



POSITIVE TECHNOLOGIES

Актуальные киберугрозы

III 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	10
Хакинг	11
Эксплуатация веб-уязвимостей	12
Подбор учетных данных	12
DDoS	13
Категории жертв	14
Государственные организации	14
Финансовые организации	16
Медицинские учреждения	18
Образовательные учреждения	19
Частные лица	20
Как защититься организации	21
Как вендору защитить свои продукты	23
Как защититься обычному пользователю	23



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 следить за актуальными угрозами информационной безопасности. Несмотря на то что третий квартал традиционно является порой отпусков, злоумышленники не дремлют, продолжая изобретать новые способы атак в киберпространстве.

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

- Количество уникальных киберинцидентов на 24% превысило показатели аналогичного периода в 2017 году.
- Продолжает расти число атак, направленных на кражу информации, их доля приблизилась к половине от общего числа киберпреступлений. В тройку по-прежнему входят персональные данные, учетные записи и данные платежных карт.
- Резко увеличилось число инцидентов, в которых злоумышленники задействовали методы социальной инженерии. Особенно велика их доля в числе атак на частных лиц. В III квартале злоумышленники использовали всевозможные каналы воздействия на людей: телефонные звонки, SMS-сообщения, электронные письма и даже обычную почту.
- Выросло число заражений вредоносным программным обеспечением. На фоне общего спада популярности шифровальщиков в III квартале их доля увеличилась до 20% (для сравнения: 12% в I квартале, 9% во II квартале). Возможно, это связано с агрессивной политикой операторов шифровальщика GandCrab: обнаруженный в начале года, к сентябрю этот зловард эволюционировал до пятой версии. Число заражений майнерами продолжает снижаться, что, вероятнее всего, вызвано падением курса ряда криптовалют.
- По сравнению со вторым кварталом выросло число атак, направленных на финансовые организации. Это связано преимущественно с волной фишинговых рассылок группировки Cobalt. Общая сумма ущерба от всех атак в III квартале для финансовых организаций составила порядка 18 млн долл. США.

Четвертый квартал — время подведения итогов. В связи с этим мы прогнозируем рост числа фишинговых атак с тематикой годовой отчетности, в том числе на государственные и финансовые организации. В преддверии главного праздника года люди активно совершают покупки в интернет-магазинах, поэтому мы предполагаем увеличение доли заражения вредоносным ПО, распространяемым посредством веб-ресурсов, и кражи данных платежных карт. Несмотря на рост числа атак на криптовалютные биржи в III квартале, мы прогнозируем их спад в связи со снижением курса биткойна.



Сводная статистика

В III квартале 2018 года основным мотивом для совершения киберпреступлений остается кража информации. Доля инцидентов с хищением данных выросла на 5% по сравнению с прошлым кварталом и на 20% по сравнению с III кварталом 2017 года, в то время как финансовая мотивация снизилась с 53% в начале 2018 года до 33% в III квартале. Украсть деньги в киберпространстве становится все сложнее, гораздо проще похитить закрытые коммерческие сведения или данные о человеке, личную переписку, фото или видео — и шантажировать жертву, требуя огромные выкупы за неразглашение информации, или продать эти данные в дарквебе.

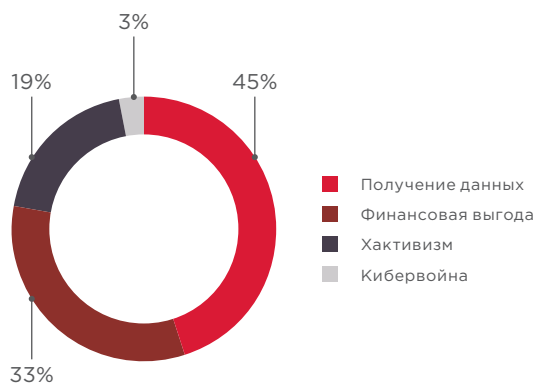


Рисунок 1. Мотивы злоумышленников

Персональные данные, учетные данные и данные платежных карт по-прежнему остаются самой привлекательной добычей для злоумышленников, они составляют более половины всей скомпрометированной информации. На наш взгляд, многие инциденты, связанные с кражей персональных данных, объясняются цифровой неграмотностью их владельцев. Зачастую люди добровольно предоставляют личные данные за небольшое вознаграждение в онлайн-сервисах или размещают их в открытом доступе в соцсетях, не понимая, насколько ценной может быть эта информация для злоумышленников.

Каждое пятое хищение информации — кража учетных данных. Часто злоумышленники воруют пароли у пользователей различных веб-сервисов, чтобы с этими паролями получить доступ к другим системам, где может обрабатываться более ценная информация, например медицинские сведения. Подобные атаки с использованием украденных учетных данных (credential stuffing) — намного эффективнее, чем простой перебор паролей, поскольку людям свойственно использовать одинаковые учетные данные для доступа к разным системам.

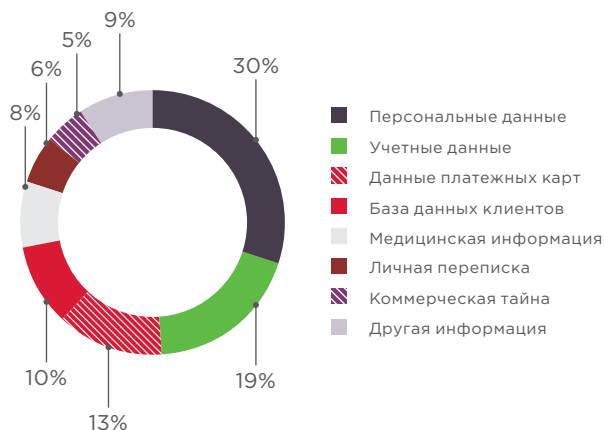


Рисунок 2. Типы украденных данных

Как и в прошлом квартале, целевые атаки преобладают над массовыми, их доля составила 55%. Таргетированные атаки совершаются преимущественно на правительственные организации. Выросла доля атак на кредитно-финансовую сферу (9% против 6% во втором квартале). По-прежнему остается высоким интерес злоумышленников к медицинским и образовательным организациям. Каждая пятая атака — это атака на частных лиц. Далее мы рассмотрим все эти категории атак более подробно. Масштабные кибератаки, преимущественно вредоносные эпидемии, которые не ограничиваются воздействием на какую-то одну отрасль, мы отнесли к категории «без привязки к отрасли».

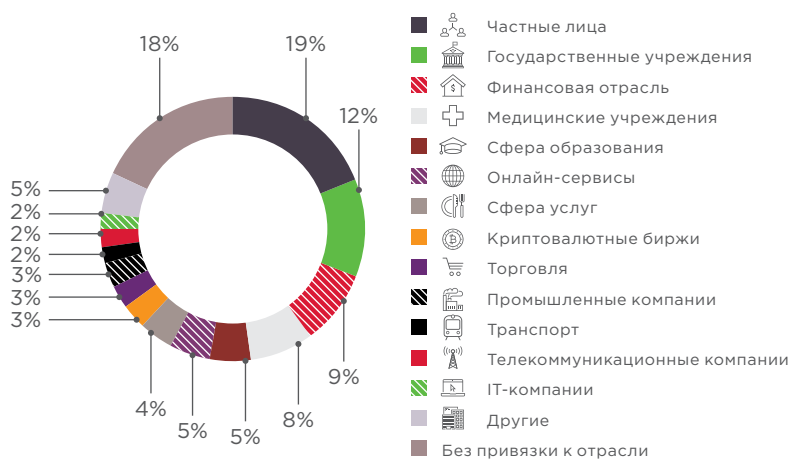


Рисунок 3. Категории жертв

Распределение объектов атак не претерпело значительных изменений по сравнению со вторым кварталом. Здесь стоит отметить только незначительное снижение числа атак на веб-ресурсы и рост атак на пользователей.

