



PT

# Актуальные киберугрозы

2019

[ptsecurity.com](http://ptsecurity.com)

## Содержание

Обозначения	3
Резюме	4
Число кибератак стремительно растет	5
Целенаправленные атаки в авангарде	7
Информация на вес золота	8
Вредоносное ПО развивается семимильными шагами	9
Шифровальщики наступают	10
Опасные уязвимости	12
Кнопка «Взломать интернет»	12
Next day, NextCry	12
BlueKeep	12
Держа руку на Pulse	13
Эпидемия MageCart	13
Методы атак	14
Категории жертв: государственные организации	17
Категории жертв: промышленные компании	18
Категории жертв: финансовые организации	19
Категории жертв: IT-компании	20
Как защититься организации	21
Как вендору защитить свои продукты	23
Как защититься обычному пользователю	24
Об исследовании	25

# Обозначения

## Объекты атак



Компьютеры, серверы  
и сетевое оборудование



Веб-ресурсы



Люди



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



Оборонные предприятия



Промышленные компании



Онлайн-сервисы



Сфера услуг



Транспорт



IT-компании



Торговля



Частные лица



Телекоммуникационные  
компании



Блокчейн-проекты



Другие сферы



## Резюме

- Количество уникальных кибератак увеличивалось из квартала в квартал и по итогам года на 19% превысило число кибератак в 2018 году.
- Наиболее часто кибератакам подвергались госучреждения, промышленность, медицина, сфера науки и образования, финансовая отрасль. На эти отрасли пришлось более половины всех кибератак на юридические лица (54%).
- Доля атак на промышленные компании выросла до 10% против 4% в 2018 году. Эту отрасль атакуют преимущественно с использованием вредоносного ПО (подобных атак 90%).
- Целенаправленных атак было существенно больше, чем массовых. Их доля составила 60%, что на 5 п. п. больше, чем в 2018 году. Одна из причин — рост числа АРТ-атак. На протяжении года мы отмечаем высокую активность 27 АРТ-групп.
- Информация по-прежнему представляет высокую ценность для киберпреступного сообщества. Доля кампаний, направленных на получение данных, составила 60% и 57% в атаках против юридических и частных лиц соответственно. Наибольший интерес для злоумышленников представляли персональные данные, учетные записи и данные банковских карт.
- Общее число заражений вредоносным ПО в 2019 году на 38% превысило аналогичный показатель 2018 года. Успеху вредоносных кампаний способствовала модернизация как самого ВПО, так и способов его доставки.
- Шифровальщики — одна из наиболее актуальных киберугроз для компаний по всему миру. На их долю пришёлся 31% заражений ВПО среди юридических лиц. Средняя сумма выплат в 2019 году достигла нескольких сотен тысяч долларов США. Операторы шифровальщиков шантажируют жертв публикацией похищенных перед шифрованием данных в случае отказа платить выкуп.
- На протяжении всего года регулярно наблюдались атаки с помощью JavaScript-снифферов MageCart. Они приобрели массовый характер за счет компрометации через поставщиков программного обеспечения для веб-ресурсов (supply chain).

## Число кибератак стремительно растет

В 2019 году мы зафиксировали более полутора тысяч атак; это на 19% больше, чем в прошлом году. В 81% кибератак жертвами были юридические лица. По итогам года в пятерку наиболее часто атакуемых отраслей вошли госучреждения, промышленность, медицина, сфера науки и образования, финансовая отрасль.

© Positive Technologies

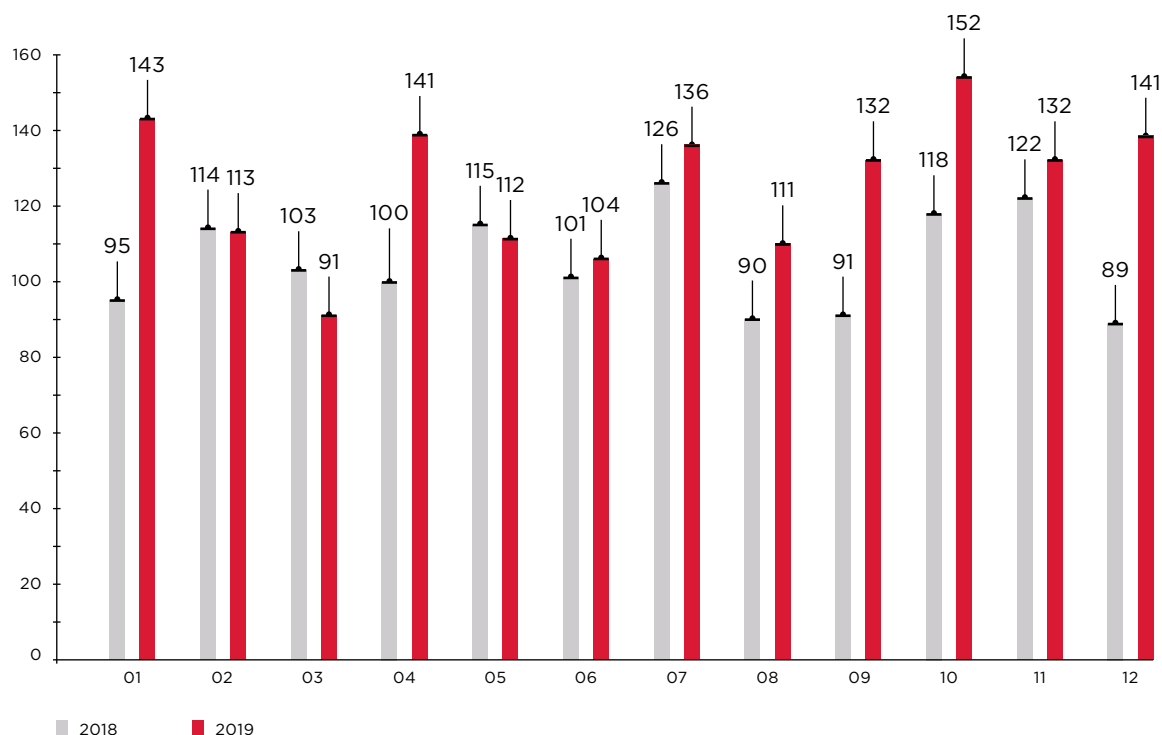


Рисунок 1. Количество кибератак в 2018 и 2019 годах (по месяцам)

