

Актуальные киберугрозы

II квартал 2020 года

Содержание

Резюме	3
Сводная статистика	4
Атаки с использованием вредоносного ПО	7
Промышленность под прицелом злоумышленников	9
COVID-19 как тема для социальной инженерии	10
Учетные данные в цене	12
Ресурсы сетевых периметров под атаками	14
Коллаборация шифровальщиков	16
Не только шифровальщики требуют выкуп	17
Об исследовании	18

Резюме

По итогам II квартала 2020 года мы отмечаем:

- Количество киберинцидентов продолжило расти: мы зафиксировали на 9% больше атак, чем в I квартале 2020 года. Наибольшее число атак в первом полугодии пришлось на разгар пандемии — апрель и май.
- Существенно выросла доля атак, направленных на промышленность. Во II квартале среди атак на юридические лица она составила 15% против 10% в I квартале. Наибольший интерес к промышленности проявляют операторы шифровальщиков и кибершпионские APT-группы.
- С темой COVID-19 было связано 16% атак с использованием методов социальной инженерии. Более трети (36%) из них не были привязаны к конкретной отрасли, 32% атак направлены против частных лиц, 13% — против госучреждений.
- В киберпреступном мире растет спрос на учетные данные. Среди общего объема данных, похищенных в атаках на организации, доля учетных данных выросла вдвое по сравнению с I кварталом. Наиболее распространенные сценарии кражи учетных данных — эксплуатация веб-уязвимостей, фишинговые письма, заражение вредоносным ПО и подбор учетных данных к сервисам, доступным на сетевых периметрах компаний.
- В атаках на организации доля атак с эксплуатацией уязвимостей в ПО и недостатках конфигурации выросла до 18% (против 9% в I квартале). Под пристальным вниманием злоумышленников находятся сетевые ресурсы компаний, доступные из интернета. Злоумышленники активно эксплуатируют уязвимости в системах удаленного доступа Palo Alto, Pulse Secure и Citrix.
- На долю троянов-шифровальщиков пришлось 39% кибератак с использованием ВПО, совершенных против организаций. Четверть атак шифровальщиков против юридических лиц была направлена на промышленность. Злоумышленники продолжают шантажировать жертв публикацией данных в случае отказа платить выкуп. Операторы LockBit и Ragnar Locker и операторы Maze объединили свои усилия по продаже похищенных у жертв данных и образовали так называемый картель Maze.
- Шантаж публикацией похищенных данных и санкциями за нарушение Общего регламента по защите данных (GDPR) теперь практикуют не только операторы шифровальщиков, но и другие злоумышленники.

Для защиты от кибератак, прежде всего, мы советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. Оставаясь на удаленном режиме работы или возвращаясь к привычному ритму жизни, не стоит забывать, что киберпреступники всегда на чеку. Они регулярно обновляют арсенал своих тактик и техник, чтобы оставаться незамеченными в инфраструктуре как можно дольше. Своевременно выявить злоумышленников помогут межсетевые экраны уровня приложений (WAF), грамотно выстроенный инцидент-менеджмент, глубокий анализ сетевого трафика, технология sandbox и SIEM-системы. Последние позволяют проводить непрерывный мониторинг событий ИБ в инфраструктуре, выявлять продвинутые атаки на домены и обеспечить безопасность удаленной работы.

Сводная статистика

Число атак во II квартале выросло на 9% по сравнению с I кварталом и на 59% по сравнению с аналогичным периодом 2019 года. По нашим наблюдениям, громкие мировые события неминуемо сопровождаются ростом числа кибератак, поскольку создают благоприятную почву для применения злоумышленниками методов социальной инженерии. Так, апрель и май 2020 года стали рекордными по числу успешных кибератак. Мы связываем это со сложной эпидемиологической и экономической ситуацией в мире, которая прилась на эти месяцы.

На 9% больше кибератак, чем в I квартале 2020 года

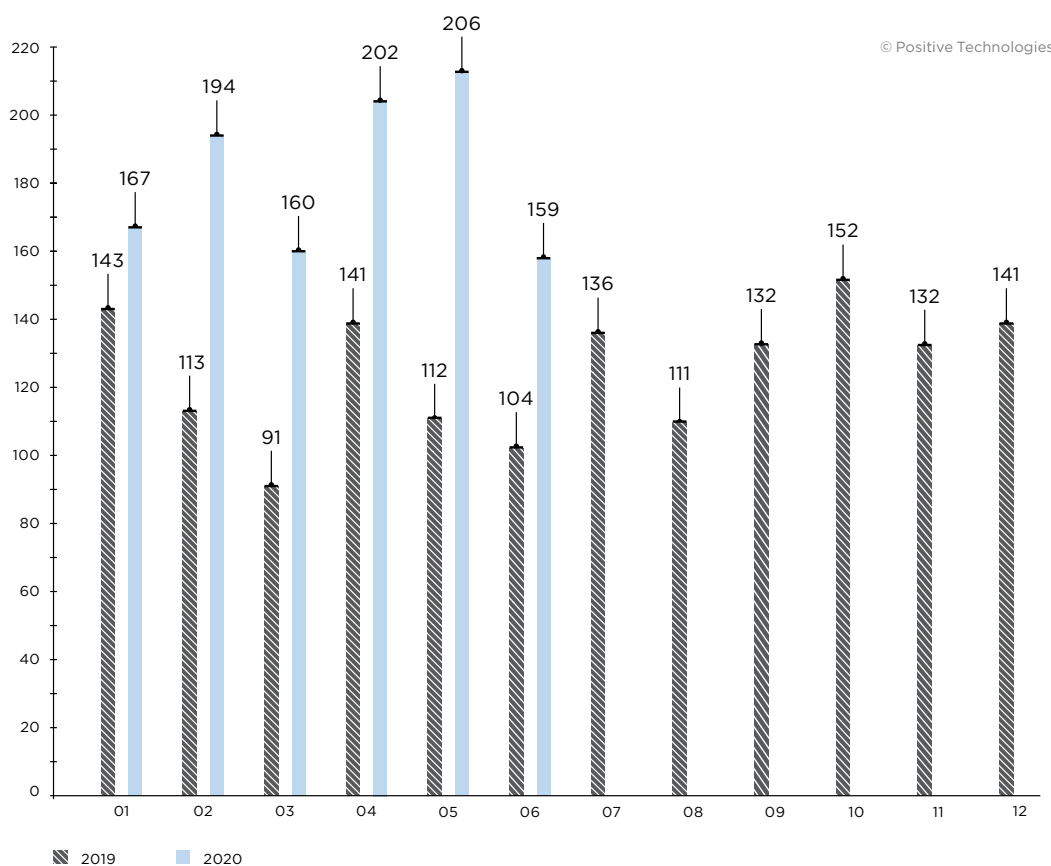


Рисунок 1. Количество атак в 2019 и 2020 годах по месяцам

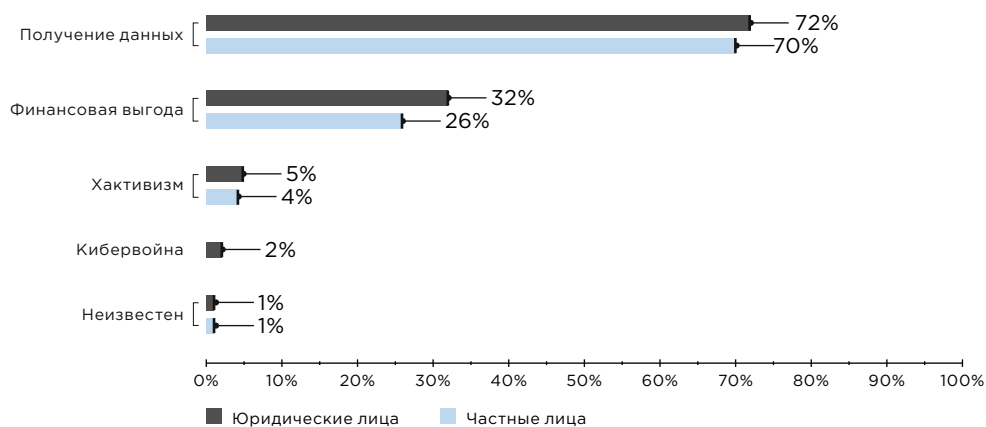


Рисунок 2. Мотивы злоумышленников (доля атак)