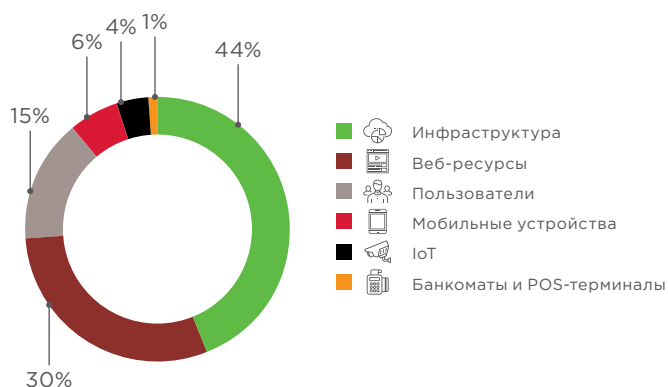


Рисунок 4. Объекты атак

В III квартале 2018 года выросла доля атак с использованием вредоносного ПО и социальной инженерии. Как правило, эти два метода используются злоумышленниками одновременно. По сравнению со II кварталом увеличилась доля инцидентов, связанных с хакингом (эксплуатацией уязвимостей инфраструктуры без применения социальной инженерии и вредоносного ПО и без учета веб-атак, которые мы выделили в отдельную категорию), она достигла 23%. В 3% случаев атаки совершались с использованием, среди прочего, легального ПО. Так, например, в августе стало известно о вредоносной кампании против российских промышленных предприятий, в ходе которой злоумышленники незаметно для жертвы устанавливали на компьютеры программы для удаленного администрирования. Аналогичные случаи расследовали эксперты PT ESC в июле, когда злоумышленники, помимо инструментов собственной разработки, использовали такие свободно распространяемые утилиты, как PortScan, GsecDump и Mimikatz.

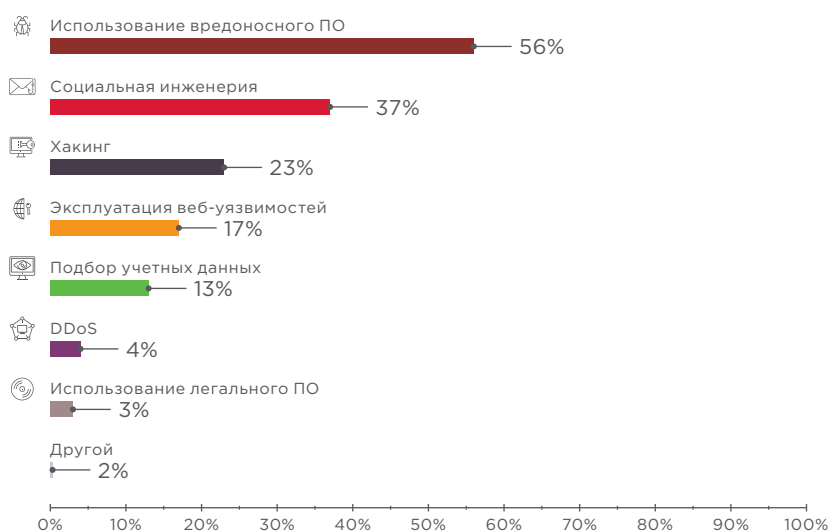


Рисунок 5. Методы атак

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

		Отрасль														
		Государственные учреждения	Финансовая отрасль	Промышленные компании	Медицинские учреждения	Онлайн-сервисы	Сфера услуг	IT-компании	Сфера образования	Торговля	Телекоммуникационные компании	Частные лица	Транспорт	Криптовалютные биржи	Другие	Без привязки к отрасли
Всего атак		36	29	9	24	16	14	5	17	8	7	58	6	9	14	55
Объект	Инфраструктура	24	21	6	15	1	5	2	9	1	3	12	3	2	6	25
	Веб-ресурсы	10		2	3	14	6	3	6	6	4	12	2	6	5	12
	Пользователи	2	4		6	1	1		2	1		20		1	2	6
	Мобильные устройства		1									13	1		1	2
	Банкоматы и POS-терминалы		2				2									
	IoT		1	1								1				10
Метод	Использование ВПО	21	21	5	8	6	5		3	3	2	39	4	1	5	49
	Социальная инженерия	13	15	2	11	1	2		7	1		35		2	7	19
	Подбор учетных данных	4	1		11	1		1	5	1	1	7	1		2	5
	Хакинг	9	10	3	3	6	5	1	3	1	1	4		6	5	15
	Эксплуатация веб-уязвимостей	7	1	3	2	7	3	2	2	4	5	6	2	1	1	6
	Использование легального ПО	2		1				1			1	1				3
	DDoS	3	1	1				2	3		1					
	Другой	1					1			1		2			1	1
Мотив	Финансовая выгода	4	23	3	6		4		2			27	1	7	6	20
	Получение данных	16	4	3	16	12	10	3	8	7	6	23	3	1	6	19
	Хактивизм	11	2	2	2	4		2	7	1	1	6	2	1	2	16
	Кибервойна	5		1								2				
Интенсивность цвета показывает долю атак в рамках 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%				



Динамика атак

В июле мы наблюдали самое большое число атак с начала года. На этот месяц пришлось более 40% всех уникальных атак, зафиксированных в III квартале. Причиной может быть чемпионат мира по футболу, который проходил в России с 14 июня по 15 июля. Во время его проведения наши эксперты помогли отразить порядка 38 000 попыток компрометации сервисов транспортной дирекции.

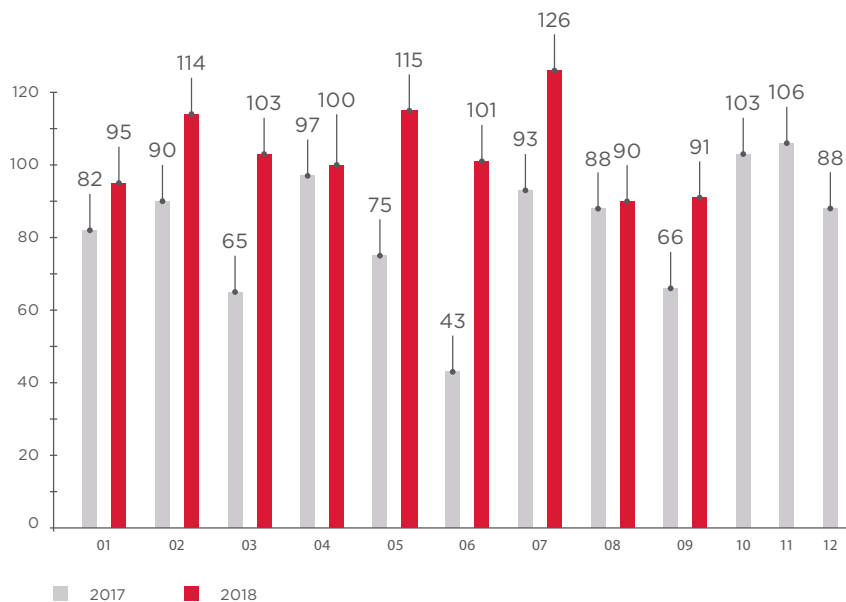


Рисунок 6. Количество инцидентов в 2017 и 2018 годах (по месяцам)

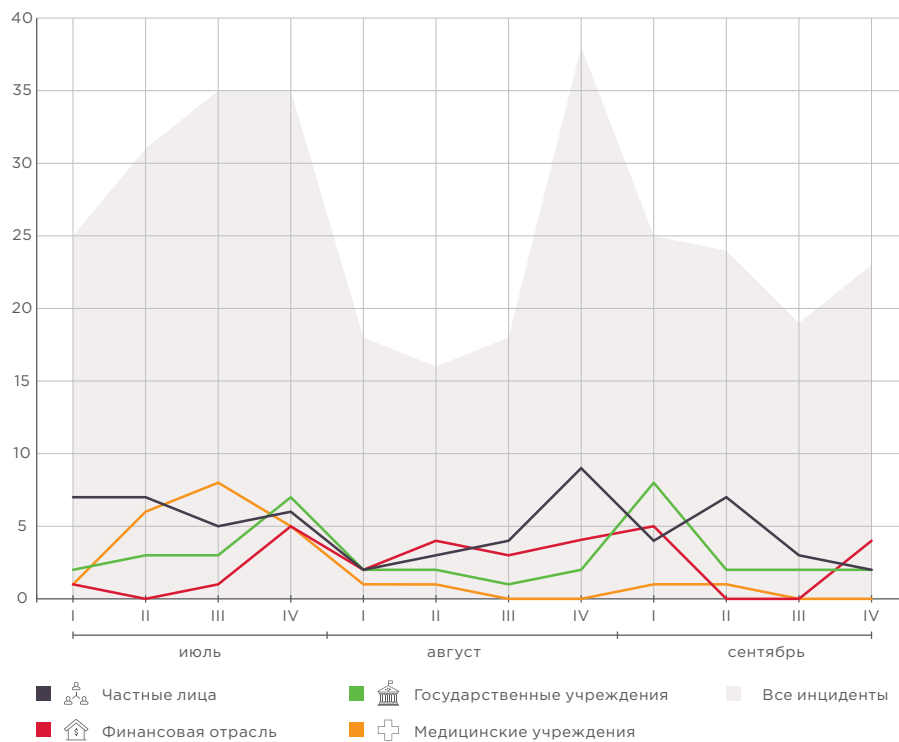


Рисунок 7. Количество инцидентов в III квартале 2018 года (по неделям)



Методы атак

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

Использование вредоносного ПО



Использование вредоносного ПО неизменно остается самым распространенным методом атак. В III квартале 2018 года число инцидентов с применением вредоносного ПО выросло до 56% против 49% во втором квартале. По сравнению с прошлым кварталом число заражений шифровальщиками увеличилось с 9% до 20%, опередив в рейтинге шпионское ПО. Заражению вирусами-вымогателями подвергались государственные учреждения, медицинские центры, учреждения сферы образования, промышленные предприятия, а также частные лица. Например, обнаруженный в начале 2018 года шифровальщик *GandCrab* продолжает набирать популярность, и в сентябре разработчики опубликовали пятую версию этого вредоносного ПО. Уровень нелегального майнинга криптовалюты, напротив, снижается: 8% инцидентов с использованием майнеров против 15% во втором квартале и 23% в первом квартале. Возможно, причина кроется в том, что обнаружить скрытый майнер бывает непросто, в то время как несанкционированное зашифрование файлов обнаруживается, как правило, в первый же день инцидента. Вероятно, большое число пользователей не знают, что помогают злоумышленникам зарабатывать деньги на незаконной добыче криптовалюты.