© Positive Technologies

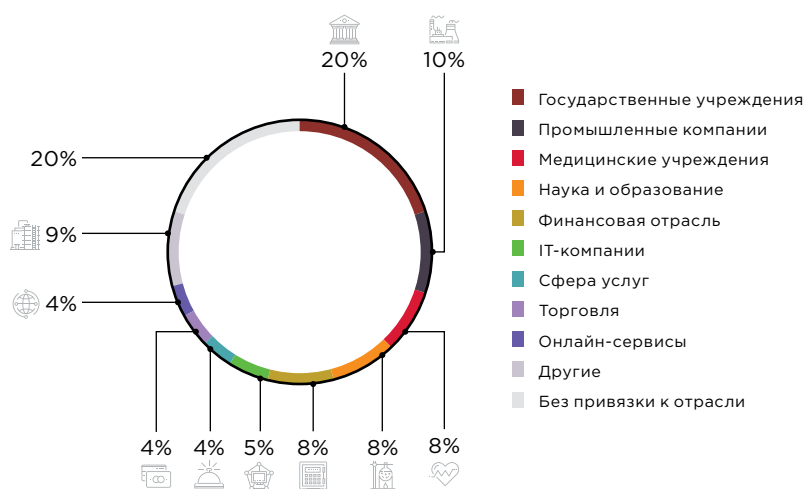


Рисунок 2. Категории жертв среди юридических лиц

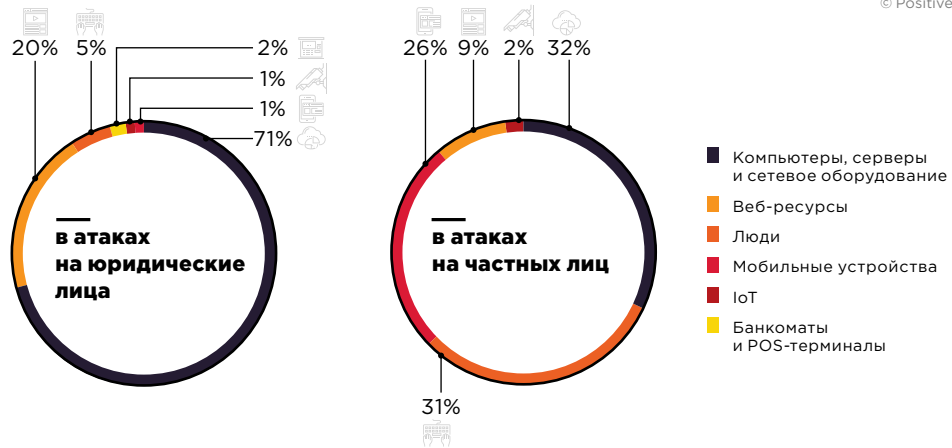


Рисунок 3. Объекты атак

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	Телекоммуникационные компании	Транспорт	Блокчейн-проекты	Другие	Без привязки к отрасли	Частные лица
Всего атак		241	92	125	93	47	51	63	93	49	15	17	23	59	248	292
Объект	Компьютеры, серверы и сетевое оборудование	169	82	118	54	15	18	51	72	17	13	11	14	41	195	92
	Веб-ресурсы	54	5	4	22	31	14	11	17	27	2	5	6	15	27	25
	Люди	15	2	3	17	1	1	1	4	1		1	3	3	12	91
	Мобильные устройства	3													5	77
	Банкоматы и POS-терминалы		3				18			4						
	IoT														9	7
Метод	Использование ВПО	154	78	112	47	5	31	34	62	19	8	11	4	37	202	169
	Социальная инженерия	130	74	105	47	2	9	20	55	15	6	11	4	30	107	184
	Подбор учетных данных	10	2	3	15	7	9	11	9	3	2	1	3	6	19	16
	Хакинг	25	5	10	4	5	4	13	9	2	1	1	14	3	73	25
	Эксплуатация веб-уязвимостей	45	1	5	3	23	8	9	9	27	3	2	2	10	25	5
	Другие	24	6	4	2	11		7	2		4		2	5	11	7
Мотив	Получение данных	143	61	110	57	29	42	37	40	37	11	10	9	26	118	167
	Финансовая выгода	51	28	12	35	3	7	21	45	9		5	13	21	111	109
	Хактивизм	39	3	2	1	15	2	5	8	3	4	2	1	10	19	16
	Кибервойна	8		1										2		
Градацией цвета показана доля атак внутри одной отрасли		<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></div></div>														
		0%	10%		20%		30%		40%		100%					

## Целенаправленные атаки в авангарде

Доля целенаправленных атак выросла на 5 п. п. по сравнению с 2018 годом и составила 60%. В каждом квартале мы наблюдали больше целевых атак, чем в предыдущем. Так, в I квартале целевыми были менее половины атак (47%), а в конце года их доля составила уже 67%.

© Positive Technologies

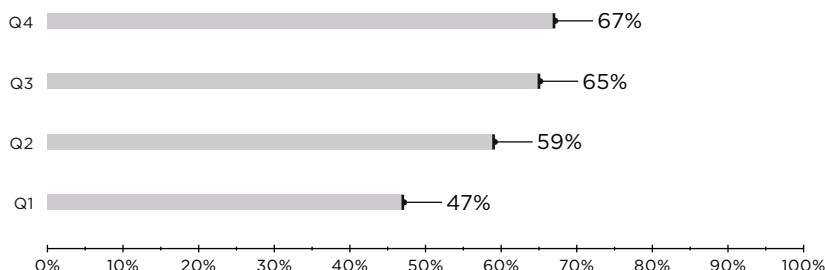


Рисунок 4. Доля целевых атак

Рост доли целенаправленных атак обусловлен рядом причин. Во-первых, злоумышленники предпочитают не тратить время на массовые кампании, которые не гарантируют им денежную прибыль. К слову, сегодня в киберпреступном сообществе наблюдается тенденция к специализации и сотрудничеству. Объединяя усилия, взломщики успешно справляются с системами защиты крупных компаний, разделяя выручку.

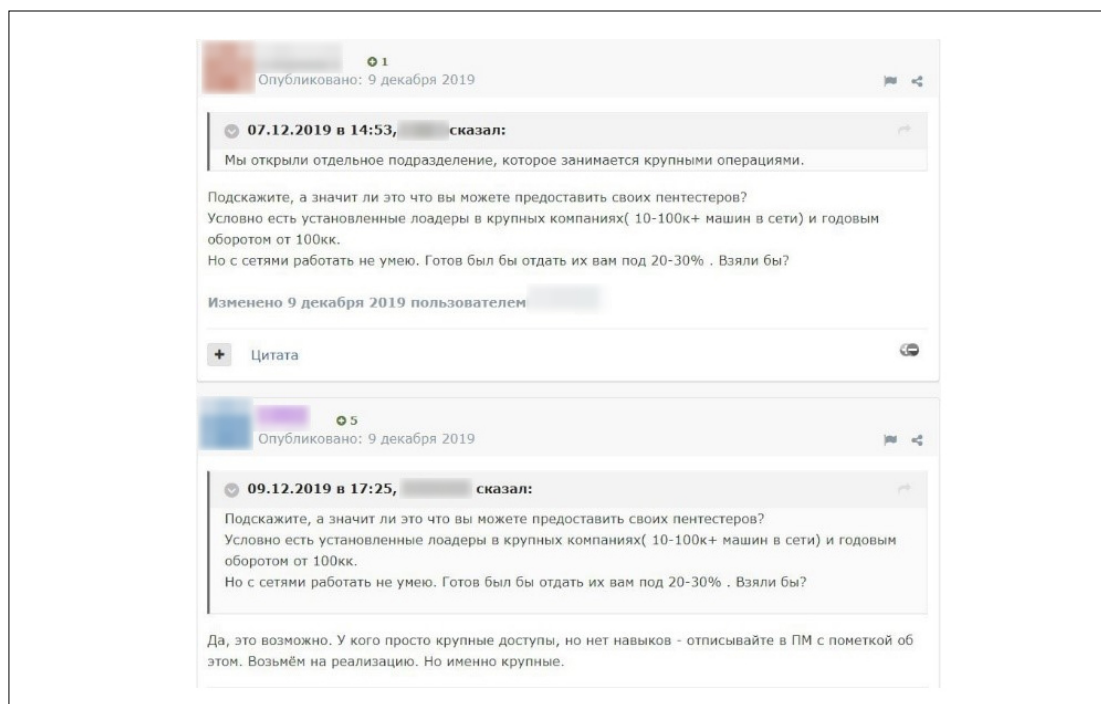


Рисунок 5. Сообщение о поиске сообщников в дарквебе

Во-вторых, ежегодно появляются новые группы злоумышленников, специализирующиеся на атаках класса APT (advanced persistent threat). В течение года эксперты Positive Technologies Expert Security Center (PT ESC) отслеживали APT-атаки 27 групп, среди которых есть как широко известные (Cobalt, Silence, APT28), так и относительно новые, малоизученные. В 2019 году специалисты PT ESC впервые подробно проанализировали APT-группу Calypso, атаковавшую государственные организации в Бразилии, Индии, Казахстане, России, Таиланде и Турции.

## Информация на вес золота

В 2019 году доля атак, направленных на кражу информации у юридических лиц, составила 60%. Значительные изменения коснулись мотивации злоумышленников в атаках против частных лиц: 57% атак были с целью хищения данных, в то время как в 2018 году аналогичный показатель составлял лишь 30%. Таким образом, в 2019 году кража информации — основной мотив злоумышленников как в атаках на организации, так и в атаках, направленных против частных лиц.