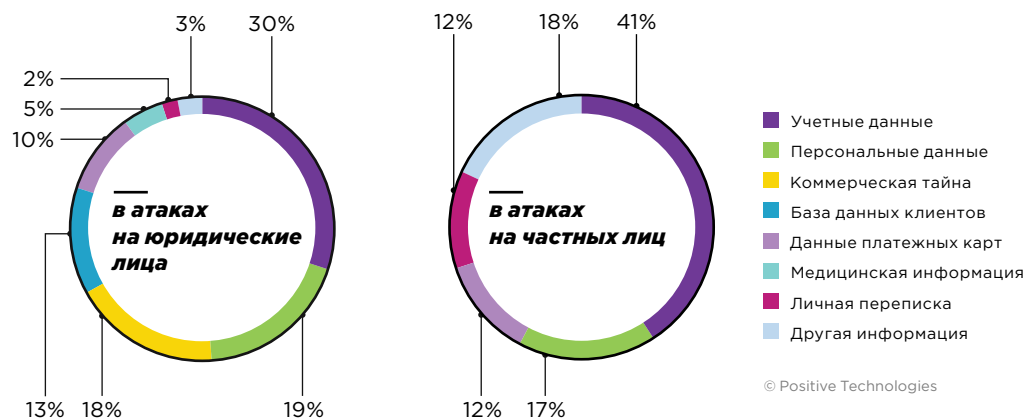


Рисунок 3. Типы украденных данных

63% атак носят целенаправленный характер

14% атак направлены против частных лиц

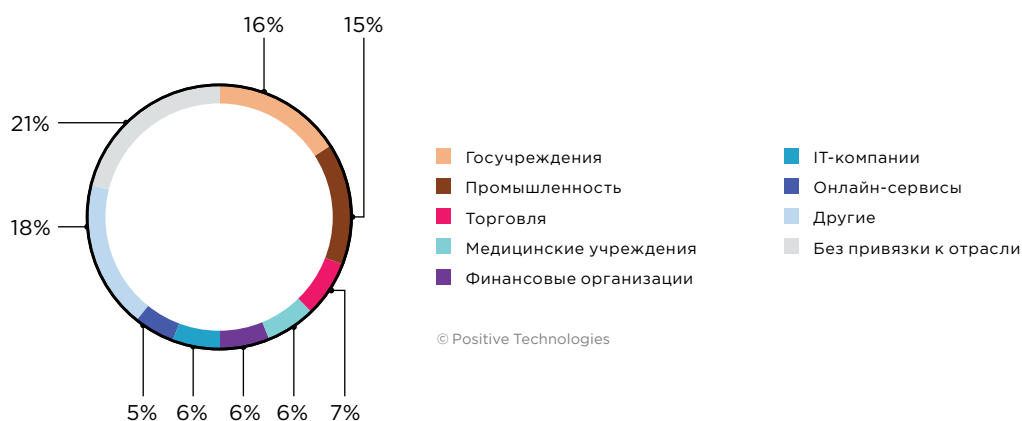


Рисунок 4. Категории жертв среди юридических лиц

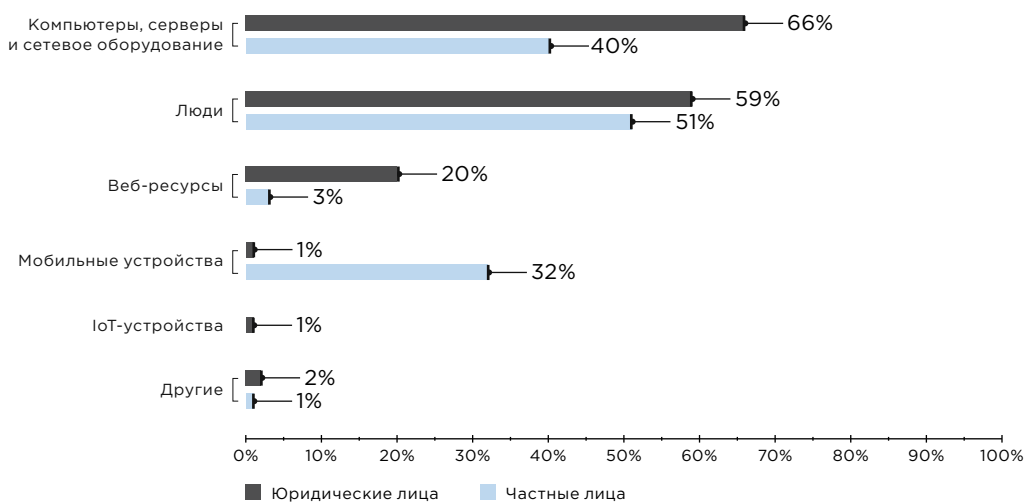


Рисунок 5. Объекты атак (доля атак)

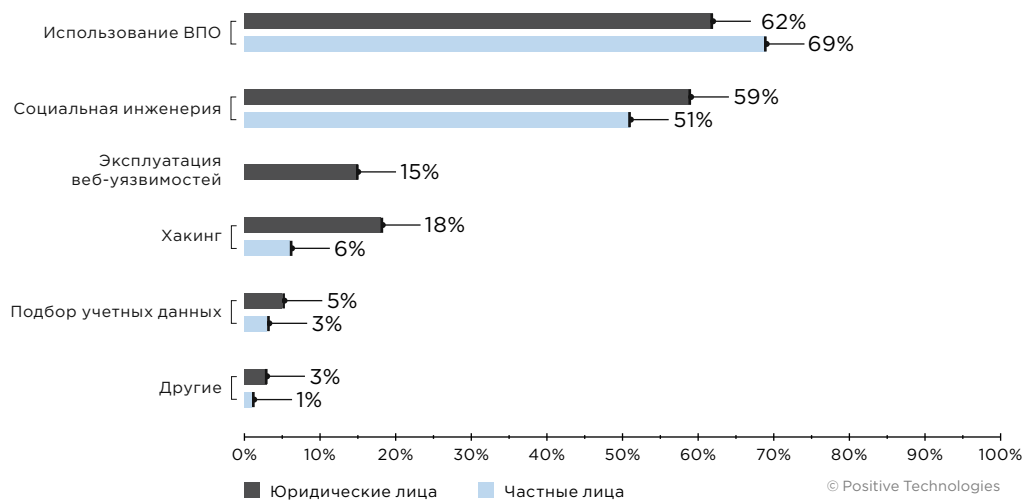


Рисунок 6. Методы атак (доля атак)

