



POSITIVE TECHNOLOGIES

# **Актуальные киберугрозы — 2018**

Тренды и прогнозы



## Содержание

Обозначения.....	2
Тренды.....	3
Общая статистика.....	4
Категории жертв .....	7
Государственные учреждения.....	8
Медицинские учреждения.....	9
Финансовая отрасль .....	10
Сфера образования.....	11
IT-компании .....	12
Торговля .....	13
Промышленные компании .....	14
Сфера услуг.....	15
Частные лица.....	16
Методы атак .....	17
Использование вредоносного ПО .....	17
Социальная инженерия.....	18
Хакинг .....	18
Эксплуатация веб-уязвимостей .....	19
Подбор учетных данных.....	19
DDoS.....	20
Прогнозы .....	20

## 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



Использование легального ПО

### Категории жертв



Финансовая отрасль



Государственные учреждения



Медицинские учреждения



Сфера образования



Промышленные компании



Онлайн-сервисы



Сфера услуг



Транспорт



IT-компании



Торговля



Частные лица



Телекоммуникационные компании



Криптовалютные биржи



Другие сферы

## Тренды

Компания Positive Technologies продолжает следить за актуальными угрозами информационной безопасности. В этом отчете мы подводим итоги 2018 года и делимся своими прогнозами на 2019 год.

### Главные тенденции 2018 года:

- Преобладают целенаправленные атаки, доля которых увеличивалась на протяжении всего года и в четвертом квартале составила 62%.
- Растет доля атак, направленных на кражу информации. Злоумышленники похищают преимущественно персональные данные (30%), учетные данные (24%) и данные платежных карт (14%).
- В 2018 году внимание преступников привлекли медицинские учреждения в США и Европе: по количеству атак они опередили даже финансовые организации. Хакеров интересует как медицинская информация, так и возможность получить выкуп за восстановление работоспособности компьютерных систем: медучреждения легче соглашаются заплатить хакерам, поскольку от этого могут зависеть жизнь и здоровье людей.
- Вредоносное ПО используется уже в 56% кибератак. Этому способствует тот факт, что вредоносные программы с каждым годом становятся более доступными, и соответственно, снижается порог входа в киберпреступный бизнес.
- Наиболее популярным стало ПО для шпионажа и удаленного управления, с помощью которого преступники собирают конфиденциальную информацию или, в случае целенаправленной атаки, закрепляются в системе.
- Доля майнеров в общем числе заражений вредоносным ПО уменьшается на фоне общего снижения курсов криптовалют и повышения сложности их добычи. Если в первом квартале года доля майнеров составляла 23%, то по итогам четвертого квартала — всего 9%.
- Преступники все чаще прибегают к сложным и многоэтапным техникам, включающим в себя взлом инфраструктуры компаний-партнеров, заражение ресурсов известных производителей ПО или комбинацию нескольких методов в рамках одной атаки.
- Существенно возросла роль социальной инженерии как в атаках на организации, так и в отношении частных лиц. Преступники используют всевозможные каналы связи — электронную почту, мессенджеры, телефонные звонки, SMS-сообщения и даже обычную почту.
- Мощность DDoS-атак продолжает расти. В 2018 году были зафиксированы две самые крупные DDoS-атаки в истории — мощностью 1,35 и 1,7 терабит в секунду. Такие результаты были достигнуты усилением атак с помощью серверов memcached.
- Грань между киберпреступлениями и другими видами преступной деятельности постепенно размывается. Большая часть инцидентов связана не непосредственно с кражей денег, а только с похищением различной информации, что свидетельствует о том, что взлом компьютерных систем может являться лишь подготовительным этапом в будущих крупных мошеннических схемах или инструментом в кибервойне. Украденные сведения могут быть использованы как против частных лиц, к примеру для оформления кредитов на чужое имя, получения бесплатных медицинских услуг или дорогостоящих медикаментов, так и против организаций и даже государств — например, с целью присвоения чужих технологий и разработок.

## Общая статистика

Большинство атак в 2018 году предсказуемо совершалось с целью обогащения или получения конфиденциальных данных. При этом атаки, направленные на получение информации, зачастую также содержат финансовый подтекст: украденные данные затем используются для кражи денег, шантажа или размещаются для продажи на теневом рынке.

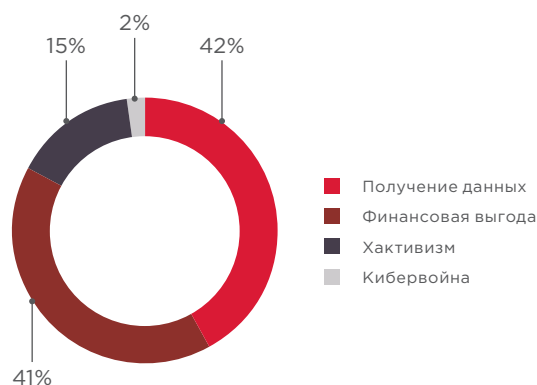


Рисунок 1. Мотивы злоумышленников

В отличие от прошлого года большую часть (55%) составили целенаправленные атаки; их доля постепенно увеличивалась из квартала в квартал.

Мы рассматриваем только уникальные события, поэтому за единичную атаку принимается вредоносная кампания в целом, а не отдельный инцидент. В рамках одной кампании может произойти множество схожих инцидентов, например миллионы случаев заражения одним шифровальщиком, которые будут учтены как одна масштабная атака.

Почти четверть атак (23%) затронули частных лиц. Среди юридических лиц в 19% инцидентов жертвами хакеров стали государственные учреждения, еще в 11% случаев пострадали медицинские учреждения, а в 10% — финансовые организации. Если атака была массовой и затрагивала компании из различных сфер, мы относили ее к категории «Без привязки к отрасли».

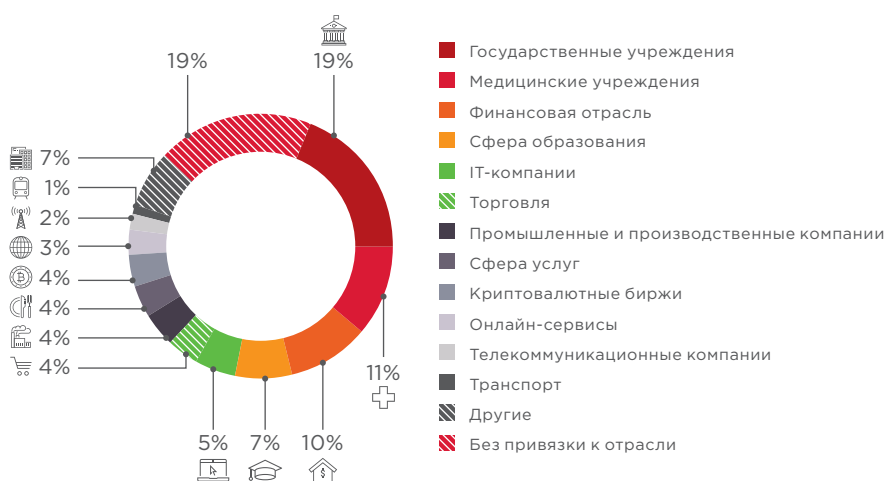


Рисунок 2. Категории жертв среди юридических лиц

В 2018 году мы зафиксировали на 27% больше уникальных инцидентов, чем годом ранее. При этом не наблюдалось значимых спадов активности. Мы выявили пики в некоторые отрезки года, например в феврале, мае, июле и в конце года, что связываем со всплесками атак злоумышленников в преддверии и во время крупных спортивных соревнований (зимних Олимпийских игр и чемпионата мира по футболу), а также с предновогодним периодом, когда финансовая активность и организаций, и частных лиц повышается.