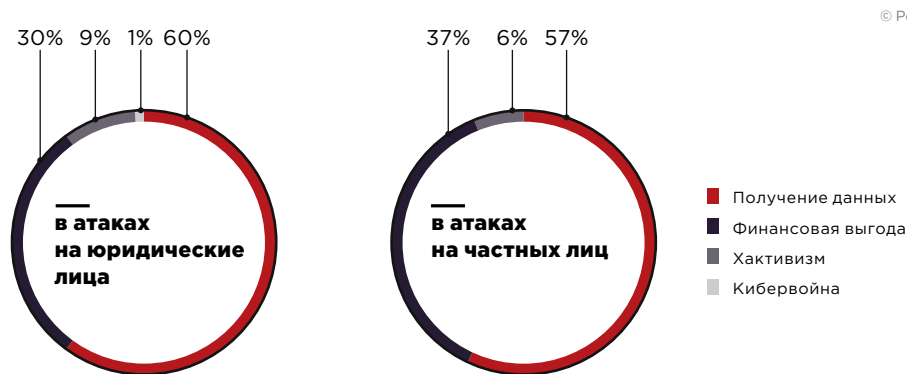


Рисунок 6. Мотивы злоумышленников

В атаках на юридические лица злоумышленников прежде всего интересовали персональные данные. Значительную долю похищенной в ходе кибератак информации составили учетные данные: 22% для юридических лиц и 40% для частных. Логины и пароли — ключи для доступа к закрытым системам, и злоумышленники старались открыть с их помощью как можно больше замков. На протяжении года мы неоднократно отмечали кибератаки, в ходе которых скомпрометированные базы учетных данных одних компаний использовались для доступа к системам других. Такой тип атак называют *credential stuffing*. Примеры жертв в 2019 году — американская группа финансовых компаний *State Farm*, сеть кофеен *Dunkin' Donuts*, японские интернет-магазины *UNIQLO* и *GU*. По нашему мнению, одной из причин успеха атак методом *credential stuffing* могла стать опубликованная в начале года база данных *Collection #1*, включающая более миллиарда уникальных пар логинов и паролей.

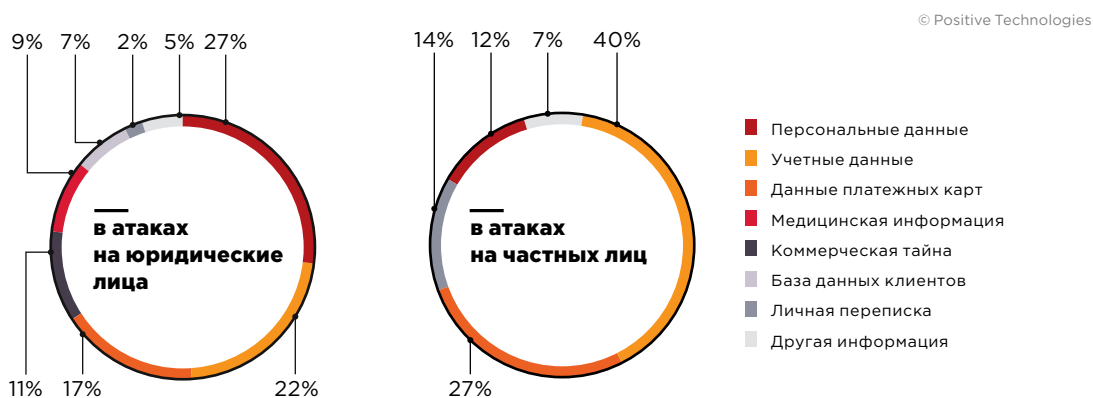


Рисунок 7. Типы украденных данных



## Вредоносное ПО развивается семимильными шагами

В 2019 году число заражений вредоносным ПО выросло на 38% по сравнению с 2018 годом. В 41% случаев заражения вредоносным ПО сочетались с методами социальной инженерии.

Росту успеха вредоносных кампаний в течение года способствовала непрерывная модернизация как самого ВПО, так и способов его доставки. Во-первых, в 2019 году злоумышленники хорошо маскировали зловредов. Например, скрывали их в файлах с расширениями, которые включены в белые списки и потому не детектируются антивирусами, использовали легитимные процессы и встроенные механизмы, чтобы избежать обнаружения, подписывали вредоносное ПО с помощью легитимных сертификатов, активно развивали бесфайловые техники заражений. Исследователи Trend Micro в сентябре 2019 года опубликовали отчет, согласно которому число бесфайловых атак в первой половине года выросло на 265% по сравнению с первой половиной 2018 года. В конце года специалисты Bitdefender рассказали о новой технике заражений майнерами, шифровальщиками и шпионским ПО через особенности работы службы RDP. Во-вторых, киберпреступники добавляли в ВПО новые эксплойты для уязвимостей, в том числе в широко используемом ПО. Например, нашедшая в 2019 году уязвимость в WinRAR, затронувшая полмиллиарда пользователей, использовалась как для заражений шифровальщиком JNEC.a, так и в сложных целенаправленных атаках. Наконец, злоумышленники старались сделать ВПО многофункциональным, что повышало их шансы на получение выгоды в случае заражения. Так, новый руткит Scranos похищает учетные и платежные данные, устанавливает рекламное ПО и подписывает на YouTube-каналы.

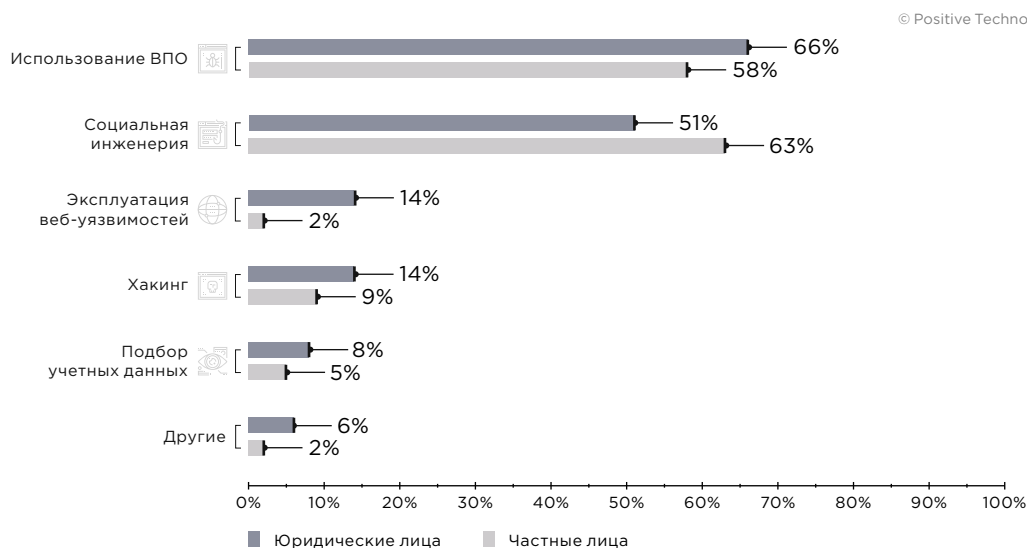


Рисунок 8. Методы атак

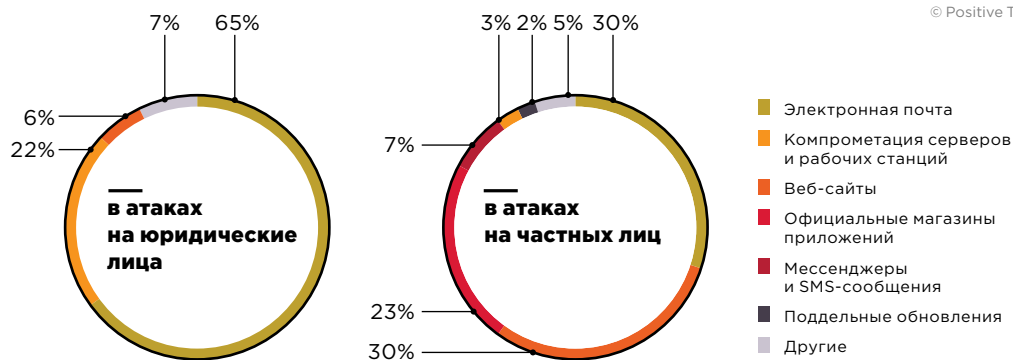


Рисунок 9. Способы распространения ВПО

## Шифровальщики наступают

В атаках на юридические лица 31% заражений ВПО пришлось на долю троянов-шифровальщиков. В течение года жертвами стали десятки городов, школ и университетов, медицинских центров, промышленных предприятий, IT-компаний. Основные векторы заражений — фишинговые письма, эксплуатация уязвимостей в ПО, атаки через RDP. Пик заражений среди государственных учреждений пришелся на первую половину года. Во втором полугодии наблюдался всплеск атак шифровальщиков на IT-компании и сферу образования. Многие жертвы предпочли заплатить выкуп, который в среднем составлял несколько сотен тысяч долларов. Осенью Федеральное бюро расследований США опубликовало заявление с рекомендациями по защите и призывом не платить вымогателям.