По данным Avast¹, появляются сайты, на которых пользователь может выбирать между просмотром рекламы и майнингом криптовалюты с использованием вычислительных ресурсов его устройства. Как сообщают эксперты, каждый пятый посетитель таких сайтов соглашается предоставить свои вычислительные ресурсы для майнинга взамен надоедливой рекламы.

Не исключено, что снижение доли инцидентов с заражением майнерами связано со снижением интереса злоумышленников к этому бизнесу, и тому есть несколько причин. С одной стороны, непрерывно растет сложность добычи криптовалюты (хешрейт), а с другой — в течение всего года наблюдается устойчивая тенденция к падению курса ряда криптовалют. Совокупность этих причин может сделать незаконный бизнес майнеров нерентабельным с точки зрения окупаемости затрат. В то же время в июле 2018 года стало известно о первом случае реального тюремного заключения за криптоджекинг². Житель Японии осужден на год за незаконную добычу криптовалюты, хотя успел заработать на ней только 45 долл. США.

¹ blog.avast.com/ru/issledovanie-avast-rossijskih-polzovatelej-ne-pugayut-ugrozy-skrytogo-majninga

² zdnet.com/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive/

С 4% во II квартале до 9% в III квартале 2018 года выросло число заражений через официальные магазины приложений. В августе специалисты компании «Доктор Веб» обнаружили³ более ста вредоносных программ под ОС Android, распространяемых через Google Play. Большинство из них подписывают жертв на различные платные сервисы или распространяют рекламу. Во второй половине сентября стало известно⁴ о более опасном зловреде — банковском трояне, найденном специалистами ESET также в Google Play. Банкер был внедрен в приложение для записи телефонных разговоров QRecorder и похищал аутентификационные данные и данные платежных карт. С его помощью злоумышленникам удалось украсть со счетов жертв около 78 000 евро.

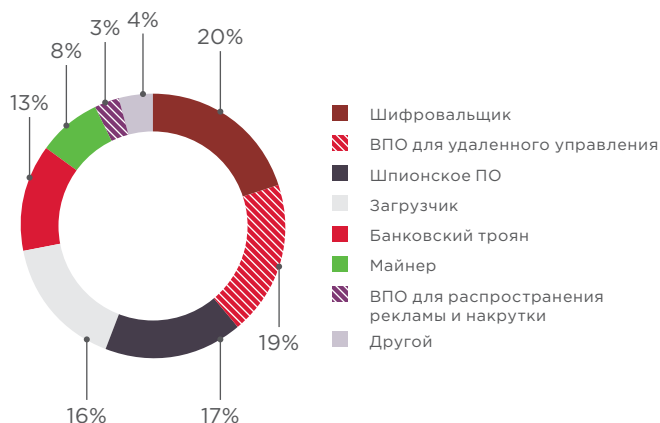


Рисунок 8. Типы вредоносного ПО

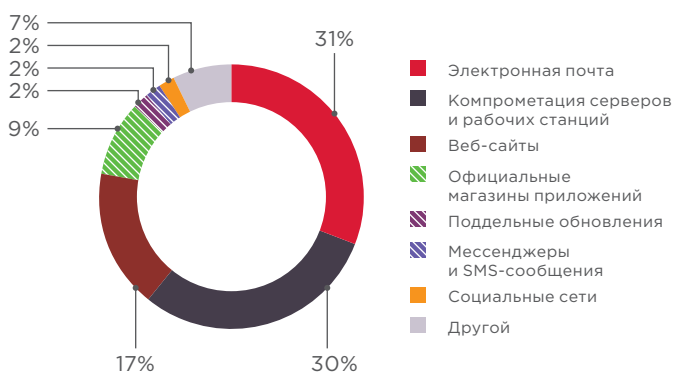


Рисунок 9. Способы распространения ВПО

В 31% инцидентов с использованием зловредов они распространялись посредством электронных писем. Это самый простой способ доставки вредоносного ПО на компьютеры жертв, который злоумышленники готовы применять вновь и вновь благодаря его эффективности. В сентябре специалисты ПТ ESC обнаружили новую волну продолжающихся APT, о которых мы упоминали ранее во втором квартале. Используя загрузчик CMstar, злоумышленники эксплуатируют уязвимость [CVE-2017-11882](#). Полезная нагрузка под названием ByeBy уже знакома нам по прошлогодней кампании [SongXY](#), направленной на военно-промышленные комплексы России и стран СНГ, главной целью которой был шпионаж.

³ news.drweb.com/show/?i=12797&lng=en

⁴ lukasstefanko.com/2018/09/banking-trojan-found-on-google-play-stole-10000-euros-from-victims.html

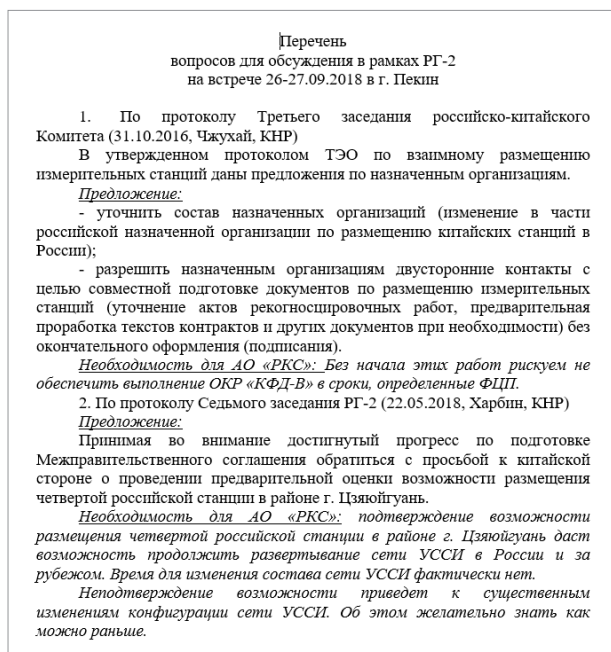
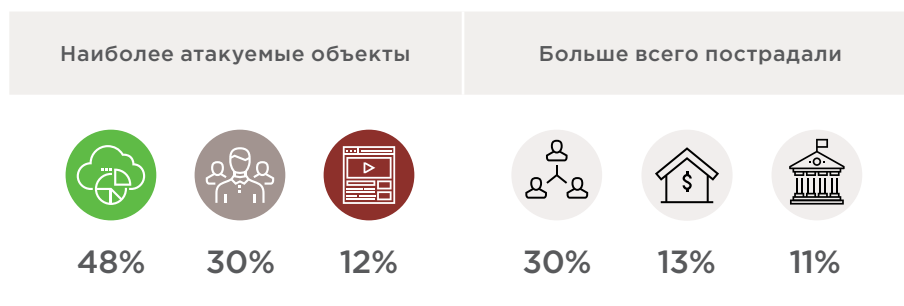


Рисунок 10. Документ в формате MS Word для доставки вредоносного ПО

Социальная инженерия



В условиях непрерывного противостояния киберпреступников и специалистов в области защиты информации первым приходится постоянно совершенствовать не только свои технические навыки, но и знания в области психологии человека. В III квартале 2018 года мы отмечаем значительное увеличение инцидентов, в которых злоумышленники достигали своих преступных целей, обманывая других людей с помощью информационных технологий. Так, 20-летнему студенту из США не однажды удалось⁵ обмануть операторов сотовой связи и совершить атаки типа SIM hijacking. Убеждая операторов, что он потерял свой телефон, преступник присваивал себе SIM-карты с интересующими его номерами телефонов и таким образом получал доступ к различным сервисам, в том числе к чужим криптокошелькам. В результате этих нехитрых действий злоумышленник заполучил 40 номеров телефонов, после чего украл несколько миллионов долларов в криптовалюте, которые принадлежали владельцам этих номеров.