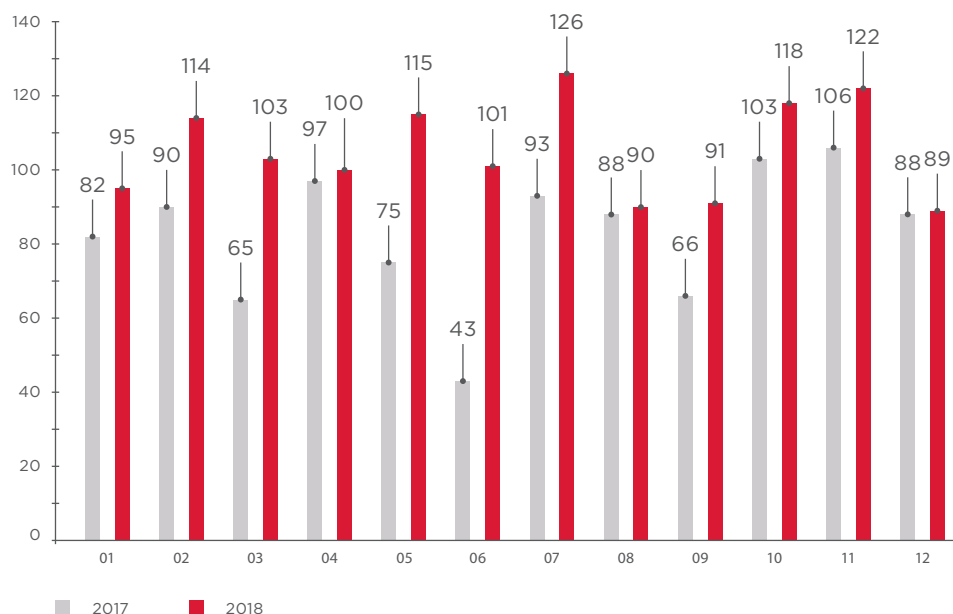


Рисунок 3. Количество инцидентов в 2017 и 2018 годах (по месяцам)

Соотношение атакуемых объектов практически не изменилось. Чаще всего злоумышленники атаковали инфраструктуру и веб-ресурсы компаний: это 49% и 26% атак соответственно. Доля атак на банкоматы и POS-терминалы за год сократилась с 3% до 1%.

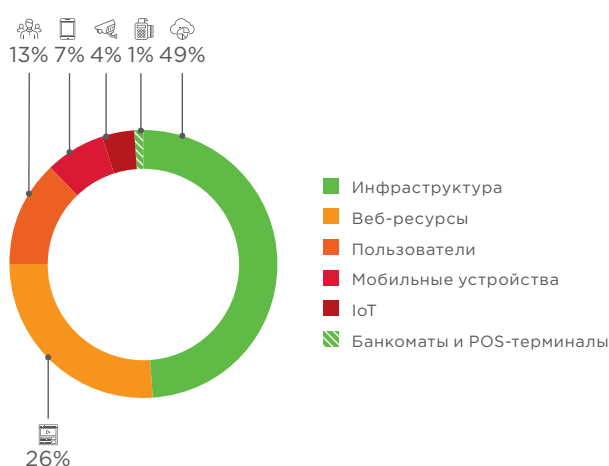


Рисунок 4. Объекты атак

Действия хакеров становятся все более хитроумными: атаки все чаще проходят в несколько этапов, в рамках которых применяются разные методы. Вредоносное ПО используется более чем в половине атак, возросла роль социальной инженерии: к ней хакеры прибегают в каждой третьей атаке. Статистические данные по каждому методу атаки приведены в конце отчета.

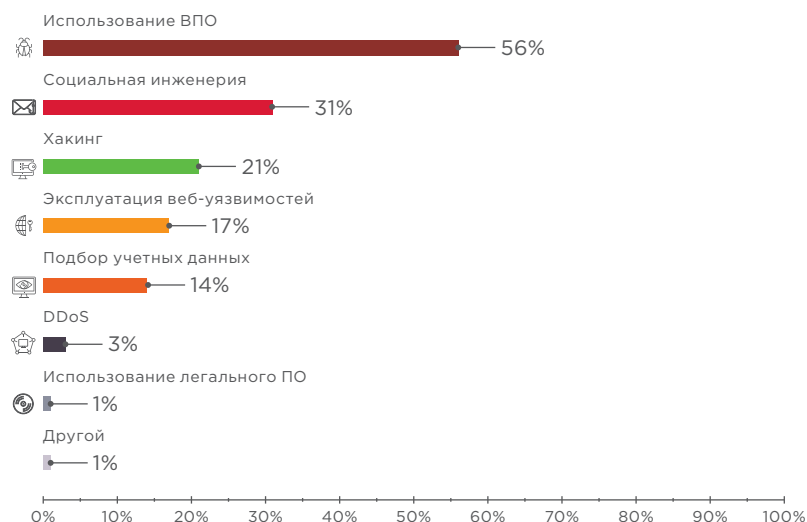


Рисунок 5. Методы атак

Рисунок 6. Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) внутри отраслей

		Отрасль														
		Государственные учреждения	Финансовая отрасль	Промышленные компании	Медицинские учреждения	Онлайн-сервисы	Сфера услуг	IT-компании	Сфера образования	Торговля	Телекоммуникационные компании	Частные лица	Транспорт	Криптовалютные биржи	Другие	Без привязки к отрасли
<b>Всего атак</b>		<b>186</b>	<b>92</b>	<b>40</b>	<b>109</b>	<b>32</b>	<b>40</b>	<b>52</b>	<b>65</b>	<b>43</b>	<b>19</b>	<b>290</b>	<b>14</b>	<b>37</b>	<b>63</b>	<b>182</b>
Объект	Инфраструктура	108	64	31	72	3	14	21	38	8	11	89	6	6	32	110
	Веб-ресурсы	57	7	6	18	25	14	24	14	27	6	52	5	27	21	27
	Пользователи	16	12	1	18	4	5	7	12	6	1	66	2	4	6	7
	Мобильные устройства	1	2	-	-	-	-	-	-	-	-	75	1	-	1	3
	Банкоматы и POS-терминалы	-	6	-	-	-	6	-	-	2	-	2	-	-	-	-
	IoT	4	1	2	1	-	1	-	1	-	1	6	-	-	3	35
Метод	Использование ВПО	100	53	26	44	10	18	16	20	17	5	212	6	3	18	159
	Социальная инженерия	60	45	9	27	5	7	5	25	4	3	124	1	6	18	47
	Подбор учетных данных	26	10	1	37	2	3	5	17	5	3	33	3	7	12	15
	Хакинг	34	33	10	16	8	9	15	9	6	8	22	2	23	16	56
	Эксплуатация веб-уязвимостей	36	5	8	13	15	10	16	8	23	6	29	3	6	17	16
	Использование легального ПО	3	-	1	-	-	-	1	-	-	2	3	-	-	1	3
	DDoS	16	3	3	-	2	-	10	3	-	2	1	-	-	2	2
	Другой	1	1	-	-	-	1	-	-	1	-	5	-	-	2	2
Мотив	Финансовая выгода	33	60	9	23	4	18	13	18	9	2	180	6	34	20	91
	Получение данных	95	28	21	80	20	20	21	32	31	14	87	6	2	25	54
	Хактивизм	44	4	6	6	8	2	18	15	3	3	19	2	1	17	36
	Кибервойна	14	-	4	-	-	-	-	-	-	-	4	-	-	1	1
Градацией цвета показана доля атак внутри одной отрасли		<div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>														
		0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%				



## КАТЕГОРИИ ЖЕРТВ

Проанализируем атаки на отдельные отрасли, которые чаще всего становились целью злоумышленников в 2018 году.