Распределение киберинцидентов по метрикам (мотивы, методы, объекты атак) и категориям жертв

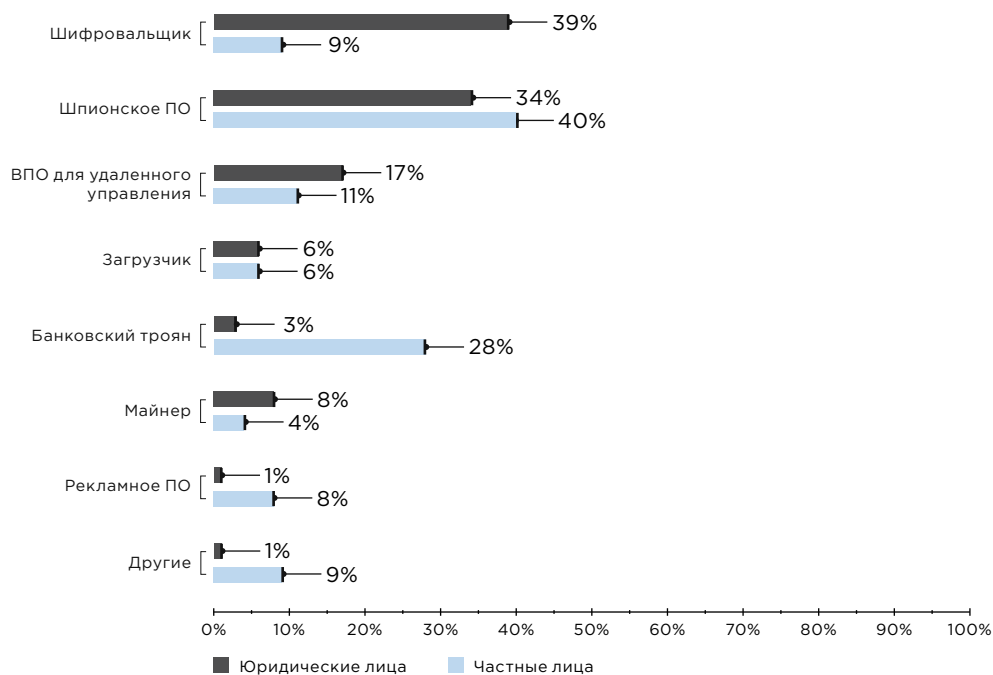
		Категории жертв									
		Госучреждения	Финансовые организации	Промышленность	Медицинские учреждения	Онлайн-сервисы	IT-компании	Торговля	Другие	Без привязки к отрасли	Частные лица
Всего атак		81	28	72	32	24	30	34	86	103	77
Объект	Компьютеры, серверы и сетевое оборудование	67	20	63	24	2	22	11	54	58	31
	Веб-ресурсы	7	3	3	5	22	5	22	17	12	2
	Люди	62	20	60	22		13	9	45	60	39
	Мобильные устройства	1							2		25
	IoT-устройства									4	
	Другие	4							5		1
Метод	Использование ВПО	66	19	63	23	3	17	9	49	54	53
	Социальная инженерия	62	20	60	22		13	9	45	60	39
	Подбор учетных данных	1	2	1	4	1	2		4	11	2
	Хакинг	13	2	9	7	3	11	2	21	19	5
	Эксплуатация веб-уязвимостей	3	1	2	2	19	1	21	15	9	
	Другие	4	1	3		1	2	2	3	1	1
Мотив	Получение данных	52	23	62	19	20	20	32	55	69	54
	Финансовая выгода	22	8	27	20	2	10	4	35	28	20
	Хактивизм	8	1			2	2	1	7	2	3
	Кибервойна	1		1	1				4	1	
	Неизвестен								1	6	1

Градацией цвета показана доля атак внутри одной категории жертв

0% 10% 20% 30% 40% 100%

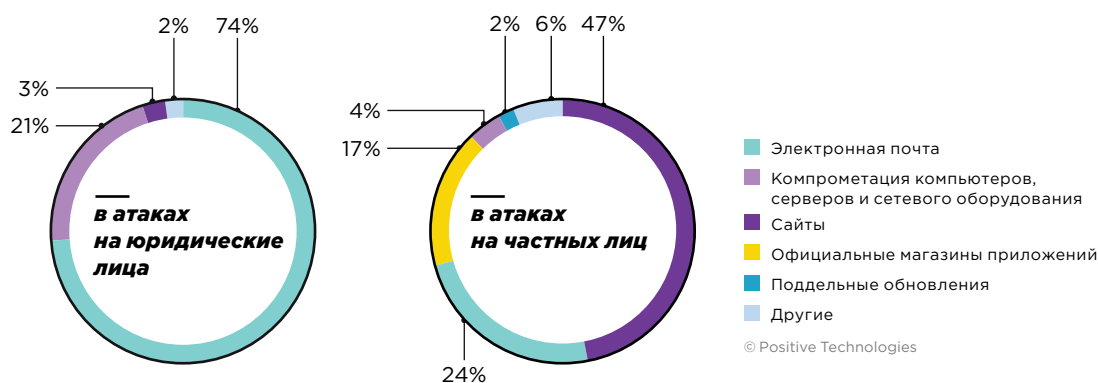
Атаки с использованием вредоносного ПО

Злоумышленники все чаще заражают жертв не одним типом вредоносного ПО, а сразу целым «букетом» троянов. Так, в ходе одной из массовых вредоносных кампаний киберпреступники доставляли на скомпрометированные компьютеры шпионское ПО LokiBot, ворующее сохраненные учетные данные из различных приложений. Помимо кражи данных, троян загружал на устройства шифровальщик Jigsaw. К слову, шифровальщики и шпионское ПО — наиболее распространенные виды троянов в атаках с использованием вредоносного ПО, их доли в атаках на организации во II квартале составили 39% и 34% соответственно.



© Positive Technologies

Рисунок 7. Типы вредоносного ПО (доля атак с использованием ВПО)



© Positive Technologies

Рисунок 8. Способы распространения ВПО

Злоумышленники дорабатывают вредоносное ПО, добавляя в него новые функции. Например, вредоносное ПО Valak, ранее выполнявшее роль загрузчика для других троянов, стало полноценным инфостилером, похищающим учетные данные и сертификаты домена. Другой пример — вредоносное ПО Sarwent. Его разработчики добавили модуль, который отвечает за предоставление удаленного доступа к зараженным узлам по протоколу RDP. Вредонос запускает на скомпрометированных узлах RDP и разрешает подключения в параметрах брандмауэра Windows. Не исключено, что полученные с помощью нового модуля доступы злоумышленники собираются продавать или сдавать в аренду другим киберпреступникам. Во II квартале мы опубликовали статью, в которой подробно рассказали о бизнесе, связанном с незаконной продажей доступов к корпоративным сетевым ресурсам.