В первой половине 2019 года одними из наиболее активных по числу заражений были операторы шифровальщика GandCrab. В конце весны владельцы GandCrab заявили, что выходят из преступного бизнеса. С апреля начали появляться первые сообщения об атаках нового шифровальщика Sodinokibi (он же REvil). Технический анализ Sodinokibi выявил много сходств с криптовымогателем GandCrab. Осенью неизвестные злоумышленники, стоящие за атаками Sodinokibi, на одном из форумов в дарквебе заявили, что приобрели исходные коды GandCrab, адаптировали их под свои нужды и готовятся к новым атакам.

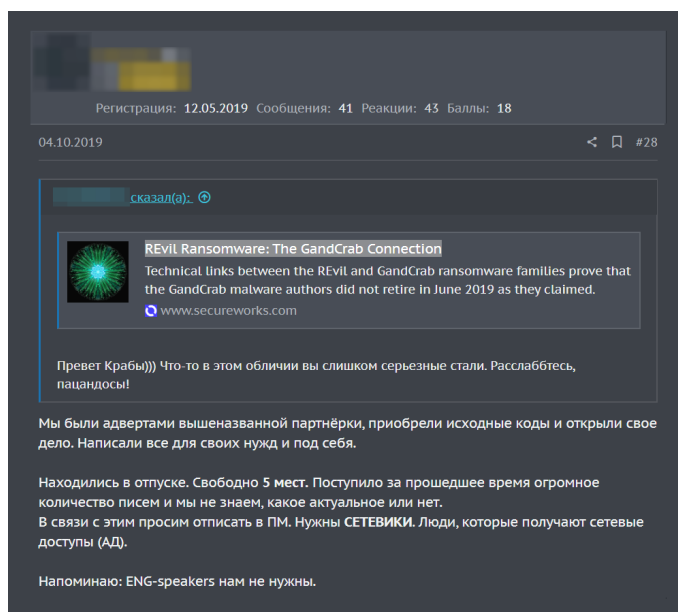


Рисунок 10. Связь GandCrab и Sodinokibi

С ноября операторы шифровальщиков начали шантажировать жертв публикацией данных, которые они скопировали перед тем, как зашифровать их. На конец 2019 года такие кампании проводили операторы шифровальщиков Maze и вышеупомянутого Sodinokibi. Возможная связь последнего с нашумевшим GandCrab, предыдущие владельцы которого, по их словам, заработали на выкупах два миллиарда долларов, позволяет сделать предположение, что в 2020 году нас ожидает новая волна атак шифровальщиков, а возникшая в конце года тенденция к публикации файлов жертв, отказавшихся платить выкуп, получит развитие.

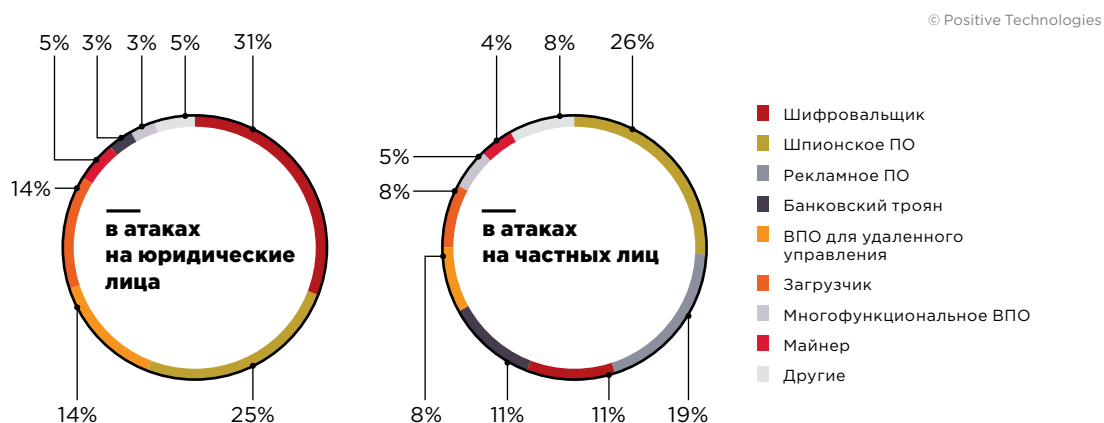


Рисунок 11. Типы вредоносного ПО

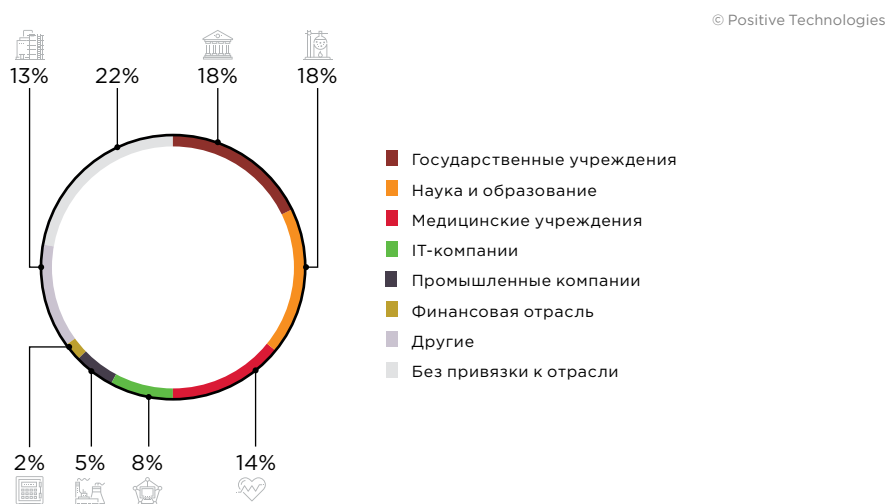


Рисунок 12. Категории жертв шифровальщиков среди юридических лиц

## Опасные уязвимости

Перечислим несколько уязвимостей ПО, которые были выявлены в 2019 году и обратили на себя внимание мирового сообщества специалистов в области ИБ из-за критического уровня риска и большого числа потенциальных жертв. Уязвимость представляет особую опасность, если для ее эксплуатации был разработан и опубликован эксплойт.

### Кнопка «Взломать интернет»

- Идентификатор: [CVE-2019-19781](#)
- Дата публикации: декабрь 2019 года
- Уязвимое ПО: Citrix Application Delivery Controller (NetScaler ADC) и Citrix Gateway (NetScaler Gateway)
- Уровень риска: критический
- Эксплойт: [есть](#)

Уязвимость, связанная с возможностью удаленного выполнения кода без авторизации. Брешь позволяет внешнему злоумышленнику не только получить доступ к опубликованным приложениям, но и проводить атаки с сервера Citrix на другие ресурсы внутренней сети атакуемой компании. Согласно [нашим данным](#), по состоянию на 2019 год под угрозой находились порядка 80 тысяч компаний. Мы полагаем, что в 2020 году уязвимость может активно эксплуатироваться в кибератаках на компании, которые не выполнили [комплекс мер защиты, разработанный Citrix](#).

### Next day, NextCry

- Идентификатор: [CVE-2019-11043](#)
- Дата публикации: октябрь 2019 года
- Уязвимое ПО: PHP-FPM
- Уровень риска: критический
- Эксплойт: [есть](#)

Уязвимость в PHP 7 позволяет неавторизованному пользователю выполнять произвольный код. Под угрозой серверы nginx с включенным FPM (пакет для обработки сценариев на языке PHP). Брешь стала причиной заражения пользователей облачного хранилища NextCloud [шифровальщиком NextCry](#).