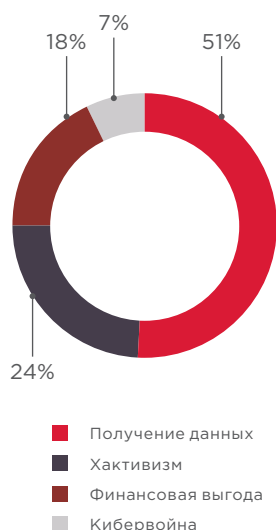


Рисунок 7. Мотивы атак

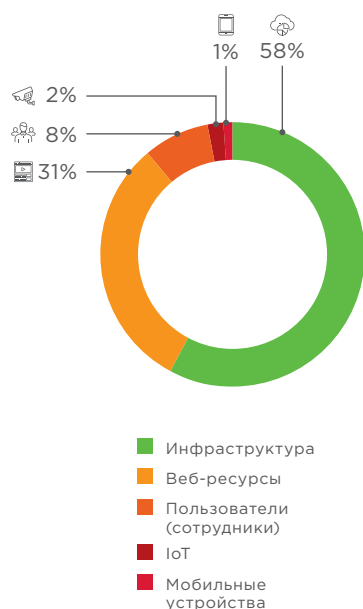


Рисунок 8. Объекты атак

## Государственные учреждения

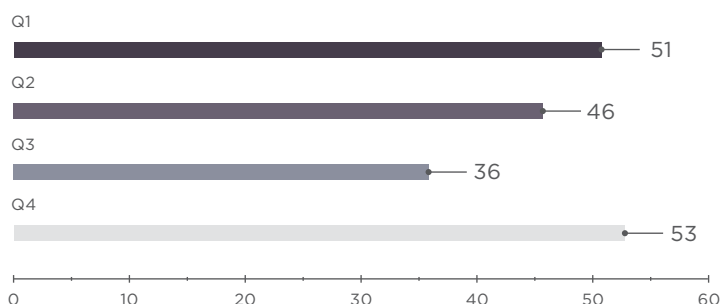


Рисунок 9. Число атак на государственные организации

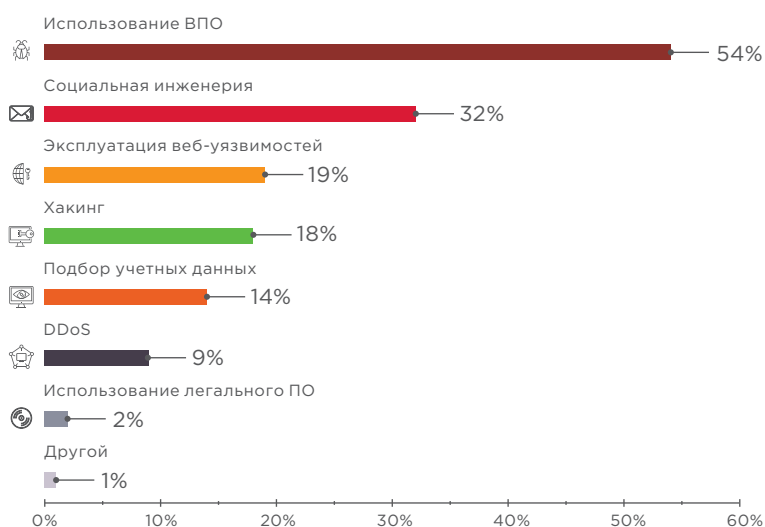


Рисунок 10. Методы атак на государственные организации

В первую очередь преступников интересовала конфиденциальная информация: получение данных было их основным мотивом в 51% случаев. Сайты государственных организаций часто используются нарушителями для привлечения внимания общественности — приблизительно четверть всех инцидентов относилась к категории «хактивизм».

В основном хакеры атаковали инфраструктуру государственных организаций и заражали компьютеры вредоносным ПО — программами для шпионажа и удаленного управления. Было также зафиксировано более 20 кампаний по заражению ресурсов госучреждений шифровальщиками.

Для внедрения в сеть организаций активно использовались методы социальной инженерии: вредоносные программы распространялись по электронной почте, через официальные магазины приложений и даже на компакт-дисках, присылаемых в конвертах по почте. Так, в первом квартале специалисты PT ESC зафиксировали фишинговые рассылки, через которые злоумышленники распространяли обновленную версию шпионского ПО SANNY и троян Fucobha, а в конце года мы отмечали активность группировок Treasure Hunters, Danti APT и SongXY, рассылающих фишинговые документы в адрес государственных организаций России и стран СНГ.

## Медицинские учреждения

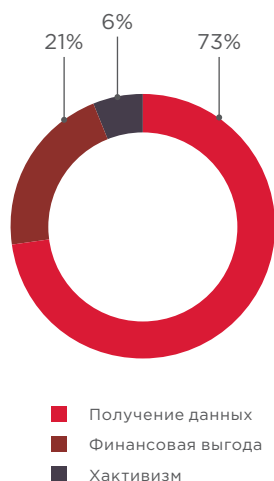


Рисунок 11. Мотивы атак

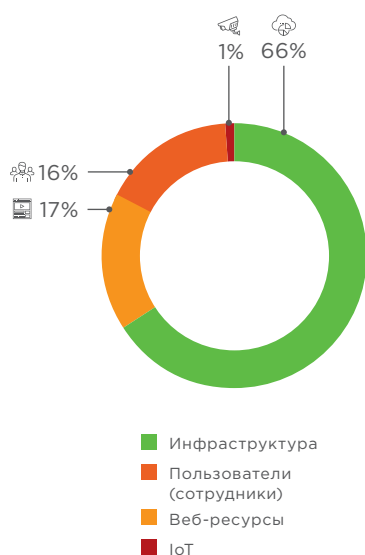


Рисунок 12. Объекты атак

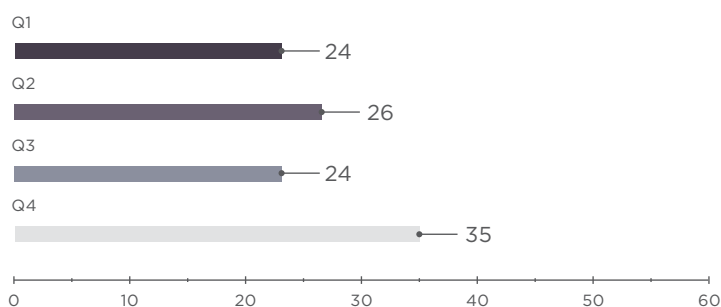


Рисунок 13. Число атак на медицинские учреждения

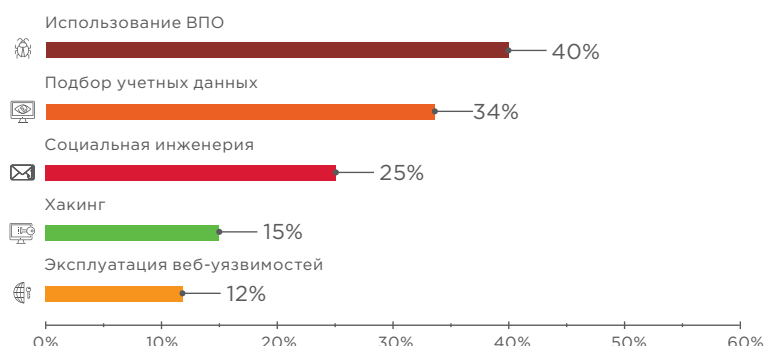


Рисунок 14. Методы атак на медицинские учреждения

В 2018 году мы зафиксировали повышенный интерес хакеров к медицинским организациям. Число атак на медучреждения даже превысило число атак на финансовые компании. В руках злоумышленников оказались персональные данные и медицинская информация более 6 млн человек.

Хакеры атакуют медицинские организации не только с целью кражи данных, но и ради непосредственной наживы, понимая, что непрерывная работа систем критически важна, когда речь идет о жизни и здоровье пациентов. Преступники проникали в инфраструктуру медицинских компаний и зашифровывали данные, требуя выкуп за восстановление работоспособности. Так, из-за действий хакеров была парализована работа компьютерных систем в американской больнице Hantock Regional, руководство которой решило заплатить вымогателям 55 тысяч долларов.

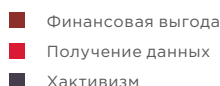
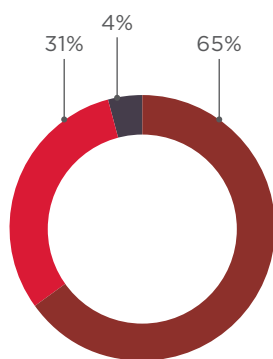


Рисунок 15. Мотивы атак

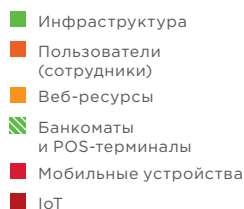
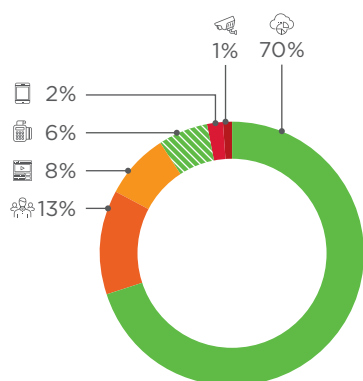