Эксперты PT ESC регулярно сталкиваются с тщательно замаскированными способами доставки вредоносного ПО. Например, для доставки зловреда на компьютер жертвы преступники могут использовать данные с политическим контекстом. Ниже приведен пример документа, обнаруженного экспертами PT ESC в августе; он предназначался для доставки загрузчика CMstar и эксплуатации уязвимости CVE-2017-11882.

⁵ motherboard.vice.com/en_us/article/a3q7mz/hacker-allegedly-stole-millions-bitcoin-sim-swapping

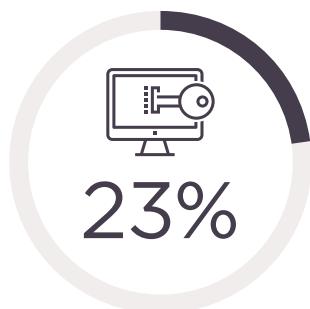


Уровень деятельности киберпреступности РФ по субъектам РФ, в %
(по данным отчета Стокгольмского Бюро России, за III квартал 2018 года)

Субъект РФ	Место по РФ	Положительная динамика	Отрицательная динамика	Разница	Итого	Динамика
РФ	-	75,6	13,4	62,2	6,5	+0,1 / +0,2
ЦФО	-	78,1	12,4	65,7	5,4	+0,6 / +3,3
Архангельская область	4	88,7	3,2	85,5	2,1	+2,8 / +0,9
Брянская область	15	78,8	8,5	70,3	8,4	+1,4 / +3,4
Владимирская область	65	71,1	14,0	57,1	13,4	+5,7 / +11,2
Воронежская область	15	79,3	15,2	64,1	3,2	+4,4 / +5,2
Ивановская область	32	76,7	12,2	64,5	6,9	+5,7 / +3,2
Калужская область	8	86,4	6,1	79,7	3,2	+10,1 / +9,1
Костромская область	84	63,7	18,0	45,7	11,5	+1,1 / -8,4
Курганская область	10	70,0	6,8	75,2	11,4	+1,0 / -6,7
Ленинградская область	20	80,0	12,2	67,8	4,3	+2,4 / +2,2
Магнитогорская область	12	81,7	10,2	71,5	4,7	+3,1 / +3,7
Московская область	21	79,1	11,5	67,6	3,7	+0,8 / -4,4
Нижегородская область	37	78,7	12,6	66,1	6,4	+5,5 / +11,7
Орловская область	28	79,1	12,4	66,7	6,0	+5,6 / +3,5
Рязанская область	31	70,3	11,2	59,1	7,8	+1,1 / -2,2
Тверская область	57	73,8	15,3	58,5	6,2	+8,6 / +4,1
Тульская область	3	87,0	6,8	80,2	4,4	+0,1 / +4,1
Ханты-Мансийский АО	69	71,4	14,0	57,4	4,9	+0,8 / -0,3
Челябинская область	53	75,4	16,4	59,0	3,4	+3,4 / -5,0
СВФО	-	72,6	14,4	58,2	5,1	+0,2 / -5,9
Республика Башкортостан	47	71,5	16,0	55,5	6,7	+5,4 / +0,1
Республика Бурятия	73	69,5	16,4	53,1	10,1	+1,4 / +0,4
Алтайская область	36	77,0	13,2	63,7	3,4	+1,0 / +3,4
Волгоградская область	81	68,9	11,1	47,8	6,7	+1,1 / -6,2
Калининградская область	39	74,1	12,1	62,0	9,8	+2,7 / +3,9
Ленинградская область	13	73,4	9,9	64,7	9,6	+1,0 / -6,6
Мурманская область	52	75,2	16,0	59,2	3,5	+2,5 / +4,4
Новгородская область	47	74,7	14,2	60,5	7,3	+10,2 / +5,8
Псковская область	17	77,8	9,9	67,9	2,5	+2,1 / +2,9
г. Санкт-Петербург	70	70,5	15,3	55,2	5,9	+5,3 / +9,7
г. Севастополь	14	81,0	10,1	70,9	1,1	+3,5 / +1,9
ЮФО	-	77,8	13,0	64,8	5,8	+3,4 / +0,9
Республика Адыгея	45	72,2	11,2	61,0	10,8	+4,4 / +5,6
Республика Алтай	15	72,8	14,0	58,8	5,8	+14,4 / +5,8
Республика Бурятия	1	84,3	1,1	83,2	1,8	+6,4 / +0,6
Республика Дагестан	29	79,3	13,9	65,4	4,0	+1,4 / -0,1
Астраханская область	74	67,2	14,2	53,0	11,4	+4,2 / +3,4
Волгоградская область	80	68,3	18,4	49,9	5,5	+6,6 / +8,8
Ростовская область	40	76,7	14,7	62,0	4,4	+3,6 / +7,4
г. Севастополь	2	91,6	2,9	88,7	3,3	+0,7 / +4,3
СКФО	-	76,1	11,2	64,9	10,3	+1,9 / +6,7
Республика Дагестан	16	71,2	12,6	58,6	13,2	+1,6 / +11,0
Республика Ингушетия	26	79,3	13,0	66,3	5,3	+10,8 / +3,6
КБР	79	65,8	14,6	51,2	16,2	+1,0 / -2,8

Рисунок 11. Документ из фишинговой рассылки для доставки загрузки

Хакинг



Наиболее атакуемые объекты

Больше всего пострадали



49%



39%



11%



14%



13%



8%

Ошибки в бизнес-логике приложений, известные уязвимости в необновленном ПО, бреши в механизмах защиты — все это любят искать злоумышленники для реализации своих преступных замыслов. Когда уязвимости найдены, злоумышленник пытается использовать их в своих корыстных целях, и этот процесс мы называем хакингом.

IoT-уязвимости открывают злоумышленникам возможности по созданию ботнетов для мощнейших DDoS-атак. Владельцы маршрутизаторов по-прежнему страдают от атак на их устройства. Эксперты из eSentire Threat Intelligence обнаружили⁶ попытку проэксплуатировать уязвимость CVE-2018-10562 в оборудовании D-Link и DASAN. Однако недавно злоумышленники стали использовать уязвимые маршрутизаторы как точку входа для майнинга криптовалюты в браузерах пользователей. С этой целью в III квартале эксплуатировалась⁷ уязвимость нулевого дня в сотнях тысяч устройств MikroTik. Здесь стоит отметить, что производитель выпустил обновление уже через день после ее обнаружения, однако многие владельцы маршрутизаторов до сих пор не обновили прошивки.

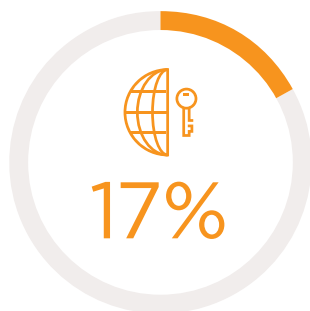
Ошибки в коде ПО могут стоить очень дорого. Криптовалютные торговые площадки привлекают злоумышленников, во-первых, возможностью финансовой прибыли, а во-вторых, большим числом уязвимостей в логике их работы, например в механизмах транзакций. В июле от уязвимости в коде Monero пострадала биржа Livecoin, ущерб составил 1,8 млн долл. США. В сентябре хакерам удалось проэксплуатировать уязвимость в протоколе Bitcoin (CVE-2018-17144), обнаружив ее в малоизвестном форке под названием pigeoncoin, разработчики которого вовремя не установили патч. В результате инцидента было похищено 15 тысяч долларов в криптовалюте.

6 esentire.com/news-and-events/security-advisories/increase-in-attacks-on-gpon-routers/

7 trustwave.com/en-us/resources/blogs/spiderlabs-blog/mass-mikrotik-router-infection-first-we-cryptojack-brazil-then-we-take-the-world/



Эксплуатация веб-уязвимостей

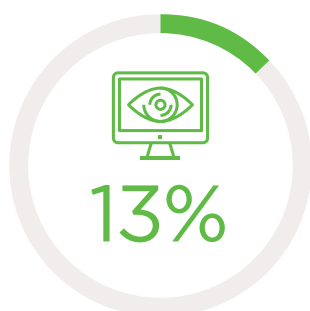


Атаки на веб-приложения позволяют не только получить контроль над ними или проникнуть во внутреннюю сеть компании — их используют и в других целях, включая политические. Веб-сайты — привлекательная мишень для хактивистов, ведь именно сайты с высокой посещаемостью позволяют оперативно донести свои идеи до миллионов людей. Так, например, в июле был атакован сайт тайваньской Демократической прогрессивной партии, хакеры оставили на взломанных веб-страницах послания политического характера⁸.