### BlueKeep

- Идентификатор: [CVE-2019-0708](#) (BlueKeep)
- Дата публикации: май 2019 года
- Уязвимое ПО: Microsoft Windows Remote Desktop Services
- Уровень риска: критический
- Эксплойт: есть несколько, в том числе в виде модуля для Metasploit

Уязвимость в реализации протокола RDP, затронувшая некоторые версии Windows, позволяет неавторизованному пользователю выполнять произвольный код, в частности распространять вредоносное ПО. Под серьезной угрозой оказались Windows Server 2008, Windows 7, Windows 2003 и Windows XP. Уязвимость потенциально могла стать причиной вредоносных эпидемий наподобие WannaCry, NotPetya и Bad Rabbit, однако этого удалось избежать. В течение года специалисты по кибербезопасности регулярно фиксировали [попытки эксплуатации BlueKeep](#), но кроме несанкционированной установки майнеров других последствий критически опасной бреши в RDP в 2019 году не обнаружено.

Вслед за BlueKeep в реализации RDP были выявлены еще две похожие уязвимости ([CVE-2019-1181](#) и [CVE-2019-1182](#)), патчи для которых выпущены в августе. Как и CVE-2019-0708, эти бреши относятся к типу wormable, то есть позволяют распространять ВПО без участия пользователей. В отличие от BlueKeep, уязвимости затронули более поздние версии Windows, включая версию 10.

## Держа руку на Pulse

- Идентификатор: [CVE-2019-11510](#)
- Дата публикации: апрель 2019 года
- Уязвимое ПО: Pulse Secure Pulse Connect Secure (PCS)
- Уровень риска: критический
- Эксплойт: [есть](#)

Уязвимость в популярном решении для VPN компании Pulse Secure позволяет неавторизованному пользователю читать произвольные файлы, включая чувствительную конфигурационную информацию, отправляя на сервер специально сформированные HTTP-запросы. По [сообщениям ФБР](#), в августе 2019 года киберпреступники, используя эту уязвимость, проникли в сети муниципального и финансового учреждений в США. Предполагается, что через эту же брешь [злоумышленники взломали](#) инфраструктуру финансовой организации Travelex и заразили ее шифровальщиком Sodinokibi. Кроме того, в августе на эксплуатацию этой и еще одной опасной уязвимости ([CVE-2018-13379](#)) в продукте Fortinet были направлены [действия группы APT5 \(Manganesa\)](#) против телекоммуникационных и технологических компаний.

## Эпидемия MageCart

Ежеквартально мы сообщали читателям о громких атаках MageCart. Так называют атаки, в ходе которых на страницы онлайн-оплаты внедряются сценарии на языке JavaScript (JavaScript-снифферы) для хищения данных платежных карт, а также группы злоумышленников, стоящих за этими действиями. Первые случаи зафиксированы еще девять лет назад, однако в 2019 году мы наблюдали бум таких атак. Жертвами стали интернет-магазины по продаже продукции легкой и пищевой промышленности, сфера услуг, образовательные учреждения, СМИ. Массовое распространение JavaScript-снифферов обусловлено атаками [supply chain](#). На протяжении года вредоносные скрипты попадали на сайты жертв через [стороннее программное обеспечение](#) для добавления функциональности или оптимизации, например через рекламные платформы, системы управления контентом, сервисы веб-аналитики. В первой половине года злоумышленники [искали уязвимые хранилища Amazon S3](#) и, получив к ним доступ, внедряли снифферы в уже имеющиеся в хранилище JavaScript-файлы. Жертвами этой кампании стали 17 тысяч сайтов. Во второй половине года злоумышленники [внедрили сниффер](#) в JavaScript-библиотеку, поставляемую платформой для электронной коммерции Volusion. По [данным компании RiskIQ](#), в 2019 году инфраструктура злоумышленников, стоящих за атаками MageCart, насчитывала около 600 доменов; среднее время присутствия на сайте жертвы — 22 дня.



## Методы атак

Приведем основные сведения по распространенным методам атак, которые использовались киберпреступниками в 2019 году.

