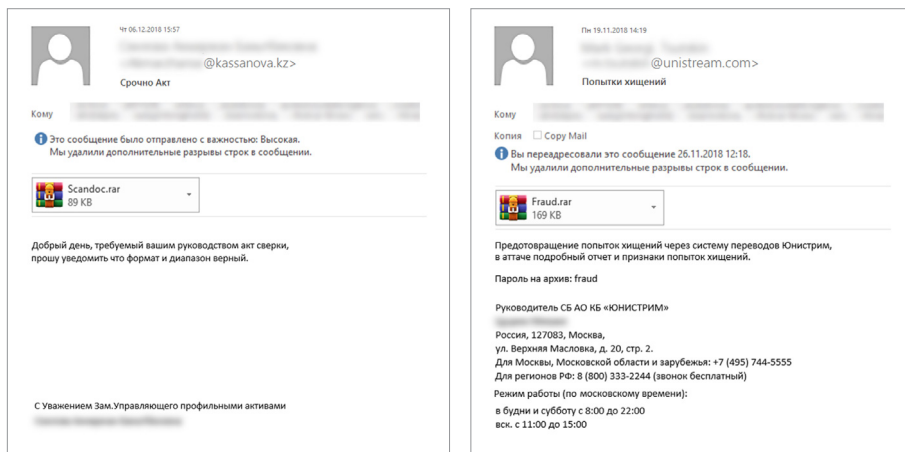


Рисунок 30. Фишинговые рассылки Cobalt от лица Unistream и Kassa Nova

²⁴ cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15982

Кроме того, в октябре специалисты PT ESC обнаружили новую группировку, атаковую финансовый сектор. Злоумышленники рассылали якобы от лица ФинЦЕРТ вредоносные документы с макросами. При исполнении макроса на компьютер загружалась полезная нагрузка — Metasploit stager. Этот stager определял версию системы (x86 или x64) и в зависимости от версии переходил по одному из двух жестко заданных в его коде URL. С этих адресов в память атакуемой системы загружался еще один payload — Meterpreter, и злоумышленник получал таким образом удаленный доступ к зараженному компьютеру. Загрузка Meterpreter и дальнейшее общение с контрольным сервером, включая загрузку дополнительных модулей, происходили по защищенному протоколу TLS.

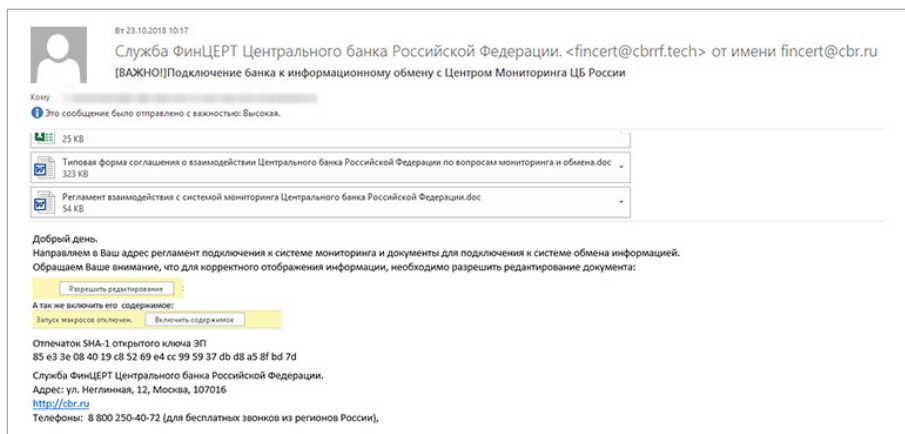


Рисунок 31. Фишинговая рассылка от лица ФинЦЕРТ

А в декабре была зафиксирована рассылка, которая проводилась через скомпрометированную учетную запись сотрудника компании «Альфа-Капитал». При анализе рассылаемого документа был обнаружен сценарий на JavaScript, который использовала группа Treasure Hunters²⁵, однако в него была добавлена функция запуска Metasploit stager.