Нередко злоумышленники эксплуатируют веб-уязвимости в приложениях, чтобы использовать их как площадку для распространения вредоносного ПО. Например, в июле стало известно⁹, что хакеры подменили ссылки на сайте бесплатного редактора VSDC. После перехода по модифицированной ссылке на компьютер жертвы загружается шпионская программа, которая собирает данные и отправляет их на сервер злоумышленника. Инцидент затронул пользователей популярного редактора более чем в 30 странах.

Ошибки в коде веб-приложения могут повлечь за собой крупные утечки данных в результате недостаточной авторизации пользователей. Такую ошибку допустил¹⁰ при разработке веб-сайта телекоммуникационный провайдер Telefónica, что повлекло за собой раскрытие личной и финансовой информации пользователей платного телевидения Movistar. За нарушение положений GDPR компании грозит штраф в размере от 2% до 4% годового оборота. Подобные штрафы грозят и популярной социальной сети Facebook, из-за ошибок в коде которой под угрозой оказались десятки миллионов аккаунтов с личной информацией¹¹.

Подбор учетных данных



В III квартале мы отмечаем небольшое снижение числа атак, направленных на подбор учетных данных. Из-за слабых паролей и отсутствия двухфакторной аутентификации в начале июля пострадали пользователи сервиса Timehop: в руках злоумышленников оказались личные данные 21 миллиона пользователей¹². Требования к стойким

⁸ taiwannews.com.tw/en/news/3473203

⁹ videosoftdev.com/news/attacks-successfully-stopped

¹⁰ galaxkey.com/telefonica-leaks-millions-of-customers-personal-information/

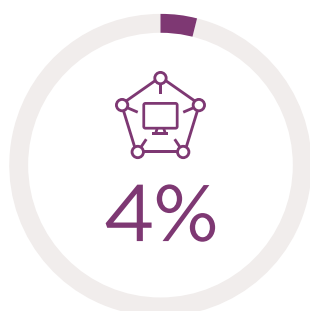
¹¹ newsroom.fb.com/news/2018/09/security-update/

¹² timehop.com/security



паролям просты и известны большей части пользователей интернета. Но, к сожалению, со взломом учетных записей сталкиваются даже люди, непосредственно связанные с миром информационных технологий. Так, хакеры получили доступ к учетной записи одного из разработчиков менеджера пакетов npm, что позволило им внедрить вредоносное ПО непосредственно в код JavaScript-библиотеки¹³. В сентябре разработчики AdGuard, блокировщика рекламы для популярных ОС, были вынуждены осуществить сброс паролей для всех пользователей из-за брутфорс-атаки¹⁴.

DDoS



Наиболее атакуемые объекты



73%



27%



27%



27%



18%

Начало учебного года ознаменовалось всплеском DDoS-атак на образовательные учреждения. Например, сайт Эдинбургского университета с 12 сентября был недоступен более суток¹⁵.

Не секрет, что некоторые недобросовестные предприниматели заказывают у злоумышленников услуги по нарушению доступности инфраструктуры и веб-сайтов своих конкурентов. В июле с разницей в несколько дней DDoS-атакам подверглись сразу два крупных разработчика игр — [Blizzard Entertainment](#) и [Ubisoft](#). Возможными причинами могут быть происки конкурентов или серьезное недовольство отдельных игроков политикой компаний.

Другой популярной причиной DDoS-атак является хактивизм. По политическим мотивам хакеры нарушили доступность сайта Социал-демократической рабочей партии Швеции¹⁶, заблокировали почти на сутки сайт кандидата в Конгресс США Брайана Кафорио в Калифорнии¹⁷, атаковали голландский правительственный веб-ресурс¹⁸, а также веб-сайт министерства труда ЮАР¹⁹.

¹³ bleepingcomputer.com/news/security/compromised-javascript-package-caught-stealing-npm-credentials/

¹⁴ adguard.com/en/blog/adguard-security-notice/

¹⁵ edinburghnews.scotsman.com/our-region/edinburgh/edinburgh-university-hit-by-crippling-cyber-attack-1-4798612

¹⁶ thelocal.se/20180822/swedens-social-democrats-website-hacked

¹⁷ thehill.com/policy/cybersecurity/407608-california-democrat-hit-with-ddos-attacks-during-failed-primary-bid

¹⁸ nltimes.nl/2018/08/01/ddos-attack-leaves-digid-site-unreachable

¹⁹ mybroadband.co.za/news/security/274161-hackers-did-not-compromise-our-servers-department-of-labour.html



Категории жертв

Проанализируем атаки на отдельные отрасли, которые нам показались наиболее интересными в III квартале 2018 года.

Государственные организации



Ущерб более
35 тыс. долл. США

Пострадали более
272 тысяч человек

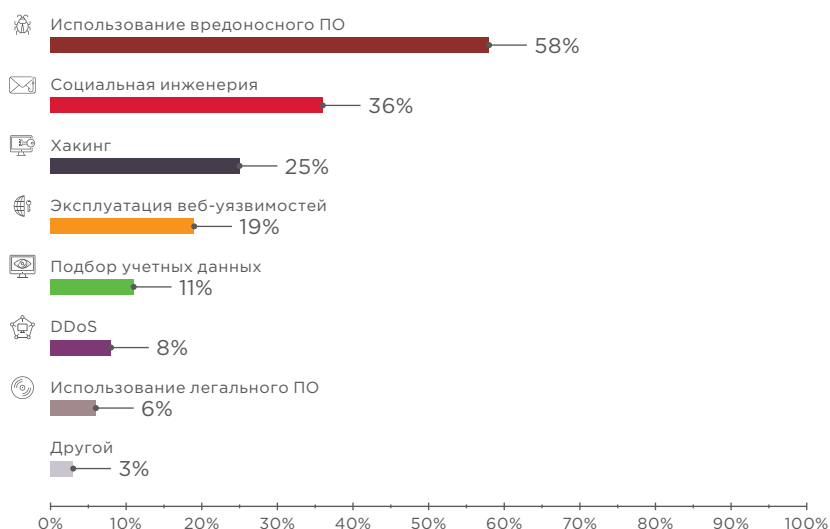


Рисунок 12. Методы атак на государственные организации в Q3 2018

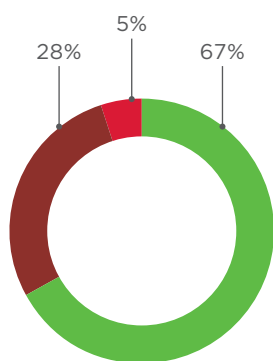
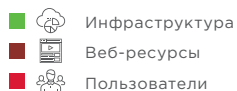


Рисунок 13. Объекты атак

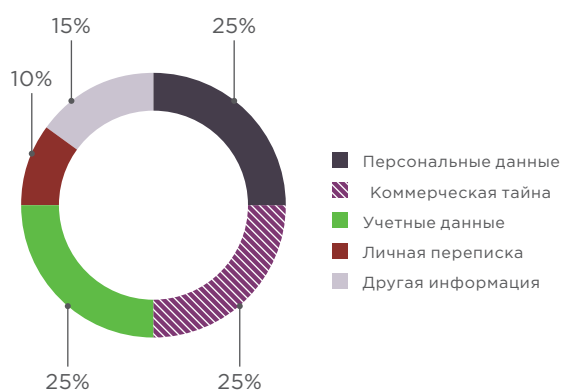


Рисунок 14. Украденные данные

Высокий интерес к секретным сведениям государственного значения заставляет злоумышленников искать новые пути проникновения в правительственные информационные системы. Интересный способ выбрали злоумышленники для доставки вредоносного ПО в правительственные учреждения США, сделав ставку на любопытство потенциальных жертв. Шпионское ПО было доставлено на обычных компакт-дисках — в конвертах по почте²⁰.