### Использование ВПО

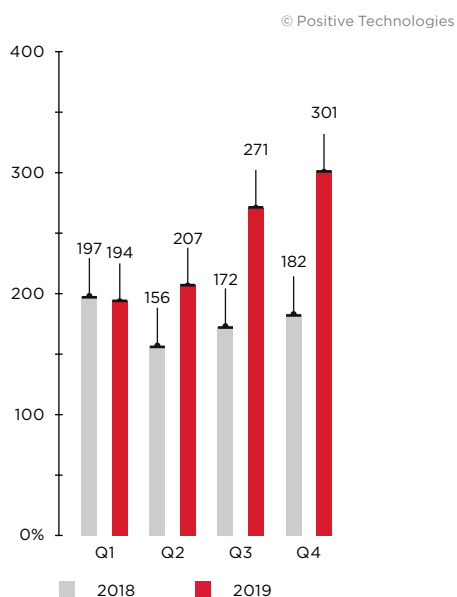


Рисунок 13. Количество атак

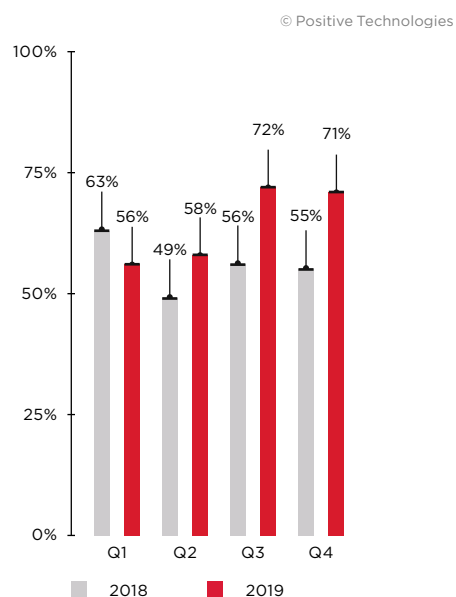


Рисунок 14. Доля атак

### Социальная инженерия

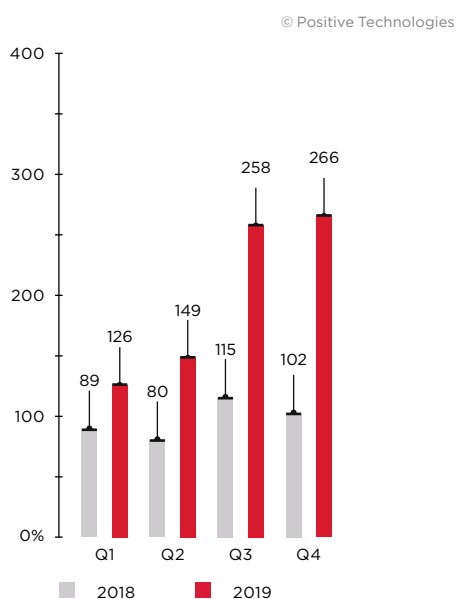


Рисунок 15. Количество атак

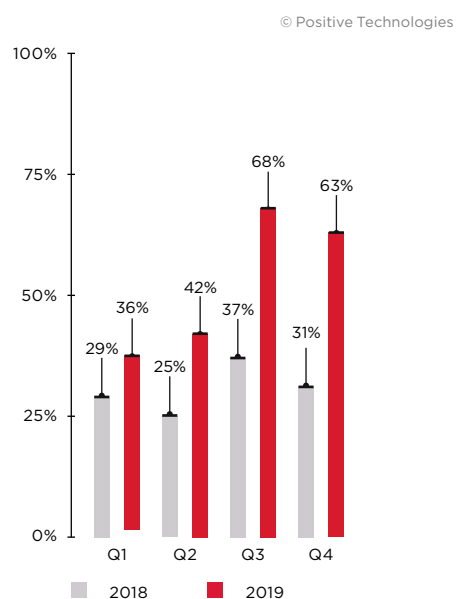


Рисунок 16. Доля атак

## Эксплуатация веб-уязвимостей

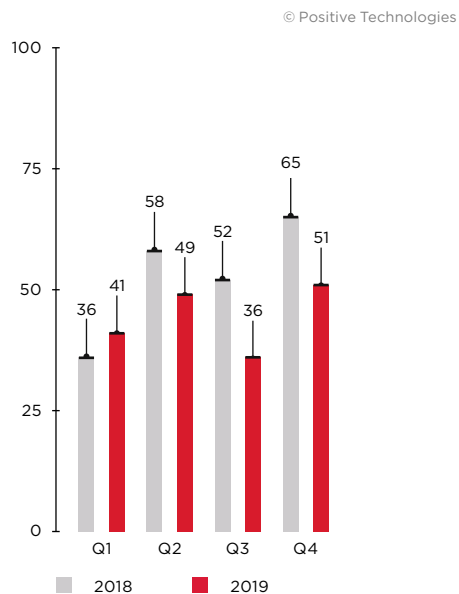


Рисунок 17. Количество атак

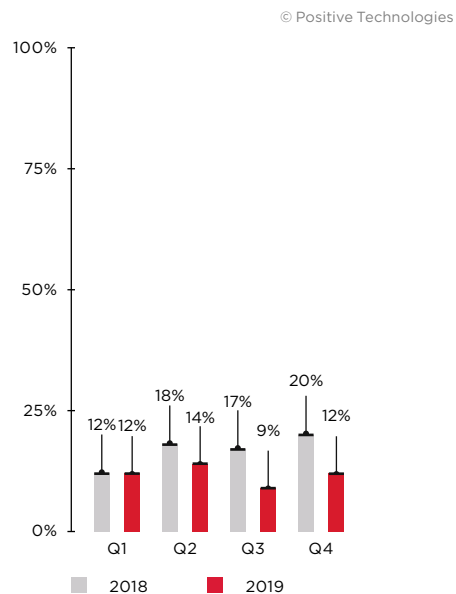


Рисунок 18. Доля атак

## Использование уязвимостей ПО и недостатков механизмов защиты

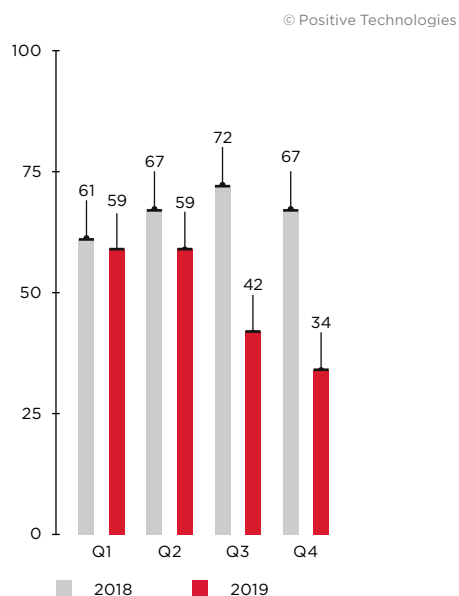


Рисунок 19. Количество атак

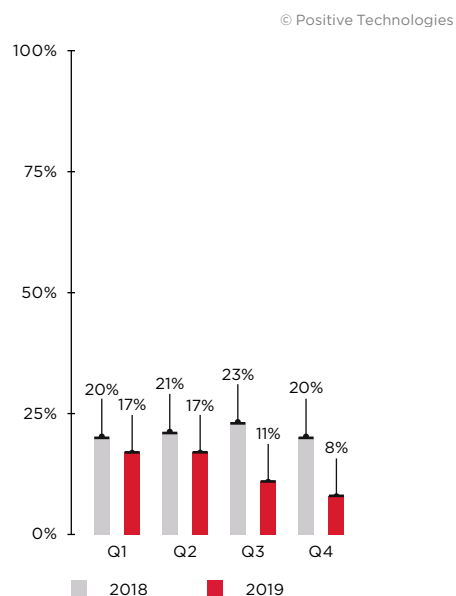


Рисунок 20. Доля атак

## Подбор учетных данных

© Positive Technologies

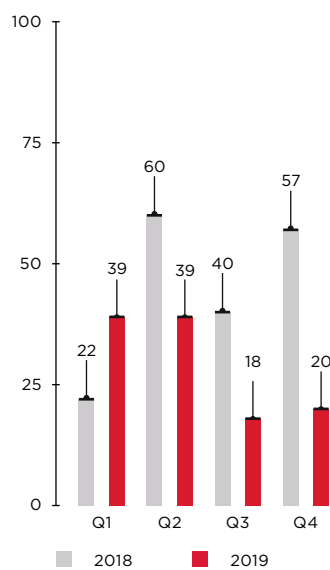


Рисунок 21. Количество атак

© Positive Technologies

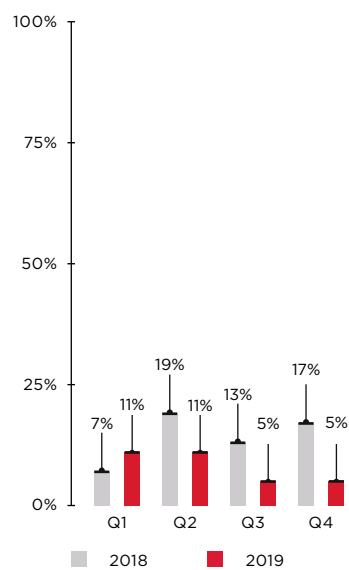


Рисунок 22. Доля атак

## Категории жертв: государственные организации

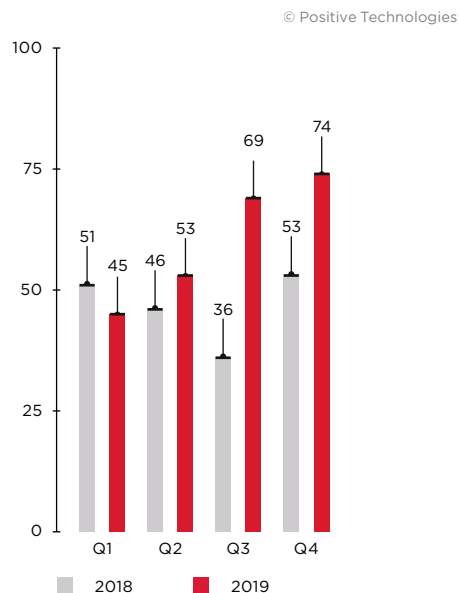


Рисунок 23. Число атак на государственные организации

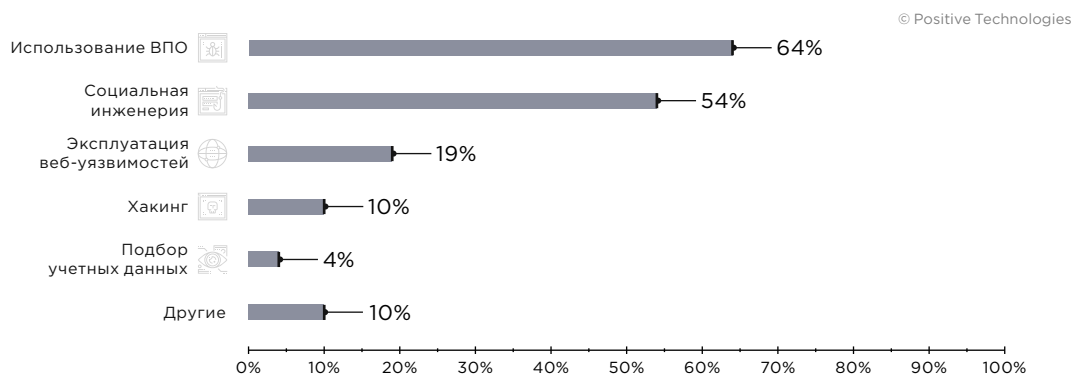


Рисунок 24. Методы атак на государственные организации

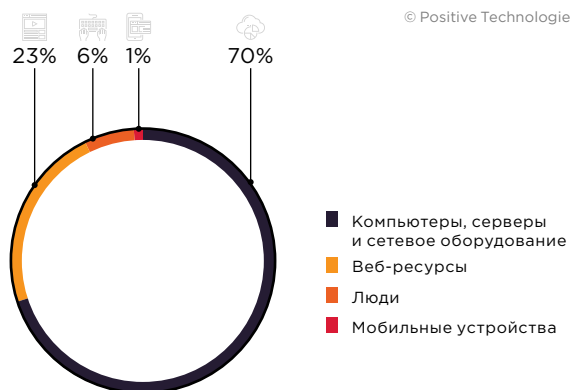


Рисунок 25. Объекты атак

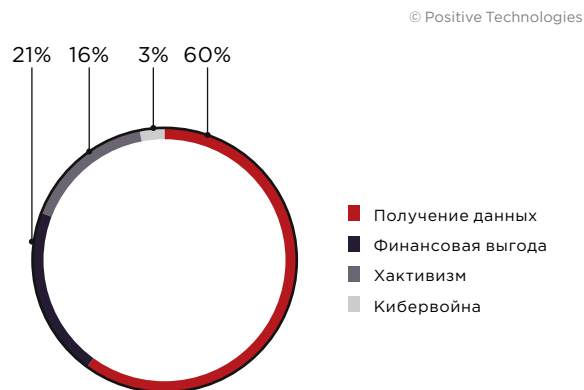


Рисунок 26. Мотивы атак

## Категории жертв: промышленные компании

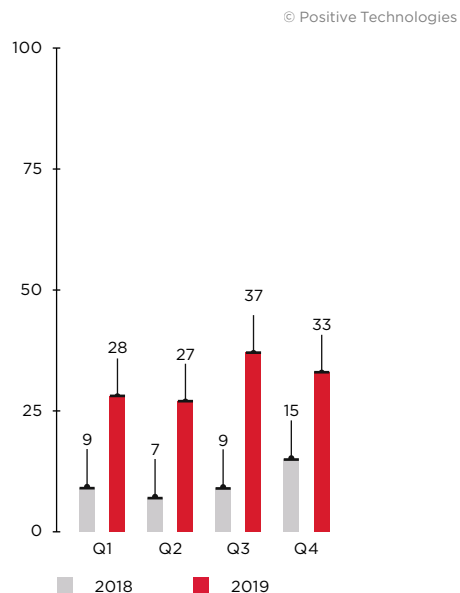


Рисунок 27. Число атак на промышленные компании

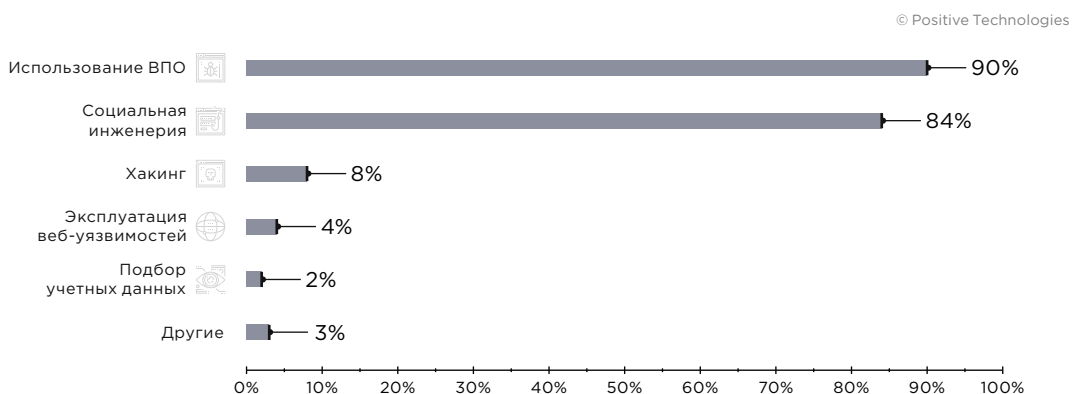


Рисунок 28. Методы атак на промышленные компании

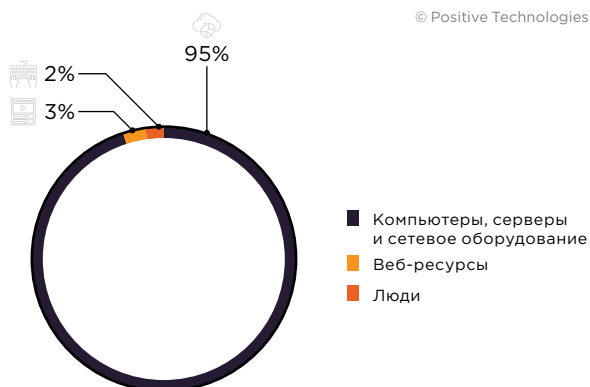


Рисунок 29. Объекты атак

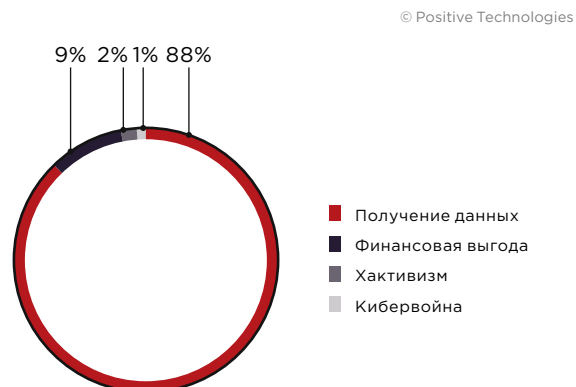


Рисунок 30. Мотивы атак



## Категории жертв: финансовые организации

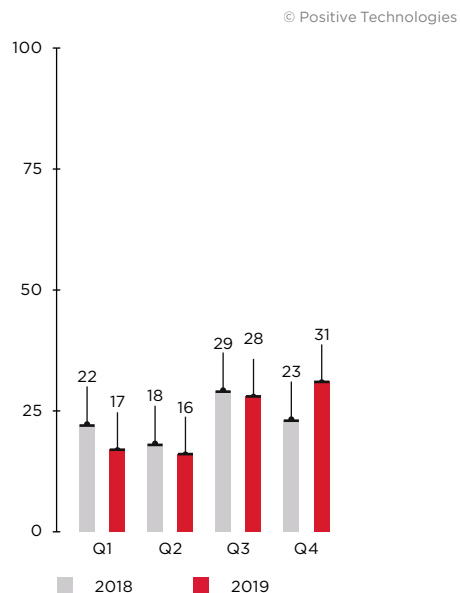


Рисунок 31. Число атак на финансовые организации

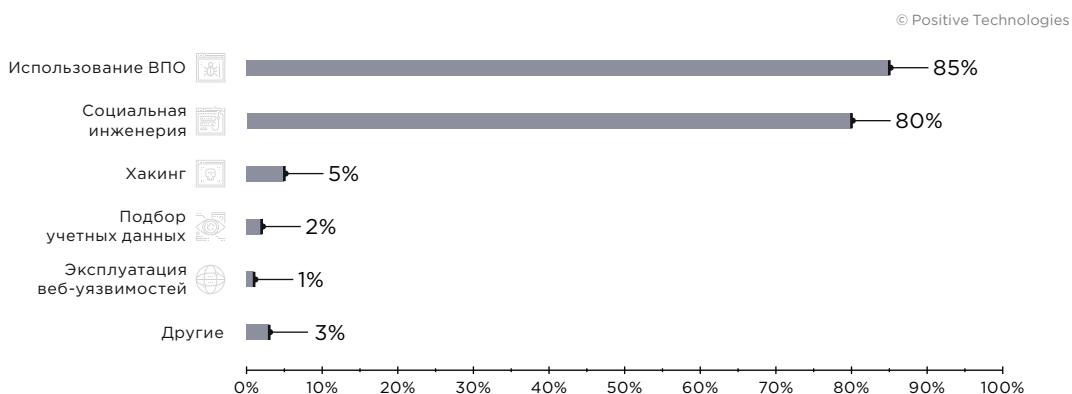


Рисунок 32. Методы атак на финансовые организации