Рисунок 16. Объекты атак

## Финансовая отрасль

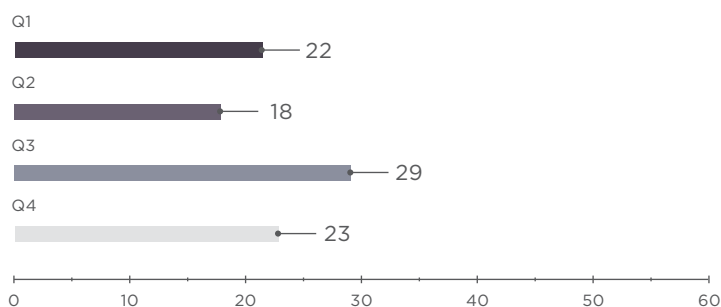


Рисунок 17. Число атак на финансовые организации

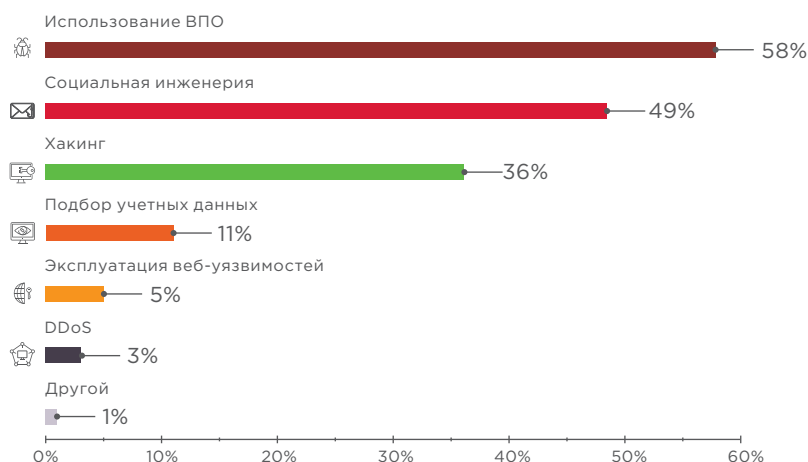


Рисунок 18. Методы атак на финансовые организации

Главным мотивом злоумышленников при проведении атак на финансовые организации очевидно является получение прямой финансовой выгоды (65% инцидентов). Тем не менее значительна и доля инцидентов, где целью было получение информации о платежных картах, персональных данных, учетных данных пользователей для доступа к личным кабинетам. Эту информацию преступники могут использовать для кражи денег со счетов клиентов или продать на теневом рынке.

В начале года в США прошла волна «джекпоттинга»: преступники устанавливали на банкоматы вредоносное ПО Ploutus-D, которое позволяло управлять выдачей наличных. Примечательно, что в арсенале преступников присутствовал медицинский эндоскоп, с помощью которого они проходили физическую аутентификацию без доступа к сейфу.

Во втором полугодии активизировались известные APT-группировки. Специалисты PT ESC зафиксировали 23 атаки, которые за этот период провела группировка Cobalt: преступники подготовили новое вредоносное ПО и, как обычно, распространяли его путем рассылки электронных писем от лица финансовых организаций.

Кроме того, эксперты PT ESC обнаружили новую кибергруппу, атакующую финансовый сектор. Эти злоумышленники также рассылали документы с макросами, которые загружали утилиты, предоставляющие удаленный доступ к зараженному компьютеру. Рассылка осуществлялась от лица ФинЦЕРТ и со скомпрометированного ящика сотрудника крупной финансовой компании. При анализе документов был обнаружен модифицированный скрипт, который ранее использовался группой *Treasure Hunters*, однако дальнейший анализ трафика и утилит позволил предположить появление новой преступной группировки.



## Сфера образования

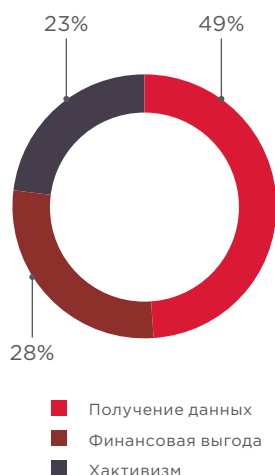


Рисунок 19. Мотивы атак

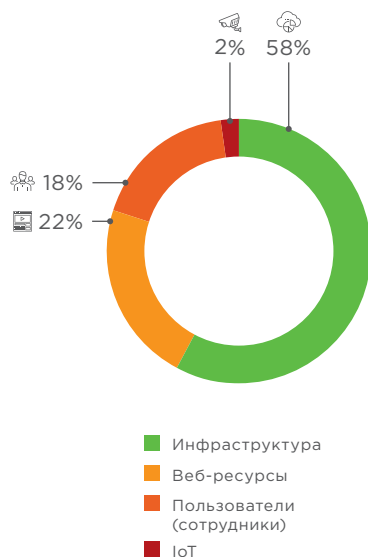


Рисунок 20. Объекты атак

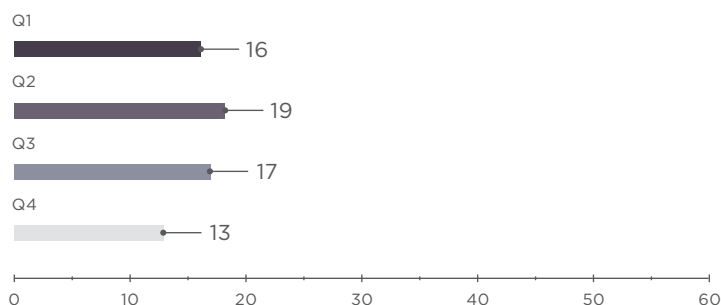


Рисунок 21. Число атак на образовательные учреждения

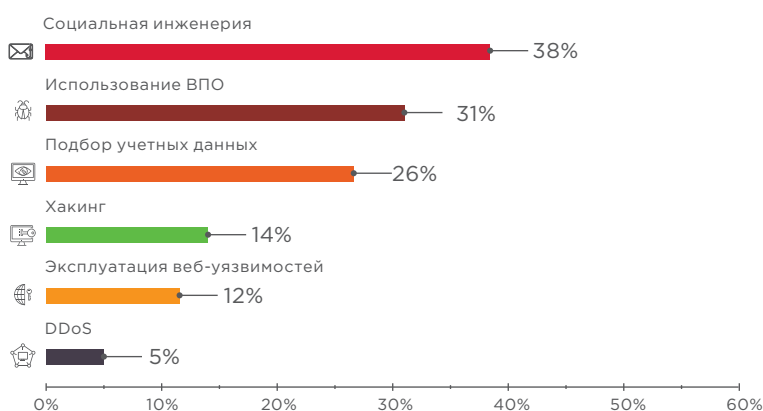


Рисунок 22. Методы атак на образовательные учреждения

В основном преступники похищали персональные данные сотрудников и учащихся, а также учетные данные для доступа к электронной почте, банковским аккаунтам и другим сервисам. Так, в нескольких учебных заведениях преступники получили доступ к банковским счетам и платежным документам и смогли похитить в общей сложности более двух миллионов долларов. Образовательные учреждения подвергались атакам шифровальщиков: они использовались в каждой шестой атаке. Мотивы преступников при этом могли быть разными — либо потребовать выкуп за восстановление данных, либо попросту парализовать работу компьютерных систем учебного заведения. Во втором квартале, на который приходится конец учебного года и подведение его итогов, чаще выявлялись атаки с целью изменения оценок в системах учета успеваемости.

В погоне за интеллектуальной собственностью — научными наработками, неопубликованными исследованиями — хакеры атаковали научные институты. Такая информация часто представляет интерес для группировок спонсируемых тем или иным правительством; ряд подобных атак приписывают хакерам из Ирана и Северной Кореи. Помимо этого, злоумышленники получают финансовую выгоду, размещая украденные научные работы на подконтрольных им ресурсах с платным доступом.