Модернизация ВПО направлена не только на добавление новых функциональных возможностей, но и на обход средств защиты. Так, специалисты Positive Technologies Expert Security Center (PT ESC) во II квартале обнаружили обновленную версию вредоносного ПО APT-группы Calypso. Злоумышленники изменили название экспортных функций в основной библиотеке, а также установили неправдоподобное время компиляции (2021 год). Возможно, это было сделано, чтобы снизить вероятность срабатывания антивирусов.

```
Imagebase : 400000
Timestamp : 60BB3BAF (Sat Jun 05 08:54:07 2021)
Section 1. (virtual address 00001000)
Virtual size : 000221F0 ( 139760.)
Section size in file : 00022200 ( 139776.)
Offset to raw data for section: 00000400
```

Рисунок 9. Неправдоподобное время компиляции вредоносного ПО Calypso

Во II квартале 2020 года специалисты PT ESC выявили 13 атак APT-группы Gamaredon. Группа продолжает атаковать госучреждения Украины. Злоумышленники добавили в свой арсенал технику удаленной загрузки VBS-скрипта через mshta.exe. Техника предполагает использование встроенных инструментов Windows и позволяет обходить ограничения на запуск ПО, накладываемые с помощью технологии AppLocker. Запуск скрипта происходит в момент открытия LNK-файла из фишингового письма.

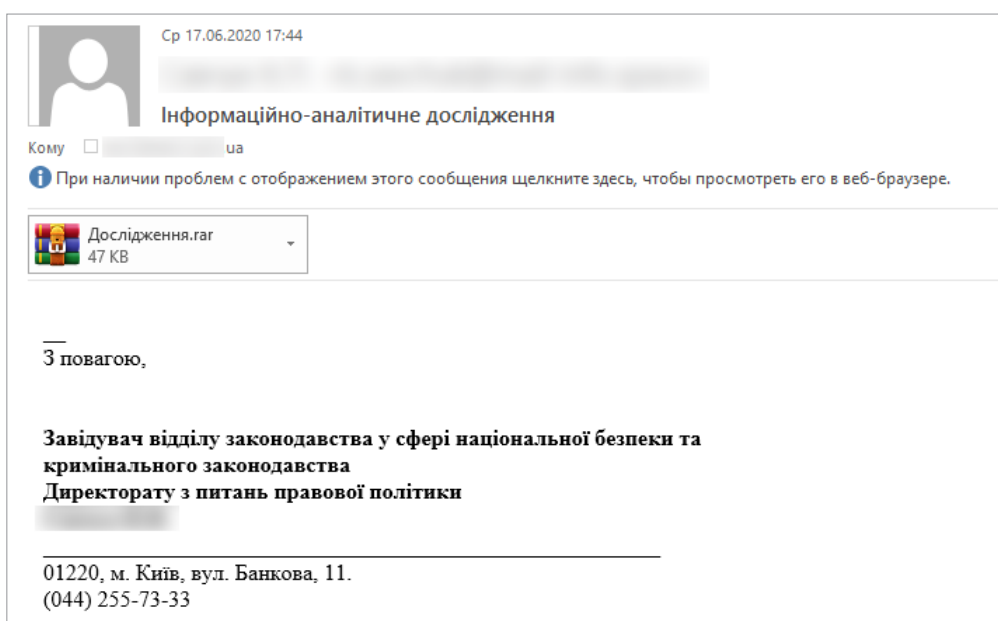


Рисунок 10. Письмо APT-группы Gamaredon в адрес госучреждения Украины

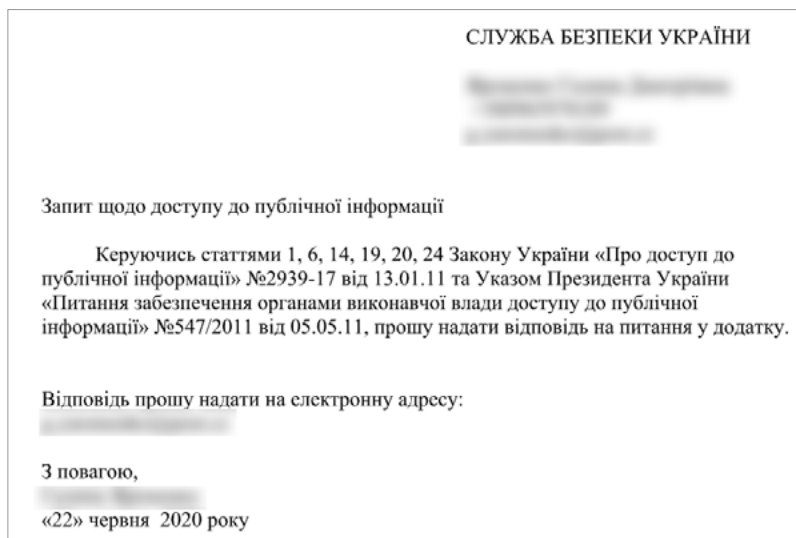


Рисунок 11. Вредоносный документ из письма Gamaredon

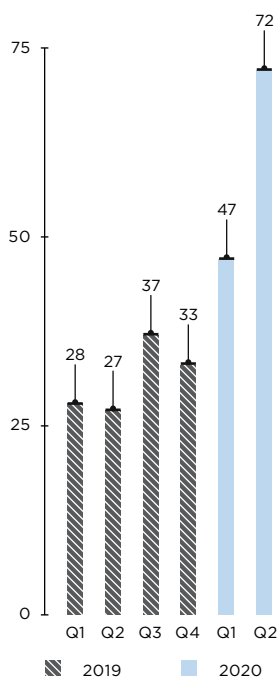


Рисунок 12. Число атак на промышленность

Промышленность под прицелом злоумышленников

Во II квартале доля промышленности в атаках на юридические лица выросла до 15% (против 10% в I квартале). В девяти из десяти атак на промышленность злоумышленники использовали вредоносное ПО. Около половины (46%) атак с использованием ВПО пришлось на шифровальщики, еще 41% — это атаки шпионских троянов.

Говоря об угрозах, актуальных в I квартале, мы рассказали о новом шифровальщике Snake, способном останавливать процессы промышленных систем управления. Во II квартале стало известно о первых жертвах — автомобильном производителе [Honda](#) и гиганте ТЭК, компании [Enel Group](#). Кроме Snake, промышленность атаковали операторы шифровальщиков Maze, Sodinokibi, NetWalker, Nefilim, DoppelPaymer.

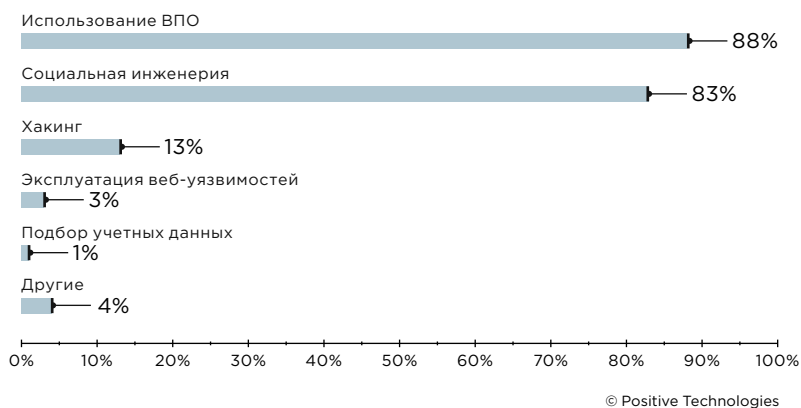


Рисунок 13. Методы атак (доля атак на промышленность)

Начальным вектором проникновения в атаках на промышленность были как фишинговые письма, так и уязвимости на сетевом периметре. Например, по мнению специалистов Bad Packets, операторы Sodinokibi [проникли в сеть компании Elexon](#) через эксплуатацию уязвимости [CVE-2019-11510](#) в Pulse Secure VPN.