²⁰ krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/

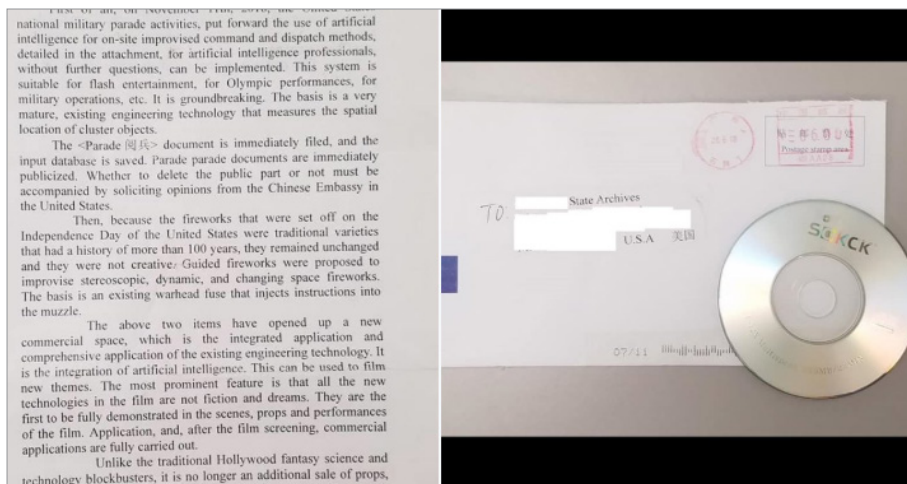


Рисунок 15. Компакт-диск с вредоносным ПО, который был доставлен
в государственное учреждение США

Интерес злоумышленников к государственным учреждениям сильно возрастает перед значимыми политическими событиями. Так, в преддверии выборов в Швеции хактивисты распространяли лозунги националистической направленности, а также ложные информационные сообщения с помощью программ-ботов в социальной сети Twitter²¹.

Но чаще мотивом злоумышленников в отношении государственных организаций становится кибершпионаж. Китайская хакерская группировка TEMP.Periscope, ранее известная благодаря своим атакам на морские предприятия, накануне выборов в Камбодже отправила²² фишинговое письмо заместителю главы оппозиционной партии от имени неправительственной правозащитной организации LICADHO. Вредоносное вложение к письму содержало загрузчик, который устанавливает на компьютер жертвы набор шпионского ПО.

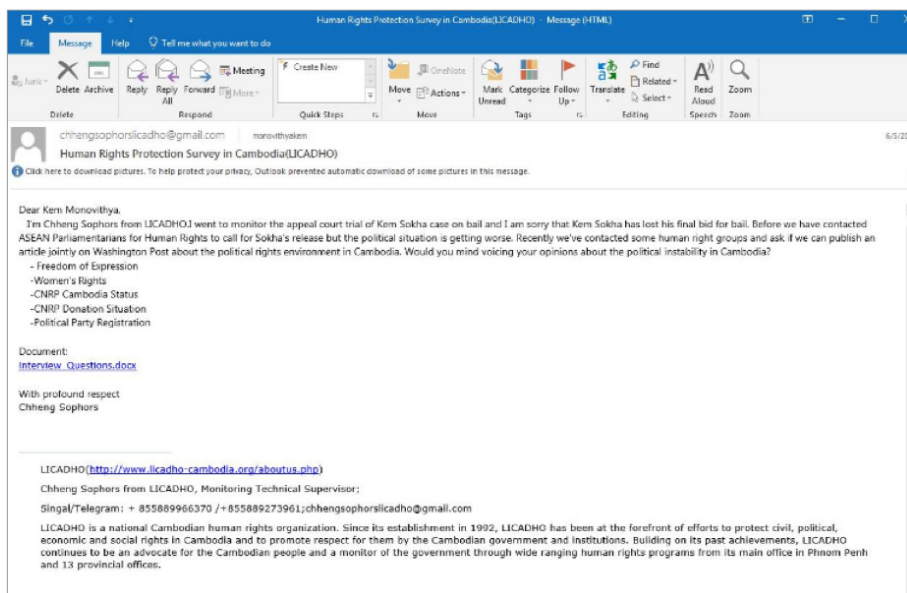


Рисунок 16. Фишинговое письмо с вредоносным вложением

21 [bloomberg.com/news/articles/2018-08-30/
sweden-sees-increase-in-cyber-attacks-seeking-to-disrupt-vote?cmpid=flipboard](https://www.bloomberg.com/news/articles/2018-08-30/sweden-sees-increase-in-cyber-attacks-seeking-to-disrupt-vote?cmpid=flipboard)

22 [fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-
elections.html](https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html)



Ущерб порядка
18 млн долл. США

Пострадали более
350 млн человек

Финансовые организации

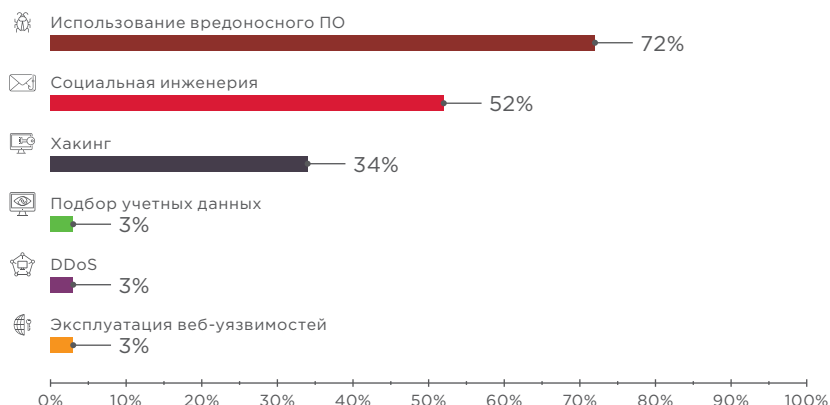


Рисунок 17. Методы атак на финансовые организации в Q3 2018

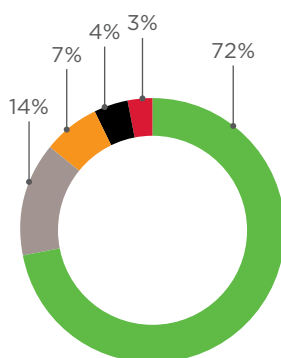
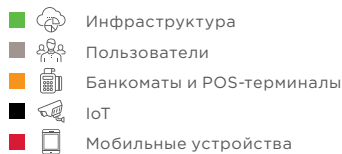


Рисунок 18. Объекты атак

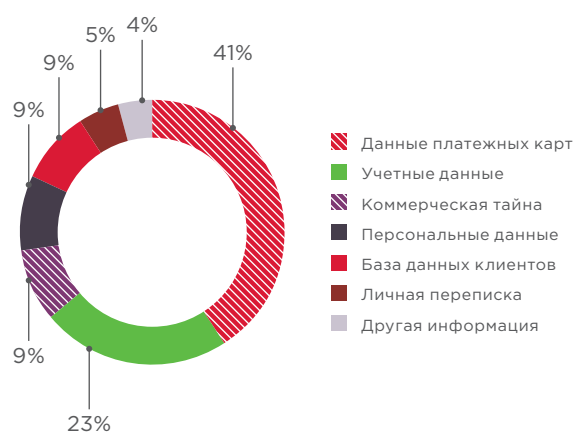


Рисунок 19. Украденные данные

Третий квартал ознаменовался атаками на финансовые организации со стороны ряда АРТ-группировок. Прежде всего необходимо упомянуть атаку²³ MoneyMaker на сетевую инфраструктуру российского «ПИР Банка», которая закончилась кражей более 58 млн рублей. Еще более крупная атака совершена²⁴ на индийский Cosmos Bank, что повлекло потерю порядка 13 млн долл. США. К преступлению, по всей видимости, причастна²⁵ североамериканская группировка APT38. В III квартале участились атаки группировки Cobalt на банки: специалисты PT ESC зафиксировали 12 атак в период с июля по сентябрь. Если в июле злоумышленники традиционно использовали JavaScript-бэкдор, то с августа они перешли на распространение вредоносного ПО CobInt. Фишинговые рассылки в августе и начале сентября проводились с поддельных доменных адресов, якобы принадлежавших платежной системе Interkassa, а также Европейскому центрбанку и банкам BBVA Compass Bancshares, Unibank, Альфа-Банку, Райффайзенбанку.

²³ banki.ru/news/lenta/?id=10554013

²⁴ <https://www.hindustantimes.com/india-news/15-000-transactions-in-7-hrs-cosmos-bank-s-server-hacked-rs-94-cr-moved-to-hong-kong/story-wazUXZs3LRhcbPLg7LYx50.html>

²⁵ content.fireeye.com/apt/rpt-apt38



Рисунок 20. Фишинговое письмо, рассылаемое Cobalt якобы от имени Альфа-Банка

Меняются способы доставки вредоносного ПО, которые применяют участники Cobalt. В начале года злоумышленники рассылали документы с эксплойтами. Начиная с мая они перешли на документы с обфусцированными макросами, которые позволяют снизить эффективность обнаружения атаки антивирусами. С сентября группировка стала использовать PDF-документы с вредоносными ссылками, эксплуатируя при этом уязвимость Open Redirect²⁶.