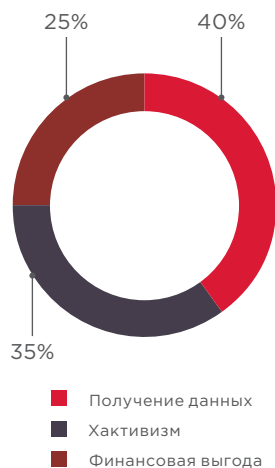


Рисунок 23. Мотивы атак

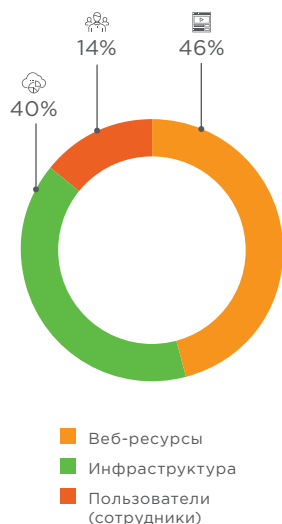


Рисунок 24. Объекты атак

## IT-компании

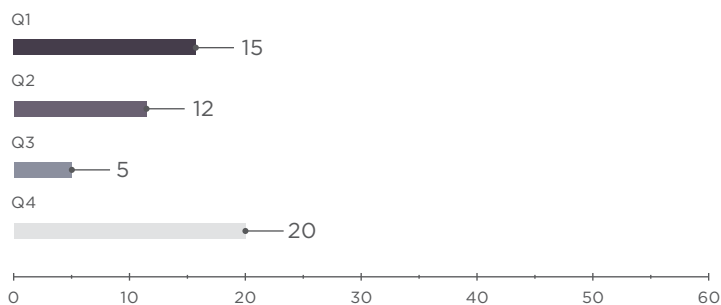


Рисунок 25. Число атак на IT-компании

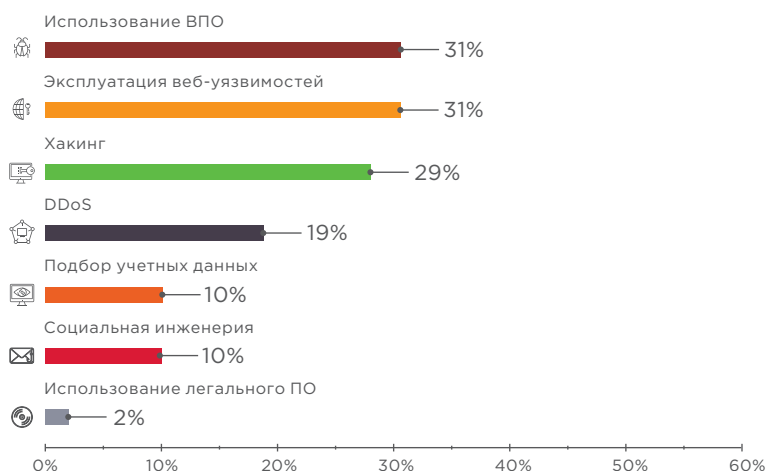


Рисунок 26. Методы атак на IT-компании

Объектами атак злоумышленников стали веб-ресурсы и инфраструктура IT-компаний. Часто взлом IT-компаний является лишь промежуточным звеном в более сложной атаке. На серверах может храниться значимая информация о клиентах, а в случае атаки на провайдера услуг — данные других компаний, в том числе их веб-сайты. Хакеров интересует и доступ к электронной почте сотрудников: ее можно использовать для фишинговых рассылок. Кроме того, ресурсы известных производителей ПО становятся удачной площадкой для распространения вредоносных программ под видом официальных обновлений.

Во втором квартале эксперты PT ESC выявили фишинговую атаку, нацеленную на крупную IT-компанию. Через электронную почту распространялся троян PlugX, который уже несколько лет используется злоумышленниками в атаках с целью шпионажа.

IT-компании чаще остальных (за исключением государственных учреждений) подвергались DDoS-атакам: хакерам удавалось приостановить работу интернет-провайдеров, владельцев игровых серверов — то есть тех компаний, которые особенно чувствительны к потере связи и перебоям в функционировании оборудования.

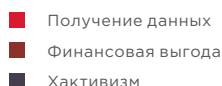
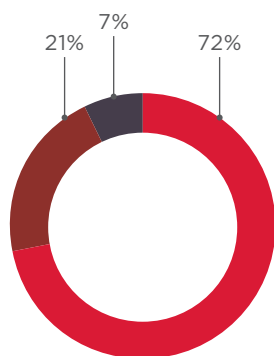


Рисунок 27. Мотивы атак

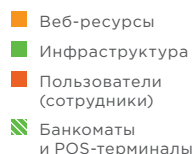
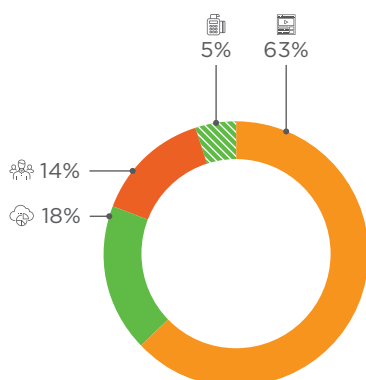


Рисунок 28. Объекты атак

## Торговля

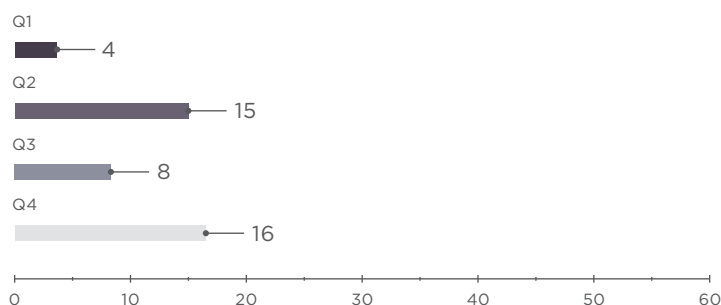


Рисунок 29. Число атак на компании из сферы розничной торговли

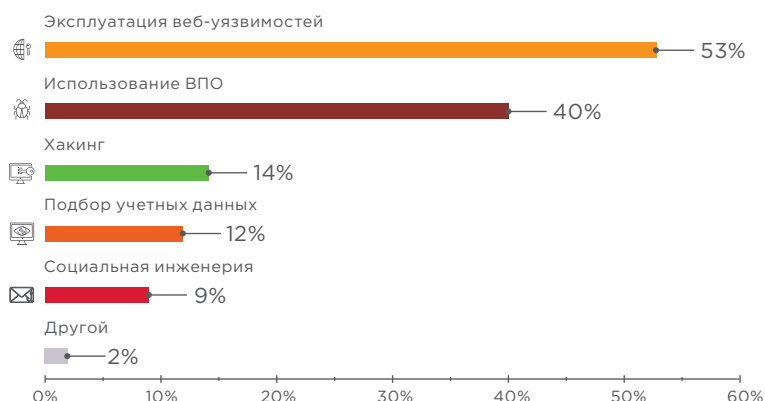


Рисунок 30. Методы атак на компании из сферы розничной торговли

Главным образом преступники были нацелены на кражу информации из интернет-магазинов, причем в 70% случаев были похищены данные платежных карт. Особо выделялась группировка Magecart, которая проводила свои атаки во второй половине года. Хакеры встраивали вредоносные скрипты в веб-приложения, которые собирали платежные и контактные данные, введенные пользователями.

Число атак на POS-терминалы сократилось в три раза по сравнению с 2017 годом, однако именно с POS-терминалами оказалась связана одна из крупнейших атак в сфере розничной торговли. Хакеры установили вредоносное ПО на терминалы, расположенные в розничных магазинах торговых сетей Saks Fifth Avenue и Lord & Taylor, и смогли похитить данные более 5 млн банковских карт.