Специалисты Cisco Talos рассказали об атаках на энергетический сектор Азербайджана, в ходе которых злоумышленники проявляли интерес к SCADA-системам, связанными с ветряными турбинами. Атаки начинались с писем с вредоносными вложениями, в том числе на тему коронавирусной инфекции. Через фишинговые рассылки действует и APT-группировка RTM, атакующая промышленность в России и СНГ. Во II квартале специалисты PT ESC зафиксировали 44 рассылки этой группы.

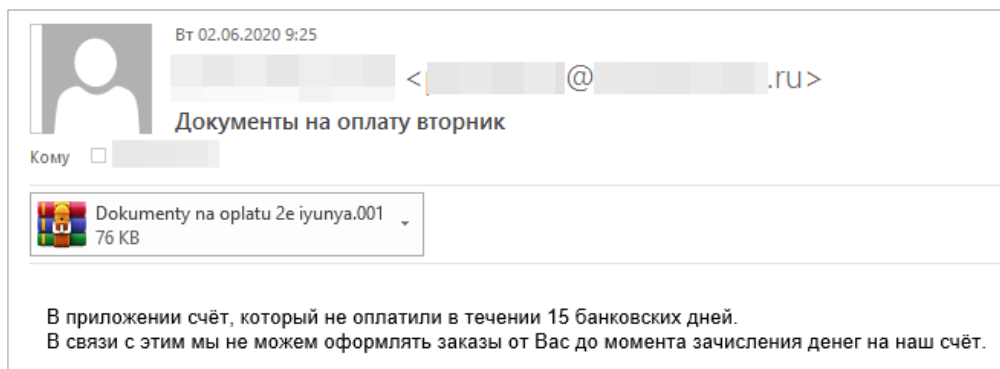


Рисунок 14. Письмо с вредоносным вложением от RTM

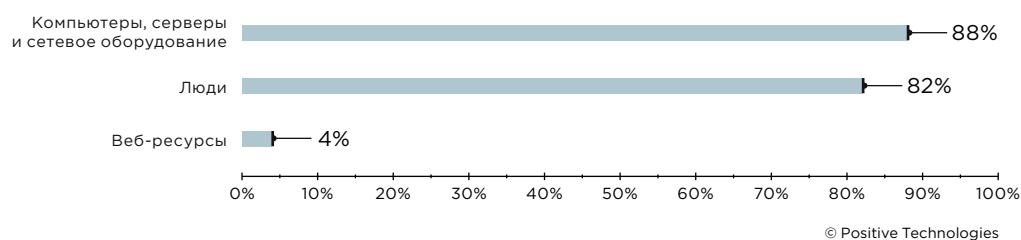


Рисунок 15. Объекты атак (доля атак на промышленность)

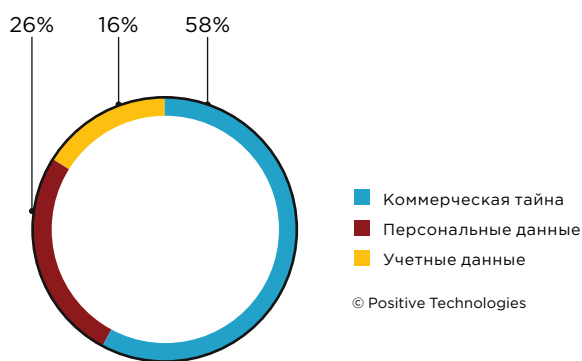


Рисунок 16. Украденные данные

COVID-19 как тема для социальной инженерии

Во II квартале злоумышленники активно использовали пандемию коронавируса. Тема COVID-19 была затронута в 16% атак с использованием методов социальной инженерии. Более трети (36%) таких атак не привязаны к конкретной отрасли, 32% атак были направлены против частных лиц. Доля атак методами социальной инженерии, в которых злоумышленники использовали тему COVID-19 против госучреждений, составила 13%.

Эксперты PT ESC выявили атаки с использованием вредоносного ПО Chinoxu на организации в Киргизии и Вьетнаме. Злоумышленники воспользовались эксплойт-билдом Royal Road для создания документа, эксплуатирующего уязвимость CVE-2018-0798 в Equation Editor. В тексте документа содержалась информация якобы о помощи ООН в борьбе с коронавирусной инфекцией в этих странах.

ООН пообещала помощь Кыргызстану в борьбе с коронавирусом

Президент Сооронбай Жээнбеков встретился с постоянным координатором системы ООН в Кыргызстане Озонниа Ожиело. Об этом сообщили в отделе информационной политики аппарата главы государства.

Стороны обсудили возможность оказания поддержки здравоохранению, образованию, обеспечению продовольственной безопасности, малому и среднему бизнесу.

Озонниа Ожиело рассказал о работе, проводимой ООН в Кыргызстане. Совместно с правительством определены восемь приоритетных секторов, в рамках которых ведется работа по противодействию дальнейшему распространению COVID-19 и преодолению его негативных последствий в социально-экономической сфере.

Он также рассказал о создании Глобального плана гуманитарного реагирования объемом в \$2 миллиарда и Экономического фонда для финансирования борьбы с «COVID-19».

Озонниа Ожиело особо подчеркнул, что Кыргызстан может рассчитывать на поддержку ООН.

Рисунок 17. Документ из рассылки с вредоносным ПО Chinoxu

В течение II квартала эксперты PT ESC выявили пять рассылок, с помощью которых доставлялась вредоносная программа KONNI. Для привлечения внимания получателей писем злоумышленники использовали информацию о средствах защиты от коронавирусной инфекции.

Face masks are only recommended for those who are taking care of a person with suspected COVID-19 Infection.

Best Type: N95 particulate respirators without respiration valve



Specification:

WHO standard

N95 or FFP2 respirator, or higher

with or without valve

Good breathability with design that does not collapse against the mouth (e.g. duckbill, cup-shaped)

Minimum "N95" respirator according to FDA Class II, under 21 CFR 878.4040, and CDC NIOSH, or

Minimum "FFP2" according to EN 149, EU PPE Regulation 2016/425 Category III, or equivalent

Рисунок 18. Документ из рассылки с вредоносной программой KONNI

Помимо тем для вредоносных писем, злоумышленники использовали пандемию для создания тематических сайтов, на которых под видом полезной информации скрывается вредоносное ПО, для кражи денег в ходе атак типа business email compromise, для распространения вредоносных мобильных приложений. Например, под видом приложения с названием Koronavirus haqida, что в переводе с узбекского языка означает «О коронавирусе», злоумышленники распространяли Android-троян SLocker, блокирующий работу мобильного устройства и требующий выкуп за восстановление работоспособности. Еще один пример — Android-шифровальщик CryCryptor, который атаковал канадских пользователей, маскируясь под приложение Covid-19 Tracer App. Чаще всего подобные мобильные трояны распространяются через сайты, поэтому мы рекомендуем не устанавливать приложения из неофициальных источников.

Учетные данные в цене

Во II квартале доля учетных данных выросла с 15% до 30% от общего объема данных, украденных при атаках на организации. В особой цене корпоративные учетные данные сотрудников. Их злоумышленники продают в дарквебе или используют для дальнейших атак, например для рассылки писем с вредоносными вложениями от имени взломанных организаций. Спросом пользуются также базы учетных данных клиентов взломанных компаний.