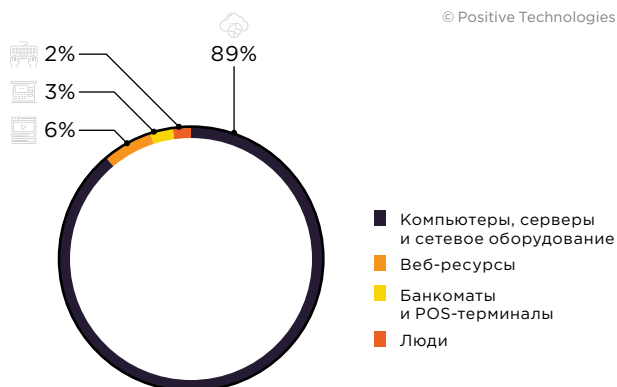


Рисунок 33. Объекты атак

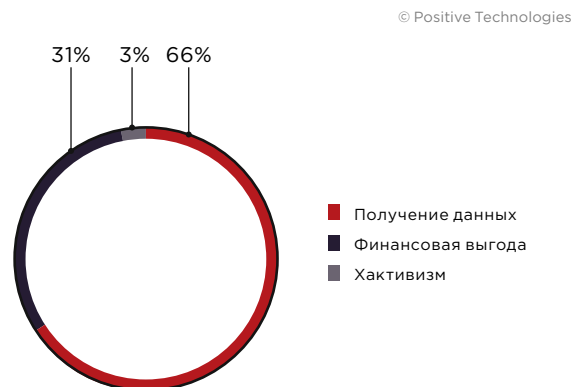


Рисунок 34. Мотивы атак

## Категории жертв: IT-компании

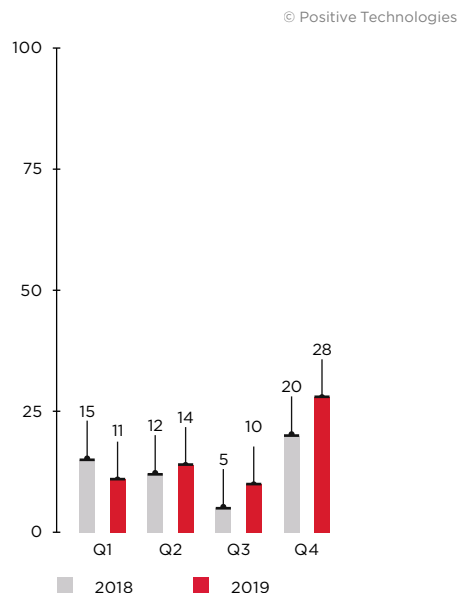


Рисунок 35. Число атак на IT-компании

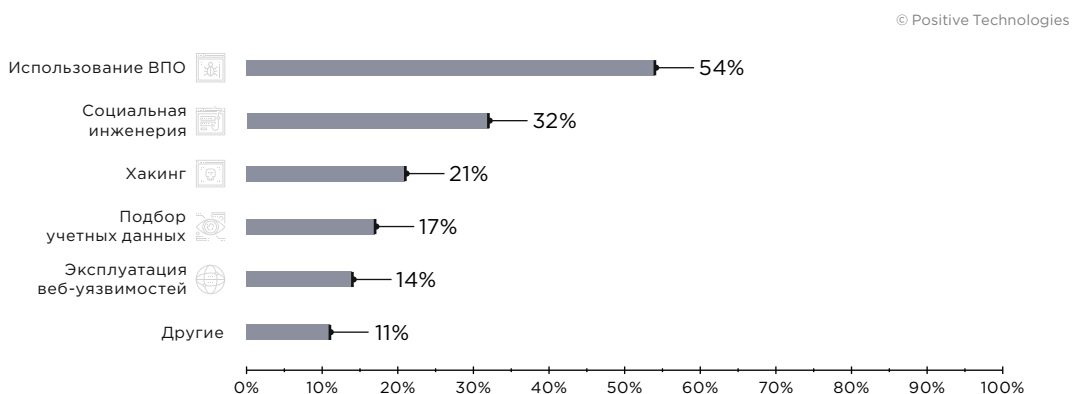


Рисунок 36. Методы атак на IT-компании

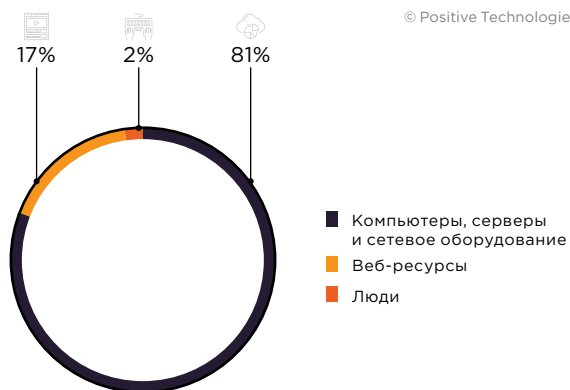


Рисунок 37. Объекты атак

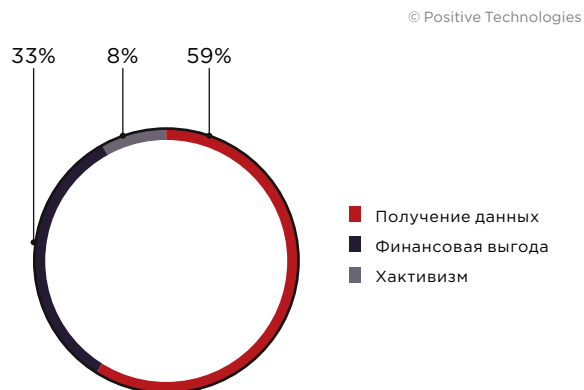


Рисунок 38. Мотивы атак

## 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 firewalls) — 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.

## Г 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.

## Г 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.

## Г 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).

## **Г** 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

### Г Не экономьте на безопасности:

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

### Г 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.

### Г 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.

### Г 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 отчета каждый массовый инцидент (например, вирусная атака, в ходе которой злоумышленники проводят многоадресные фишинговые рассылки) рассматривается как одна уникальная угроза информационной безопасности. В исследовании мы используем следующие термины:

**Киберугроза** — это совокупность факторов и условий, создающих опасность нарушения информационной безопасности. В нашем исследовании мы рассматриваем киберугрозы с точки зрения действий злоумышленников в киберпространстве, направленных на проникновение в информационную систему с целью кражи данных, денежных средств или с иными намерениями, которые потенциально ведут к негативным последствиям для государства, бизнеса или частных лиц. Действия злоумышленников могут быть направлены на IT-инфраструктуру компании, рабочие компьютеры, мобильные устройства, другие технические средства и, наконец, на человека как на элемент киберпространства.