## Промышленные компании

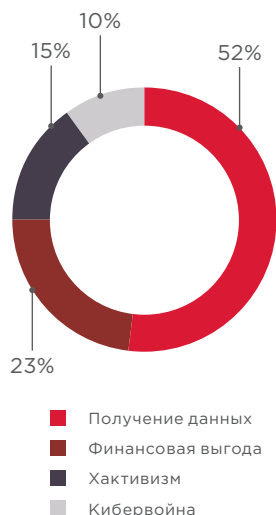


Рисунок 31. Мотивы атак

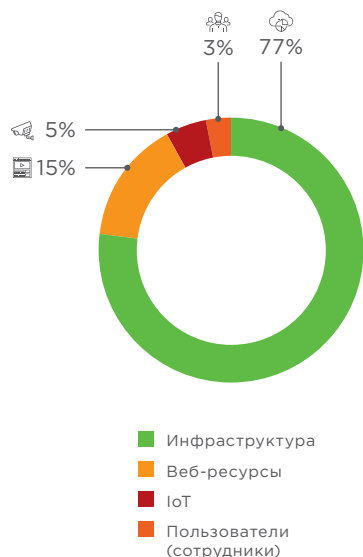


Рисунок 32. Объекты атак

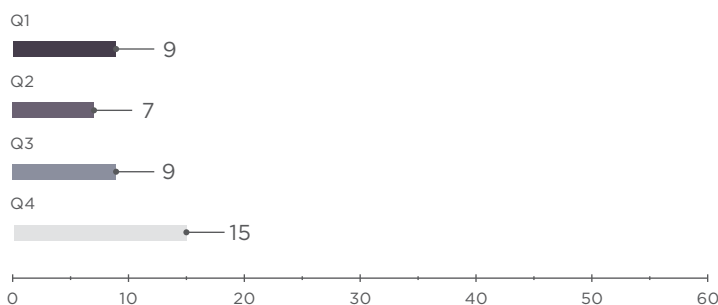


Рисунок 33. Число атак на промышленные предприятия

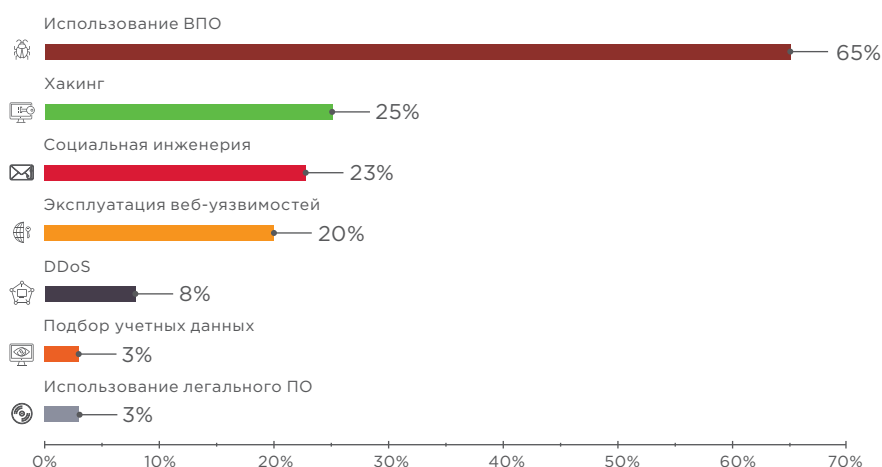


Рисунок 34. Методы атак на промышленные предприятия

2018 год не запомнился громкими атаками на сферу промышленности, однако это можно приписать лишь счастливой случайности. В августе нефтехимический завод в Саудовской Аравии подвергся атаке злоумышленников. Их целью была не просто остановка технологических процессов, а взрыв, который мог бы не только вызвать экологическую катастрофу, но и неминуемо сопровождался бы человеческими жертвами. Злоумышленники закрепились в компьютерной сети предприятия и находились в ней в течение длительного времени, и только ошибки в коде хакерского ПО не позволили им осуществить свои намерения.

Во втором квартале специалисты по безопасности обнаружили вредоносное ПО VPNFilter, которым оказалось заражено более 500 тысяч роутеров. Это ПО предназначено для перехвата и подмены трафика, проходящего через роутер. Как предполагается, целью преступников являлись системы SCADA: при анализе кода программы было установлено, что она ищет в трафике данные определенного вида, используемые в промышленных системах управления.

В промышленной сфере процветал шпионаж — хакеры похищали конфиденциальную техническую документацию, касающуюся, например, проектов АЭС или конструкции кораблей. В их распоряжении оказывалась и другая ценная информация, которую можно было бы выгодно продать преступным группировкам, к примеру планы расположения камер видеонаблюдения в тюрьмах, украденные у инженерной компании в числе прочих данных. В течение года специалисты PT ESC наблюдали атаки группировки SongXY, направленные на государственные и военно-промышленные организации. Главной целью этой группировки является шпионаж, используемое вредоносное ПО позволяет злоумышленникам следить за действиями пользователей и контролировать зараженные компьютеры.

## Сфера услуг

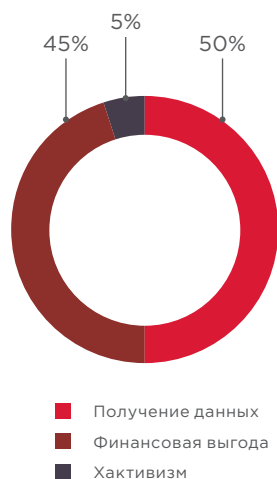


Рисунок 35. Мотивы атак

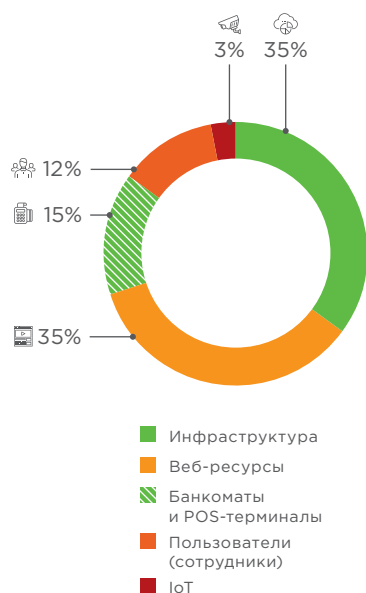


Рисунок 36. Объекты атак

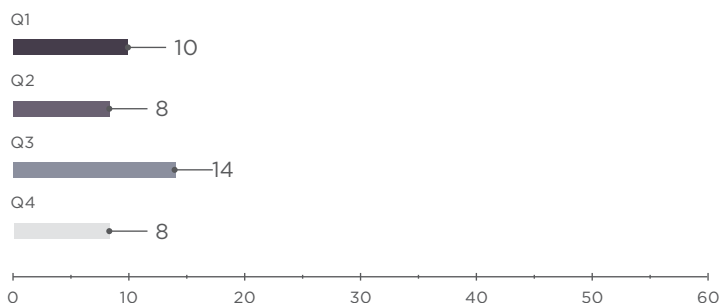


Рисунок 37. Число атак на компании из сферы услуг

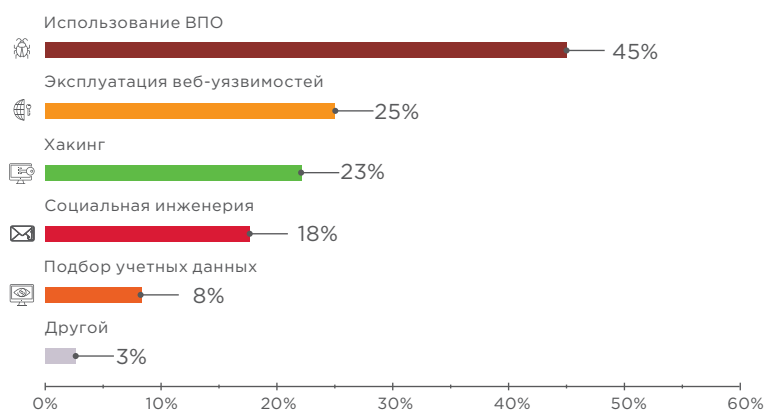


Рисунок 38. Методы атак на компании из сферы услуг

В сфере услуг хакеры были нацелены на кражу информации о клиентах, в особенности информации о платежных картах. Значительная часть инцидентов была связана с установкой вредоносного ПО на POS-терминалы.

Крупнейшая утечка данных в 2018 году произошла в результате взлома сети отелей Marriott, инцидент затронул 383 млн клиентов. Была похищена персональная информация, в том числе паспортные данные, скомпрометированы данные банковских карт. Акции компании за один день потеряли в цене около 6%, и затем падение продолжалось еще в течение двух недель.