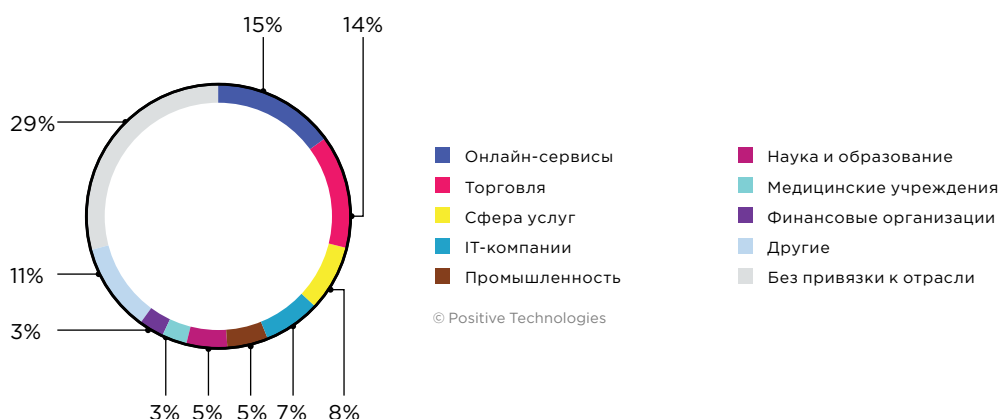


Рисунок 19. Категории жертв среди юридических лиц в атаках, направленных на кражу учетных данных

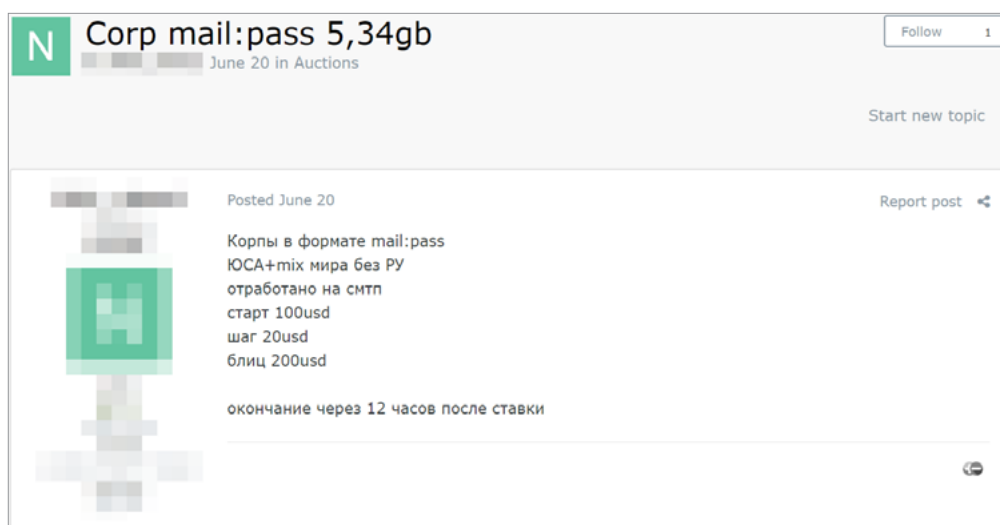


Рисунок 20. Объявление в дарквебе о продаже корпоративных учетных данных

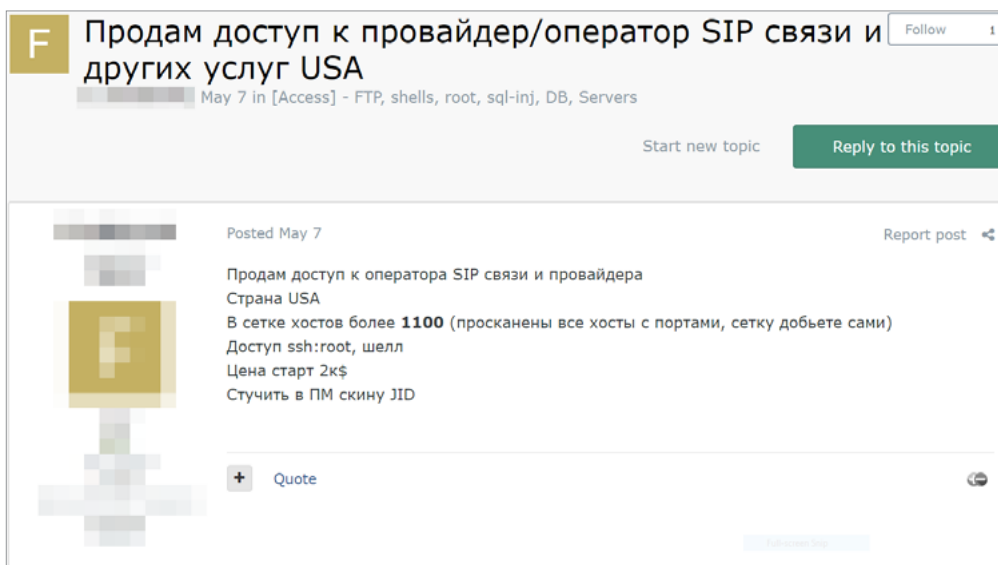


Рисунок 21. Объявление в дарквебе о продаже SSH-доступа к оператору SIP-телефонии

Рассмотрим наиболее распространенные сценарии атак, в ходе которых во II квартале 2020 года в руки злоумышленников попали учетные данные.

1. **Взлом веб-ресурсов и кража базы учетных данных.** Жертвами во II квартале преимущественно становились онлайн-сервисы, интернет-магазины и организации сферы услуг. Как правило, в ходе таких атак злоумышленники эксплуатировали веб-уязвимости или подбирали пароли для доступа к сайтам. Киберпреступная группа Shiny Hunters во II квартале опубликовала на теневом маркетплейсе объявления о продаже баз данных десятков организаций. Среди жертв онлайн-сервис Unacademy, новостной сайт Daily Chronicle, CRM-платформа Кноск. Стоимость одной базы данных колеблется от тысячи до двух тысяч долларов, но, например, базу данных интернет-магазина Tokopedia из 91 миллиона учетных записей киберпреступники оценили в 5000 долл. США.
2. **Фишинговые письма со ссылкой на поддельную форму аутентификации.** Надо отметить, что, как правило, злоумышленники подделывают формы аутентификации продуктов Microsoft — Office 365, Outlook, SharePoint. Однако во II квартале на фоне пандемии наблюдались также атаки, направленные на кражу учетных данных для подключения к системам аудио- и видеосвязи. Например, в ходе фишинговой кампании, направленной на удаленных сотрудников, использующих Skype, злоумышленники рассылали письма с фэйковыми уведомлениями от сервиса. Получатель, перейдя по ссылке из письма, попадал на поддельную форму аутентификации, где его просили ввести логин и пароль от Skype. Зафиксированы также подобные атаки на пользователей платформ Webex и Zoom.