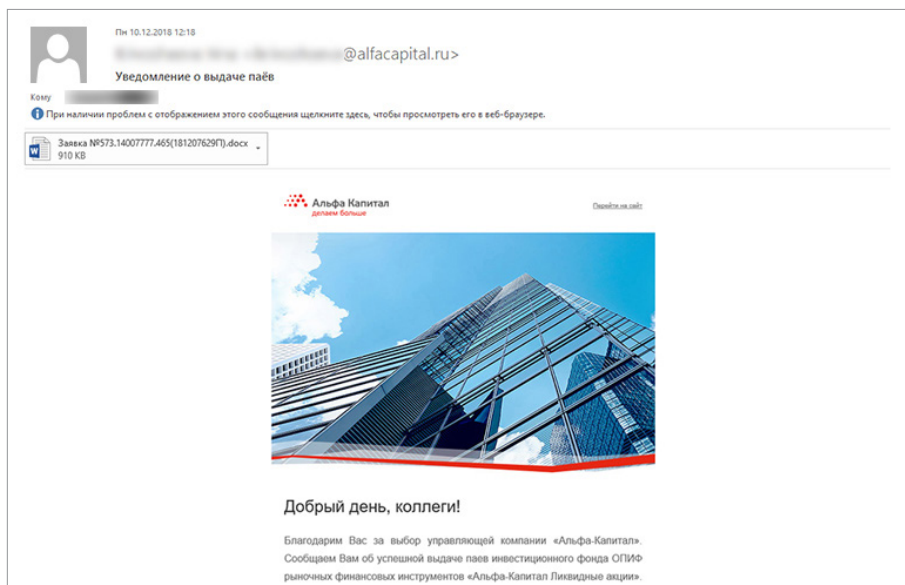


Рисунок 32. Фишинговая рассылка от лица компании «Альфа-Капитал»

²⁵ habr.com/company/pt/blog/432172/



Несмотря на схожесть атак от имени ФинЦЕРТ и компании «Альфа-Капитал» с активностью группы Treasure Hunters, в результате анализа трафика и на основании использования в качестве полезной нагрузки Metasploit stager и Meterpreter были сделаны выводы о появлении новой группы киберпреступников, нацелившейся на финансовые организации.

IT-компании



Пострадали более
1 млн человек

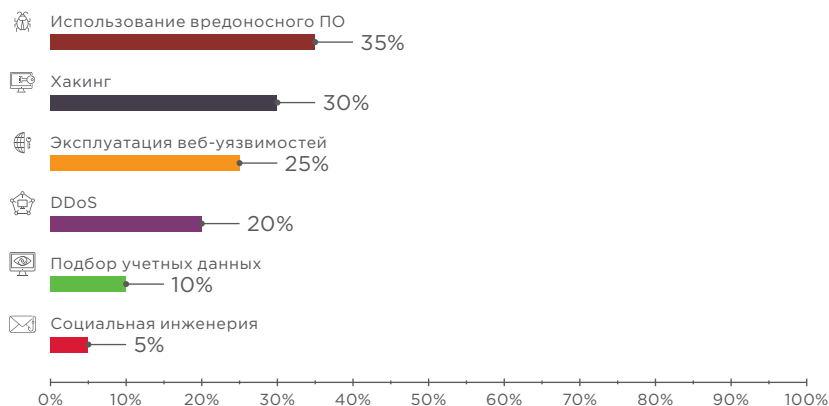


Рисунок 33. Методы атак на IT-компании в Q4 2018

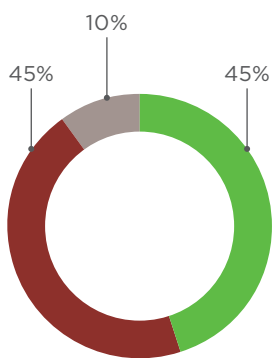
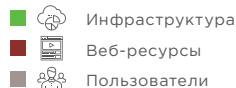


Рисунок 34. Объекты атак

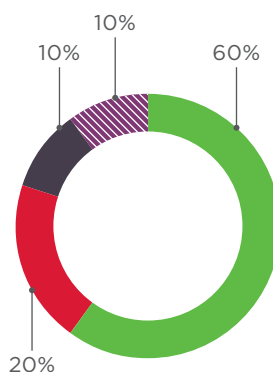


Рисунок 35. Украденные данные

IT-компании разрабатывают программное обеспечение, обслуживают IT-инфраструктуру организаций, оказывают услуги по хранению данных в облачной инфраструктуре — и этим привлекают к себе киберпреступников. Кибератаки стали многоэтапными, и взлом контрагентов (например, разработчика ПО) может быть одним из таких этапов. Кроме того, облачные провайдеры становятся привлекательной целью для вымогателей, ведь эти компании обещают клиентам безопасность размещения больших объемов данных, а также непрерывный доступ к ним, а значит — готовы платить злоумышленникам за прекращение атаки. В конце декабря провайдер облачного хостинга Dataresolution.net стал жертвой шифровальщика Ryuk²⁶. Предполагается, что группировка Lazarus с конца августа 2018 года использует это ВПО в целенаправленных атаках по всему миру.