## Частные лица

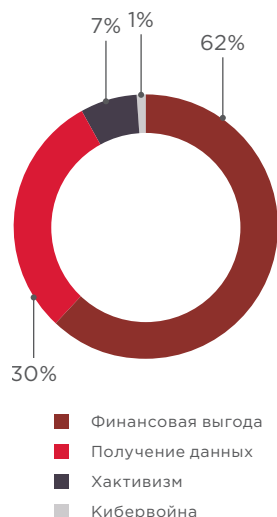


Рисунок 39. Мотивы атак

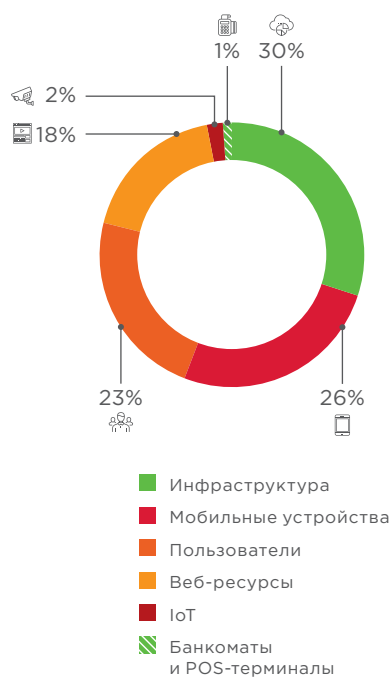


Рисунок 40. Объекты атак

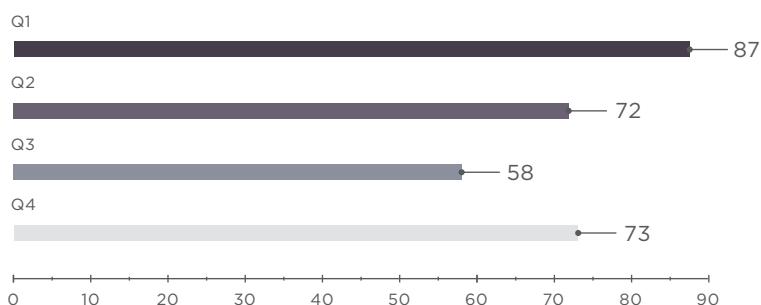


Рисунок 41. Число атак на частных лиц

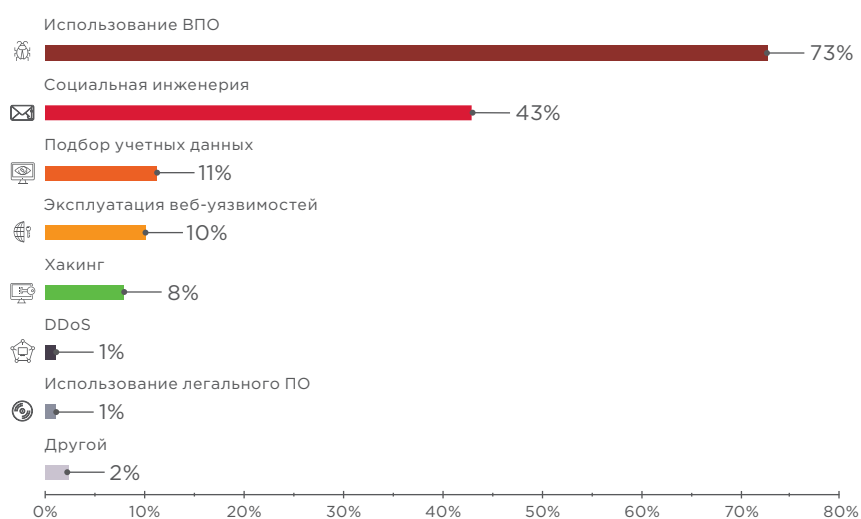


Рисунок 42. Методы атак на частных лиц

Обычные пользователи наиболее часто подвергались атакам злоумышленников. В ходе атак преступники главным образом прибегали к социальной инженерии (43% от общего числа инцидентов) и использовали вредоносное ПО (73% от общего числа инцидентов). Чаще всего компьютеры и мобильные устройства пользователей заражались шпионским ПО (21%), которое собирало учетные данные для доступа к личным кабинетам в онлайн-банках, криптовалютным кошелькам и другим сервисам. Как правило, источником вредоносных программ становились официальные магазины приложений, веб-сайты и электронная почта.

С общим падением курсов криптовалют уменьшается и доля атак с применением майнеров, которые были на пике популярности в прошлом году; майнинг становится нерентабельным для злоумышленников. Если в первом квартале при атаках на частных лиц майнеры составляли 27% выявленного вредоносного ПО, то к концу года их доля постепенно снизилась до 13%.



## Методы атак

Приведем основные факты для самых распространенных методов атак, которые использовались преступниками в 2018 году.

### Использование вредоносного ПО

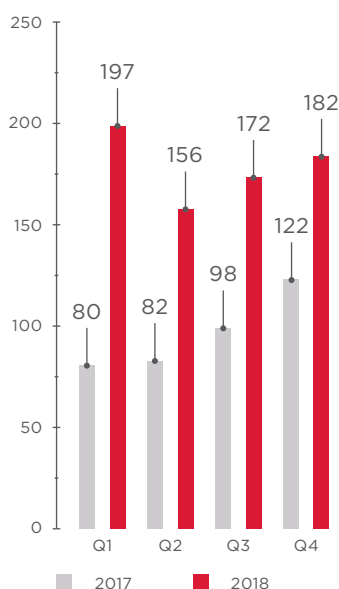


Рисунок 43. Количество атак с использованием ВПО

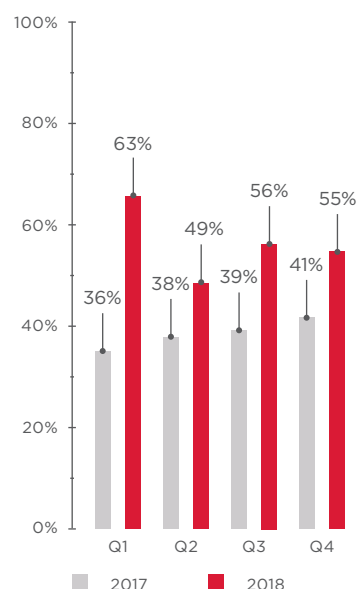


Рисунок 44. Доля атак с использованием ВПО

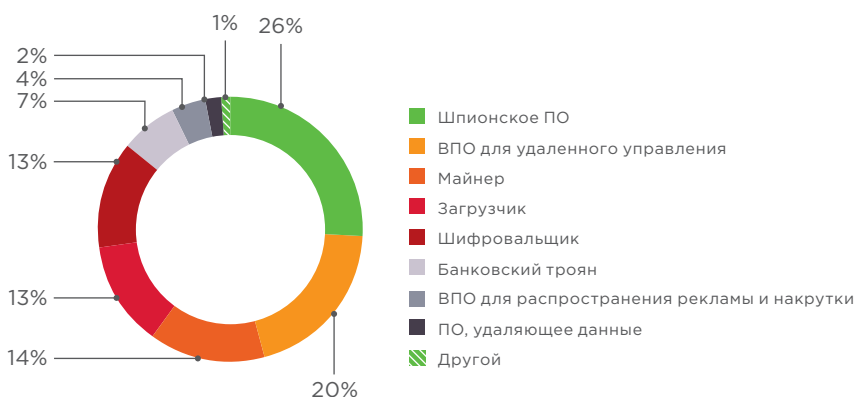


Рисунок 45. Типы ВПО

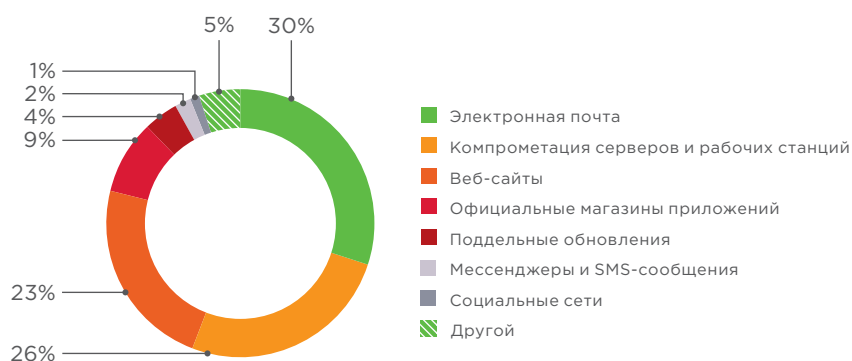


Рисунок 46. Способы распространения ВПО

## Социальная инженерия

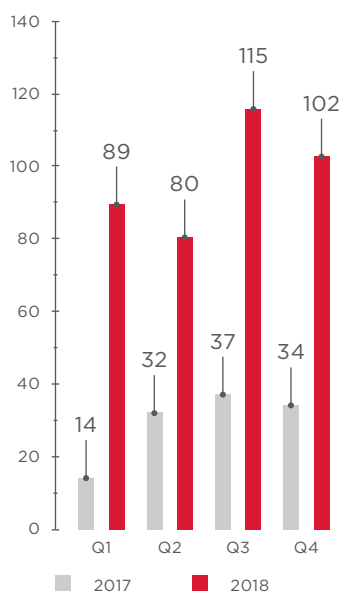


Рисунок 47. Количество атак методами социальной инженерии

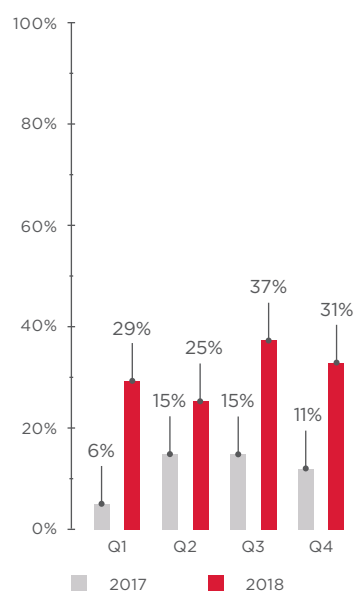


Рисунок 48. Доля атак методами социальной инженерии

## Хакинг

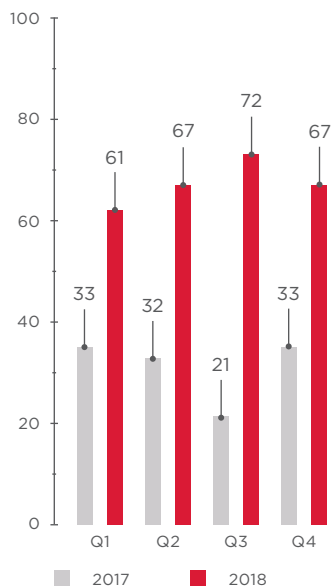


Рисунок 49. Количество атак с использованием уязвимостей ПО и недостатков механизмов защиты