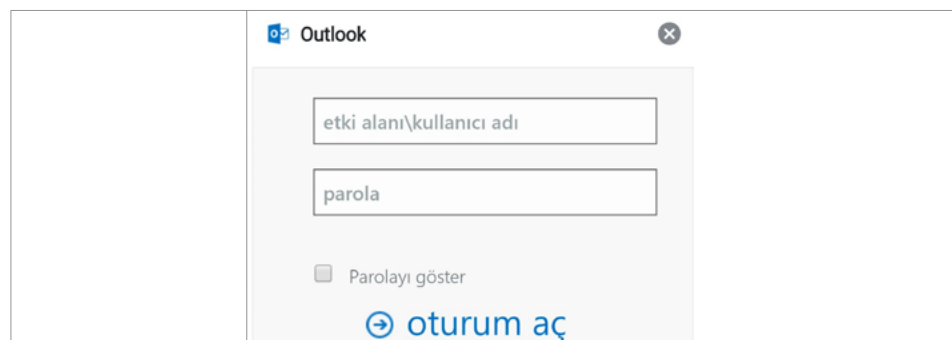


Рисунок 22. Поддельная форма аутентификации Outlook из фишинговой атаки на производителя военной техники Otokar

3. **Заражение вредоносным ПО, похищающим учетные данные.** Как правило, заражение организации происходит после того, как сотрудники открывают вложения из фишинговых писем. В последнее время актуальна угроза кражи учетных данных не только со стороны кибершпионских групп, но и со стороны операторов шифровальщиков. Так, во II квартале жертвой шифровальщика Light стала компания [Zaha Hadid Architects](#). Злоумышленники похитили множество внутренних документов компании, а также учетные записи сотрудников.
4. **Подбор учетных данных для подключения к службам, доступным на сетевых периметрах организаций.** В первом полугодии 2020 года такие атаки приобрели особую актуальность, так как многие предприятия, переводя сотрудников на удаленную работу, сделали часть сервисов доступными из интернета. Специалисты по кибербезопасности в течение апреля отметили во всем мире рост числа атак, направленных на подбор учетных данных для подключения по RDP. Чтобы не стать жертвой, необходимо использовать стойкие пароли, многофакторную аутентификацию, а также делать подключения по RDP доступными только через корпоративную сеть VPN. Если вы не используете RDP, рекомендуется закрыть порт 3389. Своевременно выявить брутфорс-атаки на корпоративные системы удаленного доступа можно с помощью специально настроенных правил корреляции в SIEM-системе.

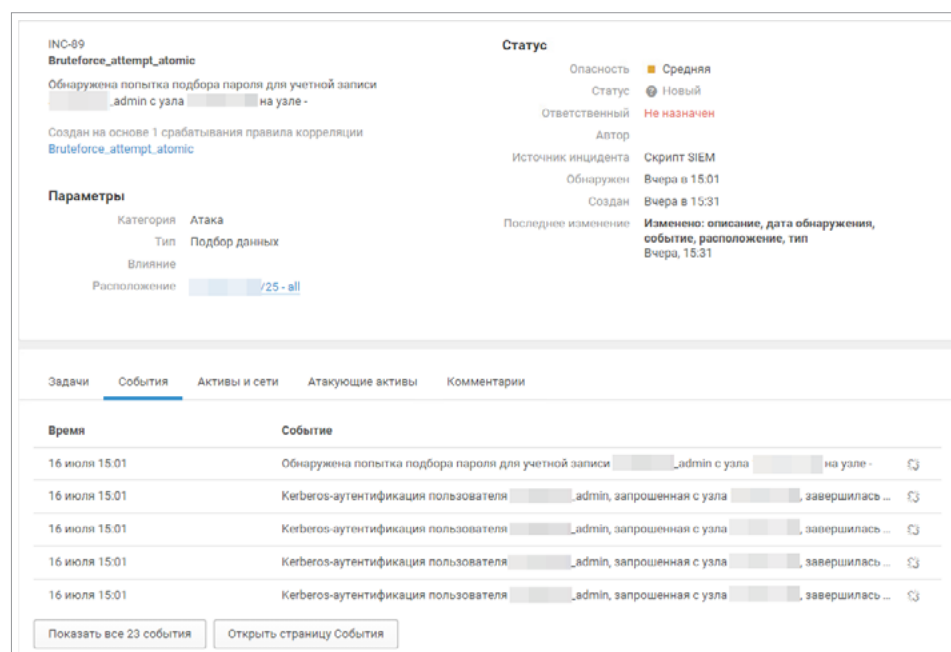


Рисунок 23. Инцидент, связанный с подбором учетных данных (интерфейс MaxPatrol SIEM)

Ресурсы сетевых периметров под атаками

Во II квартале пандемия и переход на удаленную работу спровоцировали во всем мире рост числа атак, направленных на эксплуатацию уязвимостей в корпоративных сервисах, доступных из интернета. Как следствие, доля атак с эксплуатацией уязвимостей в ПО и недостатков конфигурации во II квартале выросла до 18% (в I квартале — 9%). Киберпреступники преследовали самые разные цели — от установок майнеров до кибершпионажа в сетях крупных компаний.

**Во II квартале 2020 года злоумышленники
были нацелены на эксплуатацию уязвимостей:**

- CVE-2020-11651 и CVE-2020-11652 (SaltStack Framework)
- CVE-2019-19781 (Citrix ADC, Gateway)
- CVE-2019-11510 (Pulse Secure VPN)
- CVE-2019-18935 (Progress Telerik UI)
- CVE-2019-0604 (Microsoft SharePoint)
- CVE-2020-0688 (Microsoft Exchange)

Под особым прицелом взломщиков были системы удаленного доступа. Как мы уже отмечали выше, операторы шифровальщика Sodinokibi проникли в инфраструктуру энергетической компании Elexon в Великобритании, проэксплуатировав уязвимость CVE-2019-11510 в VPN-сервере на базе решения от Pulse Secure. Тот же вектор проникновения во II квартале использовали операторы шифровальщика Black Kingdom. Австралийский центр кибербезопасности выпустил отчет о тактиках и техниках атак, из которого следует, что эксплуатация уязвимости CVE-2019-19781 в некоторых продуктах Citrix стала одним из векторов проникновения в государственные учреждения и частные компании в Австралии. Уязвимость позволяет неавторизованному злоумышленнику выполнять произвольный код и развивать атаку на ресурсы внутренней сети компании.

Во II квартале стало широко известно о двух уязвимостях, выявленных специалистами Positive Technologies. На этот раз речь идет о межсетевом экране Cisco ASA. Уязвимость CVE-2020-3187 дает возможность неавторизованному злоумышленнику проводить DoS-атаки на сервис VPN. Вторая брешь (CVE-2020-3259) позволяет злоумышленнику получить идентификатор сессии пользователя, подключенного к VPN, и попасть во внутреннюю сеть компании. Для устранения уязвимостей советуем незамедлительно обновить Cisco ASA до последней версии.

Признаками компрометации систем удаленного доступа могут быть, например, многократные неудачные подключения к VPN, попытки подключений из VPN к узлам критически значимых подсетей, включение доступа по RDP на межсетевом экране, дублирующие подключения (параллельные сессии). Выявить подобные инциденты можно используя SIEM-системы с настроенными правилами корреляции событий ИБ.