**Кибератака** — несанкционированное воздействие на информационные системы со стороны киберпреступников с использованием технических средств и программного обеспечения с целью получения доступа к информационным ресурсам, нарушения нормальной работы или доступности систем, кражи, искажения или удаления информации.

**Объект атаки** — объект несанкционированного воздействия со стороны киберпреступников. Если методы социальной инженерии направлены на получение информации непосредственно от частного лица, клиента или сотрудника компании, то объектом атаки является категория «Люди». Если же методы социальной инженерии применяются с целью доставки ВПО в инфраструктуру компании или на компьютер частного лица, то в качестве объекта атаки выбирается категория «Компьютеры, серверы и сетевое оборудование».

**Мотив атаки** — первостепенная цель киберпреступников. Например, если в результате атаки похищены данные платежных карт, мотивом в этом случае является получение данных.

**Метод 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 (консалтинговые организации, гостиницы, рестораны и др.). 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 для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. Данное исследование проводится с целью обратить внимание организаций и обычных граждан, интересующихся современным состоянием информационной безопасности, на наиболее актуальные методы и мотивы кибератак, а также с целью выявить основные тенденции в изменении ландшафта киберугроз.

## О компании

[ptsecurity.com](https://ptsecurity.com)  
[pt@ptsecurity.com](mailto:pt@ptsecurity.com)  
[facebook.com/PositiveTechnologies](https://facebook.com/PositiveTechnologies)  
[facebook.com/PHDays](https://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.