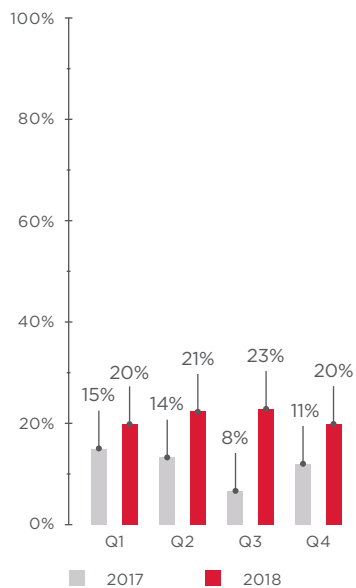


Рисунок 50. Доля атак с использованием уязвимостей ПО и недостатков механизмов защиты

## Эксплуатация веб-уязвимостей

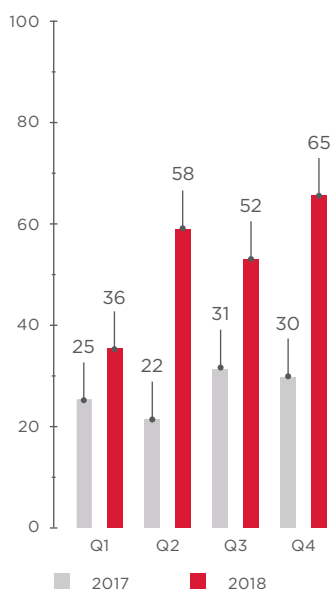


Рисунок 51. Количество атак с использованием веб-уязвимостей

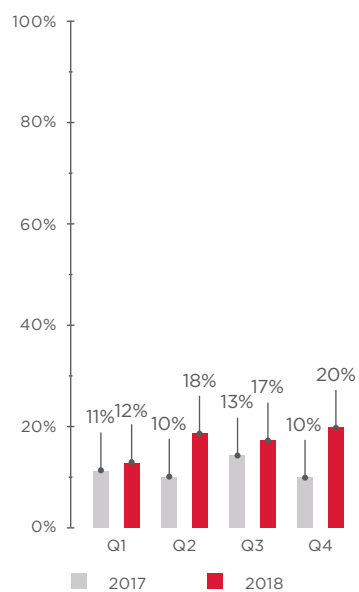


Рисунок 52. Доля атак с использованием веб-уязвимостей

## Подбор учетных данных

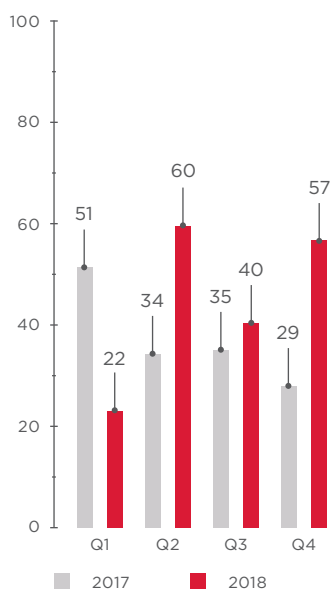


Рисунок 53. Количество случаев подбора учетных данных

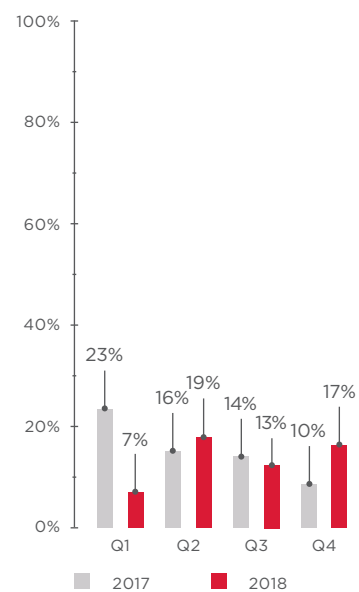


Рисунок 54. Доля подбора учетных данных





В 2018 году зафиксированы две самые мощные DDoS-атаки в истории — 1,7 и 1,35 терабит в секунду

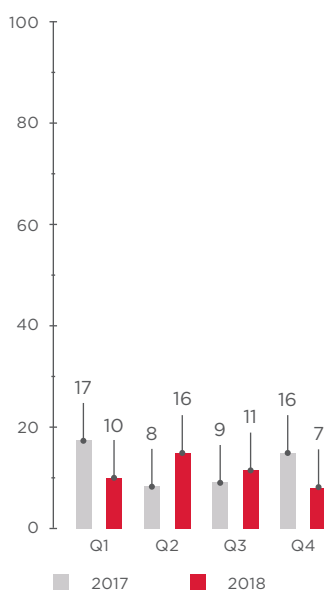


Рисунок 55. Количество DDoS-атак

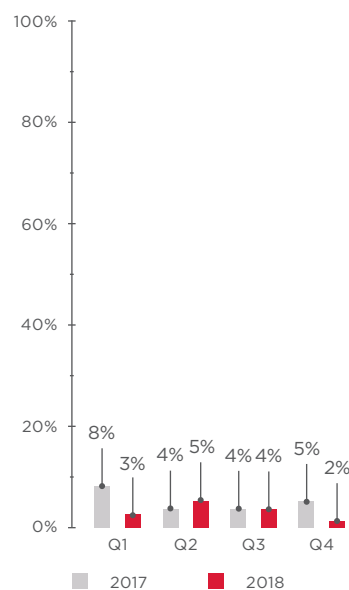


Рисунок 56. Доля DDoS-атак

## Прогнозы

Прогнозы на 2019 год:

- Тенденция к росту атак, направленных на хищение данных, скорее всего, сохранится. Преступники продолжают атаковать слабо защищенные ресурсы для кражи персональных, медицинских, платежных данных. В зоне риска находятся компании из тех областей, где уровень защищенности пока не очень высок, например из сфер услуг, образования, медицины или розничной торговли. Вредоносное ПО для сбора платежных данных с веб-сайтов, POS-терминалов и банкоматов будет активно развиваться.
- Преступники будут искать новые пути распространения вредоносного ПО и совершенствовать старые. Социальная инженерия, вероятно, останется основным путем распространения, однако в связи с ростом осведомленности о различных способах мошенничества преступники начнут разрабатывать более хитроумные схемы обмана пользователей. Многоэтапные атаки (через supply chain) также не потеряют актуальности.
- Продолжатся атаки шифровальщиков-вымогателей на наиболее чувствительные к простоям и потере данных компании. Как показывает практика, некоторые организации не имеют плана действий и резервных ресурсов на случай сбоя в функционировании критически важных систем — и предпочитают заплатить преступникам, чтобы как можно скорее возобновить рабочие процессы.
- Майнеры стали приносить своим владельцам намного меньший доход, поэтому если ситуация на рынке криптовалют не изменится, количество заражений майнерами продолжит снижаться.
- Мощность DDoS-атак будет увеличиваться как в связи с продолжающимся ростом ботнетов, так и в связи с использованием новых техник и уязвимостей, позволяющих многократно усиливать атаки, а также наличия в свободном доступе ПО, которым может воспользоваться даже неопытный злоумышленник.

- Проправительственные группировки продолжают атаковать промышленные предприятия. Причем их целью может стать уже не шпионаж, а нарушение технологических процессов, которое приведет к человеческим жертвам. В прошедшем году мы видели попытки таких атак, но в ближайшее время они могут претвориться в жизнь, если компании не примут мер для повышения уровня защищенности.
- Киберпреступность будет все больше переплетаться с другими видами преступной деятельности. Инциденты, связанные со взломом компьютерных систем, например кража персональных данных, будут находить продолжение в тех преступлениях, которые обычно не попадают в поле зрения специалистов по информационной безопасности.
- Рынок киберуслуг продолжит развиваться. Будет появляться все больше группировок, которые предпочтут не вкладывать ресурсы в разработку собственного ПО, а покупать уже готовое. В результате одни и те же программы будут использоваться разными группами киберпреступников, что существенно усложнит атрибуцию.
- Разработчикам вредоносного ПО выгодно продавать как можно больше копий одной утилиты, поэтому они будут нацелены на широкую аудиторию. В приоритете будет расширяемое модульное ПО с гибкой архитектурой, которая позволяет легко добавлять новые функции для выполнения разных задач. Такие универсальные программы наверняка будут более востребованы у преступников, чем узконаправленные.
- В 2018 году за невыполнение требований GDPR уже были оштрафованы первые компании, но в целом регуляторы применяли штрафные санкции лишь в крайних случаях. Вероятно, в будущем они будут более строги в отношении организаций, проявивших халатность при обработке данных.

## О компании

[ptsecurity.com](http://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.