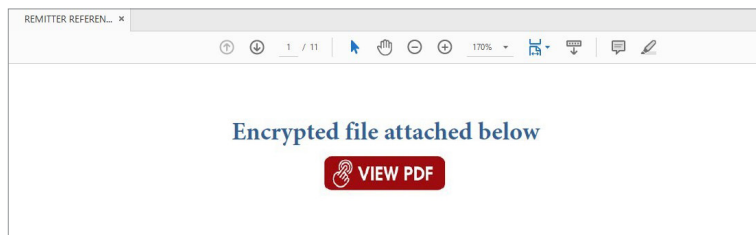


Рисунок 21. Файл в формате PDF со ссылкой на вредоносный код

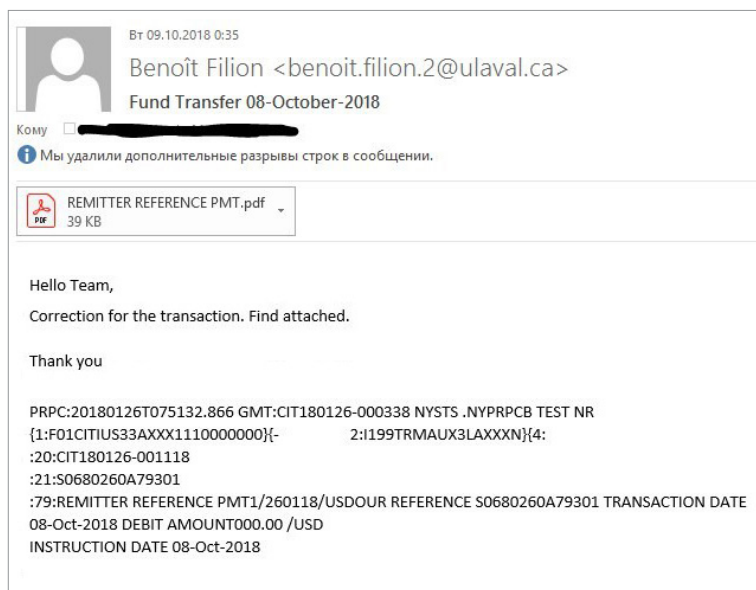


Рисунок 22. Фишинговое письмо с вредоносным PDF-документом

²⁶ openbugbounty.org/reports/81002/

Медицинские учреждения



Пострадали более
2 млн человек

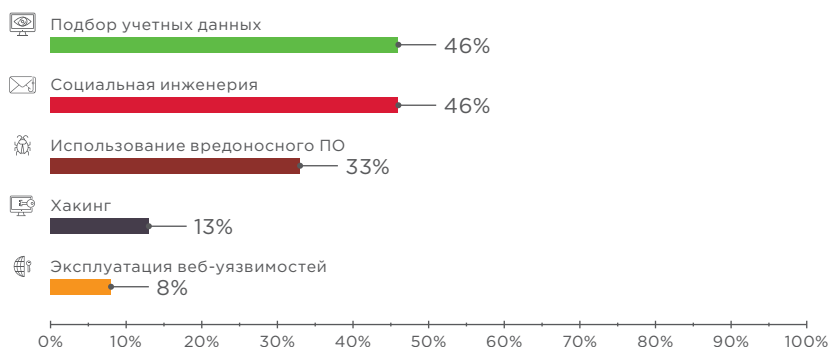


Рисунок 23. Методы атак на медицинские учреждения в Q3 2018

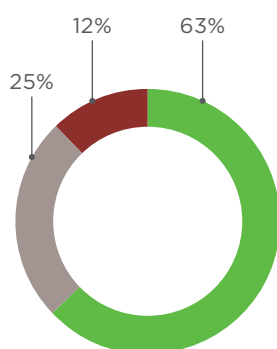
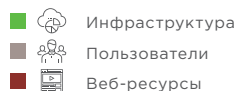


Рисунок 24. Объекты атак

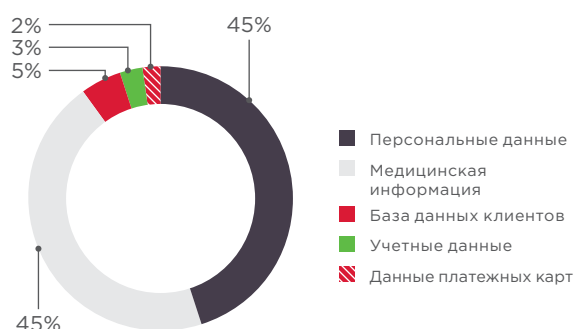


Рисунок 25. Украденные данные

Медицинские организации привлекают злоумышленников возможностью украсть данные, которые можно выгодно продать. Особенно высокую прибыль можно получить от продажи персональных и медицинских данных высокопоставленных лиц государства. Атака на SingHealth в Сингапуре закончилась кражей персональных данных более 1,5 млн человек и медицинских данных порядка 160 тыс. пациентов, включая премьер-министра страны и других членов правительства²⁷. Часто в результате фишинговых атак в руки злоумышленников попадают учетные данные сотрудников медучреждений, что открывает им доступ к закрытым базам данных. В калифорнийском медицинском центре Guardant Health подобный инцидент привел к утечке персональных и медицинских данных более тысячи клиентов²⁸.

Несмотря на снижение числа вредоносных кампаний в отношении учреждений здравоохранения (33% против 38% во II квартале), несколько медицинских центров все же были атакованы. Заражению шифровальщиками подверглись компьютеры медицинских организаций в США, Канаде, Индии и Гонконге. В большинстве случаев заражение становится возможным потому, что организации не уделяют должного внимания своевременному обновлению программного обеспечения. Процесс обновления ПО может быть трудоемким, а в случае сбоя или ошибки в обновлении под угрозой могут оказаться жизни и здоровье пациентов. Из-за уязвимости в устаревшем программном обеспечении канадская компания CarePartners в результате атаки шифровальщика подвергла угрозе медицинские и контактные данные десятков тысяч своих клиентов²⁹. Теперь компании грозят серьезные штрафы.

²⁷ moh.gov.sg/news-highlights/details/singhealth's-it-system-target-of-cyberattack

²⁸ mddionline.com/guardant-exposed-cybersecurity-threat-phishing-scheme

²⁹ cbc.ca/news/technology/carepartners-data-breach-ransom-patients-medical-records-1.4749515



Образовательные учреждения



Пострадали более
42 тысяч человек



Рисунок 26. Методы атак на образовательные учреждения в Q3 2018

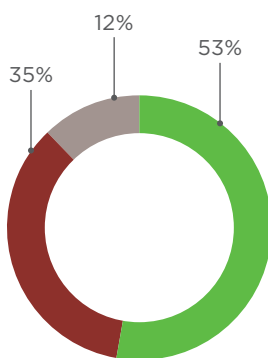
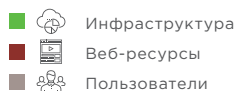


Рисунок 27. Объекты атак

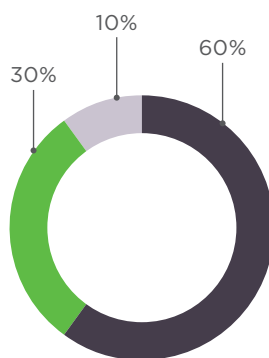


Рисунок 28. Украденные данные

Как мы уже отмечали выше, в начале учебного года, которое приходится на III квартал, ежегодно возрастает число атак на образовательные учреждения. В конце августа школы города Клокей в США второй раз за последние три года были атакованы трояном-шифровальщиком³⁰. Отразить атаку шифровальщика не смогли и в образовательных учреждениях американского округа Монро³¹.

Масштабная кампания группировки Cobalt Dickens, напротив, развернулась в самый разгар летних каникул, но затронула 76 университетов в 14 странах по всему миру³². Злоумышленники создали поддельные формы аутентификации на веб-ресурсах, якобы принадлежащих учебным заведениям, ссылки на которые разослали сотрудникам сферы образования с помощью фишинговых писем. Ворую таким способом учетные данные, хакеры охотятся за интеллектуальной собственностью.