²⁶ krebsonsecurity.com/2019/01/cloud-hosting-provider-dataresolution-net-battling-christmas-eve-ransomware-attack/



Частные лица



Ущерб более
8 млн долл. США
Пострадали более
30 млн человек

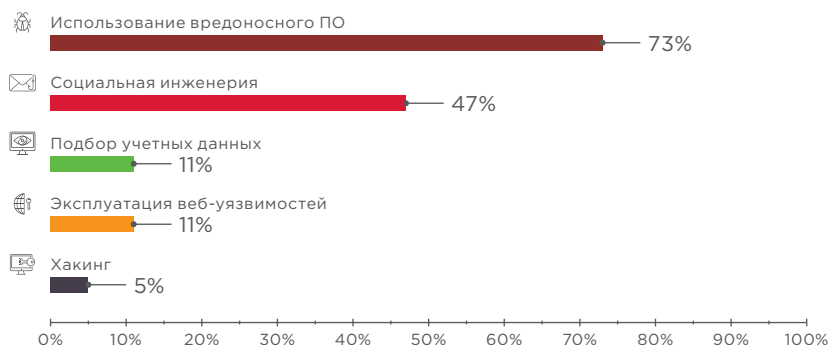


Рисунок 36. Методы атак на частных лиц в Q4 2018

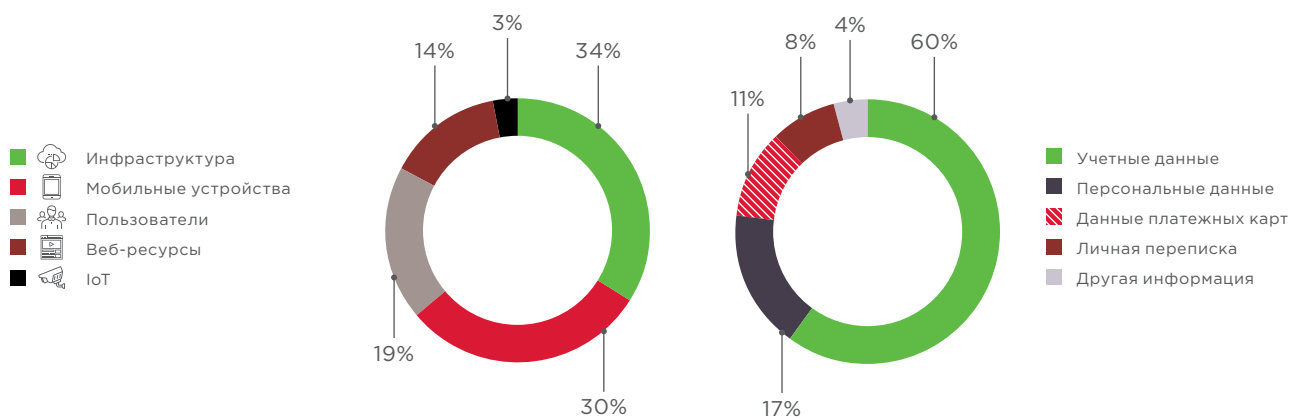


Рисунок 37. Объекты атак

Рисунок 38. Украденные данные

Треть атак на частных лиц была нацелена на получение данных. Наибольший интерес для злоумышленников представляют учетные данные (в 60% случаев крадут именно их). В октябре Национальное управление кибербезопасности Израиля рассказало о новом методе взлома аккаунтов мессенджера WhatsApp с использованием голосовой почты²⁷. Злоумышленник добавляет номер телефона жертвы в качестве новой учетной записи и приложение отправляет код проверки по SMS. Однако если пользователь не видит этих уведомлений (например, спит), то после нескольких неудачных попыток WhatsApp предлагает голосовую проверку. Если жертва опять же не находится возле телефона, то сообщение уходит в голосовую почту. Если пользователь не менял пароль для голосовой почты, то злоумышленник вводит код по умолчанию и может прослушать это сообщение, а значит, авторизоваться в приложении под чужой учетной записью. Далее украденные аккаунты могут использоваться для атак методом социальной инженерии, например для вымогательства денег у друзей жертвы или отправки ссылок на фишинговые ресурсы.

Получить вредоносное ПО по электронной почте рискуют не только сотрудники организаций, заинтересовавших киберпреступников, но и обычные люди. Так, например, в ноябре была обнаружена спам-компания, нацеленная на пользователей macOS, использующих криптокошелек Exodus: под видом обновления кошелька злоумышленники рассылали шпионское ВПО²⁸.

²⁷ scribd.com/document/390119600/Whatsapp-Israel-National-Cyber-Directorate

²⁸ labsblog.f-secure.com/2018/11/02/spam-campaign-targets-exodus-mac-users/



Как защититься организации

Используйте эффективные технические средства защиты

- Системы централизованного управления обновлениями и патчами для используемого ПО.
- 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.

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 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.

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.