30 spamfighter.com/News-21734-Cloquet-School-District-Again-Targeted-by-a-Ransomware-Attack.htm

31 scmagazine.com/home/news/new-gandcrab-variant-attacks-florida-school-district/

32 secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities



Частные лица



Ущерб порядка
28 млн долл. США

Пострадали около
43 млн человек

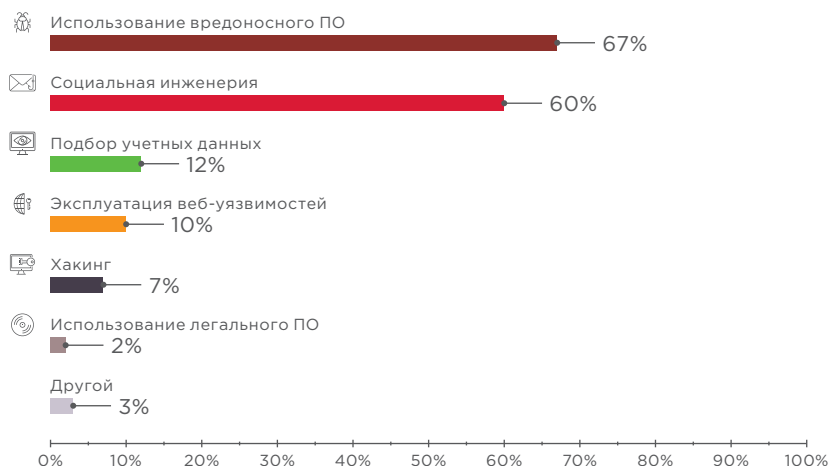


Рисунок 29. Методы атак на частных лиц в Q3 2018

- Пользователи
- Мобильные устройства
- Веб-ресурсы
- Инфраструктура
- IoT

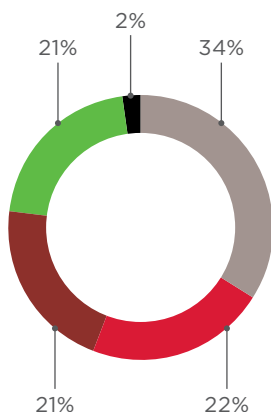


Рисунок 30. Объекты атак

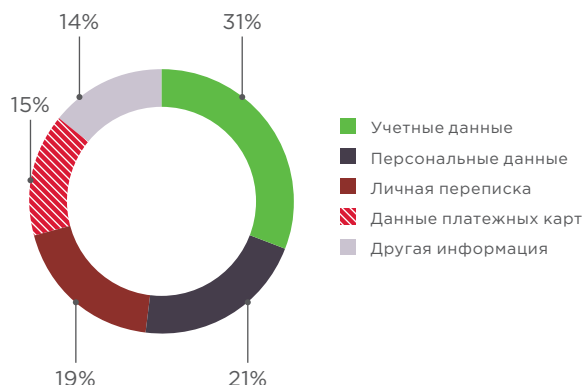


Рисунок 31. Украденные данные

В III квартале сильно выросла доля атак в отношении частных лиц с применением методов социальной инженерии (60% против 38% во II квартале). Манипулируя чувствами людей, злоумышленники успешно совершают преступные действия в отношении лиц, которые недостаточно осведомлены в вопросах кибербезопасности. Например, в августе прошла волна рассылки электронных писем, в которых сообщалось якобы о взломе телефонов и создании компрометирующих видеороликов с веб-камер жертв, за нераспространение которых вымогатели требовали денежную компенсацию³³. А в сентябре эксперты рассказали о массовой SMS-рассылке, в которой злоумышленники предупреждали владельцев банковских счетов о блокировке их карт якобы из-за подозрительных операций³⁴. Текст SMS-сообщения призывал позвонить по указанному номеру для подтверждения транзакции. Во время телефонного разговора злоумышленники узнавали данные платежных карт и выводили деньги со счетов жертв. Ущерб от этой кампании составил около 2 млн рублей.

³³ twitter.com/secguru_otx/status/1028364785631617025

³⁴ iz.ru/784746/anastasiia-alekseevskikh/blokirovka-udalas-khakery-snova-vyvodiati-dengi-s-kart-rossii

Не только данные банковских карт, но и сведения личного характера, переписка, фотографии могут представлять ценность для злоумышленников. Эта информация используется преступниками для шантажа и вымогательства. С этой целью в III квартале злоумышленники взламывали учетные записи в популярных мессенджерах и социальных сетях. Так, в августе и сентябре прошли массовые атаки на пользователей Instagram^{35,36}. Свои аккаунты потеряли тысячи человек, многие из них имели более десяти тысяч подписчиков. Законные владельцы таких аккаунтов, как правило, готовы заплатить выкуп, чтобы вернуть свою учетную запись, поскольку ранее они вложили немало ресурсов для «раскрутки» своей страницы. Если же получить выкуп злоумышленнику не удастся, он может попытаться продать эту учетную запись или использовать ее для рассылок спама.

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.

35 mashable.com/2018/08/13/instagram-hack-locked-out-of-account/?europa=true#KzywbMs8rqg6

36 cyberpolice.gov.ua/news/kiberpolicziya-vykryla-grupu-zlovmysnykiv-u-vykradenni-oblikovyh-zapysiv-korystuvachiv-soczialnoi-merezhi-6290/



Защищайте данные

- не храните чувствительную информацию в открытом виде или в открытом доступе;
- регулярно создавайте резервные копии систем и храните их на выделенных серверах отдельно от сетевых сегментов рабочих систем;
- минимизируйте, насколько это возможно, привилегии пользователей и служб;
- используйте разные учетные записи и пароли для доступа к различным ресурсам;
- применяйте двухфакторную аутентификацию там, где это возможно, например для защиты привилегированных учетных записей.

Не допускайте использования простых паролей

- применяйте парольную политику, предусматривающую строгие требования к минимальной длине и сложности паролей;
- ограничьте срок использования паролей (не более 90 дней);
- смените стандартные пароли на новые, удовлетворяющие строгой парольной политике.

Контролируйте безопасность систем

- своевременно обновляйте используемое ПО по мере выхода патчей;
- проверяйте и повышайте осведомленность сотрудников в вопросах информационной безопасности;
- контролируйте появление небезопасных ресурсов на периметре сети;
- регулярно проводите тестирование на проникновение для своевременного выявления новых векторов атак на внутреннюю инфраструктуру и оценки эффективности принятых мер по защите;
- регулярно проводите анализ защищенности веб-приложений, включая анализ исходного кода, с целью выявления и устранения уязвимостей, позволяющих проводить атаки, в том числе на клиентов приложения;
- отслеживайте количество запросов к ресурсам в секунду, настройте конфигурацию серверов и сетевых устройств таким образом, чтобы нейтрализовать типичные сценарии атаки (например, TCP- и UDP-флуд или множественные запросы к БД);
- эффективно фильтруйте трафик для минимизации доступных внешнему злоумышленнику интерфейсов сетевых служб.

Позаботьтесь о безопасности клиентов

- повышайте осведомленность клиентов в вопросах ИБ;
- регулярно напоминайте клиентам о правилах безопасной работы в интернете, разъясняйте методы атак и способы защиты;
- предостерегайте клиентов от ввода учетных данных на подозрительных веб-ресурсах и тем более от сообщения такой информации кому бы то ни было по электронной почте или во время телефонного разговора;
- разъясняйте клиентам порядок действий в случае подозрений о мошенничестве;
- уведомляйте клиентов о событиях, связанных с информационной безопасностью.



Как вендору защитить свои продукты

- применяйте все те же меры защиты, что рекомендованы для обеспечения безопасности организации;
- внедрите процессы обеспечения безопасности на протяжении всего цикла разработки ПО;
- проводите регулярный анализ защищенности ПО и веб-приложений, включая анализ исходного кода;
- используйте актуальные версии веб-серверов и СУБД;
- откажитесь от использования библиотек и фреймворков, имеющих известные уязвимости.

Как защититься обычному пользователю

Не экономьте на безопасности

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

Защищайте ваши данные

- наиболее важные файлы храните не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище;
- для повседневной работы в ОС используйте учетную запись без привилегий администратора;
- используйте двухфакторную аутентификацию там, где это возможно, например для защиты электронной почты.

Не используйте простые пароли

- используйте сложные пароли, состоящие из незначущих комбинаций букв, цифр и знаков, длиной не менее 8 символов. Для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей).
- не используйте один и тот же пароль для разных систем (для сайтов, электронной почты и др.).
- меняйте все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.

Будьте бдительны

- проверяйте все вложения, полученные по электронной почте, с помощью антивирусного ПО;
- с осторожностью относитесь к сайтам с некорректными сертификатами и учитывайте, что введенные на них данные могут быть перехвачены злоумышленниками.
- будьте предельно внимательны при вводе учетных данных на веб-сайтах и во время работы с онлайн-платежами;
- не переходите по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности;
- не переходите по ссылкам из всплывающих окон, даже если рекламируемые компания или продукт вам знакомы;
- не загружайте файлы с подозрительных веб-ресурсов или из других неизвестных источников.

О компании

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.