INC-10

Detect_connect_to_significant_hosts_from_VPN

Обнаружено подключение к узлу [REDACTED] в критически важном сегменте сети с узла VPN [REDACTED]

Создан на основе 2 сработавших правила корреляции

Detect_connect_to_significant_hosts_from_VPN

Статус

Опасность ■ Средняя

Статус ● Новый

Ответственный Не назначен

Автор

Источник инцидента

Обнаружен

Создан

Последнее изменение

Скрипт SIEM

Сегодня, в 14:14

Сегодня, в 14:14

Изменено: событие 1 минуту назад

Параметры

Категория

Не определена

Тип

Не определен

Влияние

Расположение

Unmanaged hosts

Задачи

События

Активы и сети

Атакующие активы

Комментарии

Показать все 15 событий

Открыть страницу События

Рисунок 24. Выявление подключения к критически важным ресурсам из VPN в *MaxPatrol SIEM*

После публикации информации о серьезной уязвимости злоумышленники незамедлительно пытаются использовать ее в атаках. Например, уже спустя всего несколько дней после освещения уязвимости [CVE-2020-5902](#), выявленной экспертом нашей компании в контроллере доставки приложений BIG-IP от F5 Networks, наблюдались активные попытки ее эксплуатации. Уязвимость имеет высший балл по шкале CVSS. Мы считаем, что брешь могли взять на вооружение, среди прочего, и APT-группы, а значит, каждая компания, которая еще не установила официальные обновления, находится под большой угрозой. Для блокировки возможных атак, нацеленных на эксплуатацию описанных нами уязвимостей, рекомендуется использовать межсетевые экраны уровня приложений (WAF).

Коллаборация шифровальщиков

Шифровальщики — одно из самых быстроразвивающихся направлений киберпреступного бизнеса. Шантаж публикацией данных в случае отказа жертвы платить выкуп поставлен на поток. Наибольшую активность в таких атаках во II квартале 2020 года проявили операторы Maze и Sodinokibi. В лидерах по числу атак с вымогательством денег за неразглашение данных также DoppelPaymer, NetWalker, Ako, Nefilim, Clor. Некоторые, например Ako, требуют отдельно выкуп за расшифрование данных и отдельно за неразглашение.

Для продажи похищенных данных многие операторы шифровальщиков сделали собственные сайты, где публикуют список жертв и похищенную информацию, другие — размещают данные на хакерских форумах. Операторы LockBit и Ragnar Locker пошли дальше и заключили партнерское соглашение с «флагманом» отрасли Maze, и теперь операторы Maze публикуют на своем сайте данные, похищенные их партнерами. Образовался так называемый картель Maze.

Но это не единственный вариант взаимовыгодного сотрудничества среди злоумышленников. Зачастую киберпреступники, стоящие за атаками шифровальщиков, покупают доступы в организации-жертвы у других злоумышленников. Так, операторы NetWalker развернули целую кампанию по поиску партнеров для распространения их трояна-вымогателя и обещают своим подельникам долю от суммы выкупа.

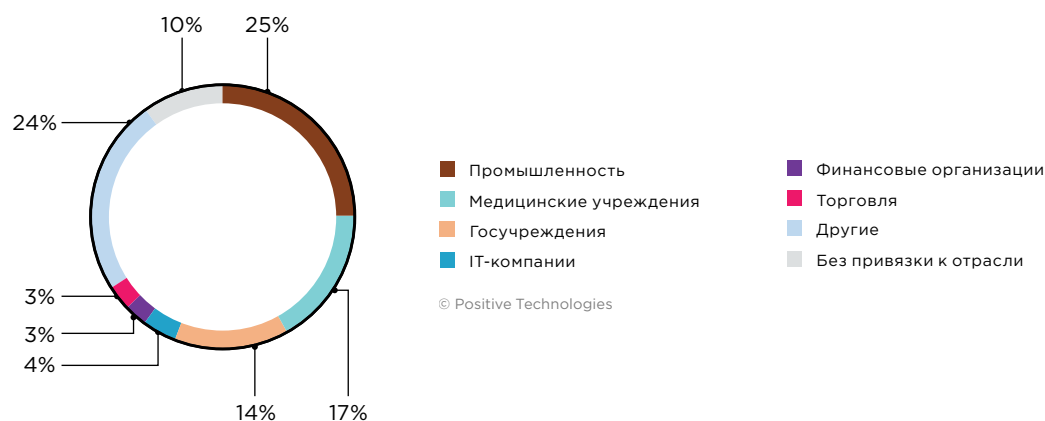


Рисунок 25. Категории жертв шифровальщиков среди юридических лиц

Несмотря на необходимость делиться прибылью с подельниками, владельцы шифровальщиков остаются в плюсе. Во II квартале 2020 года они «заработали» миллионы долларов США. После атаки шифровальщика NetWalker руководство медицинского исследовательского университета в Калифорнии приняло решение заплатить вымогателям выкуп в размере 1,14 млн долл. США. Операторы шифровальщика Sodinokibi взломали американскую юридическую компанию Grubman Shire Meiselas & Sacks (GSMS), клиентами которой являются многие знаменитости. Не получив в назначенный срок выкуп в размере 21 млн долл. США, киберпреступники сначала удвоили сумму, после чего начали выставлять на продажу похищенные данные известных людей. Злоумышленники утверждают, что им уже удалось найти покупателя информации о Дональде Трампе. В мае Sodinokibi ввели на своем сайте аукционы и в качестве первого лота выставили на продажу досье на певицу Мадонну.

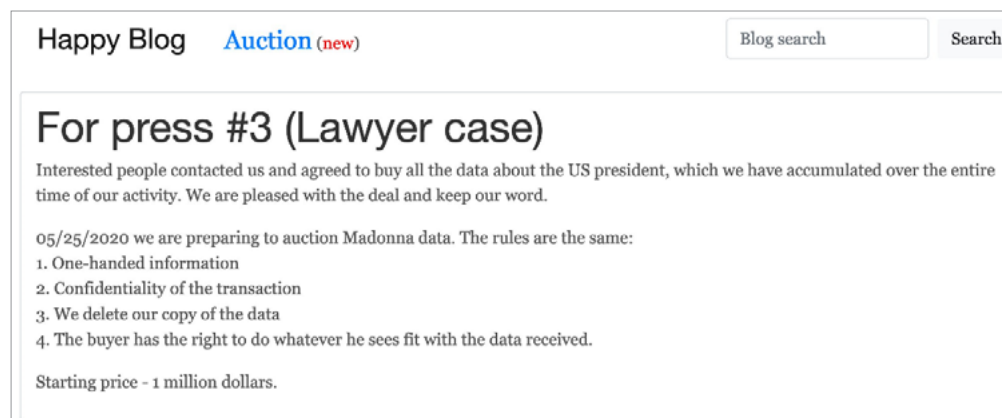


Рисунок 26. Объявление о начале аукционов на сайте Sodinokibi

Не только шифровальщики требуют выкуп

Тренд на требование выкупа за неразглашение похищенных данных подхватили и другие злоумышленники. Так, взломщики интернет-магазинов предлагают жертвам заплатить выкуп, чтобы преступники не продавали данные третьим лицам. По сравнению с операторами Sodinokibi они требуют более скромные суммы — порядка 500 долл. США. Тем

не менее такая бизнес-модель позволяет злоумышленникам в разы увеличить свои доходы, ведь зачастую законные владельцы баз данных мотивированы платить, чтобы сохранить свою репутацию, а киберпреступникам не приходится тратить время на поиск покупателей.

Еще одна группа киберпреступников взламывает сетевые хранилища LenovoEMC, удаляет данные и требует выкуп в размере от 200 до 275 долл. США за их возвращение. Аналогичные кампании во II квартале проводились и в отношении плохо защищенных баз данных MongoDB. В этих атаках злоумышленники удаляют скомпрометированную базу данных и далее, как и операторы шифровальщиков, шантажируют жертв возможными санкциями за нарушение Общего регламента по защите данных (GDPR), требуя выкуп в размере 140 долл. США. Отметим, что такие атаки могут проводить даже низкоквалифицированные хакеры, поскольку существуют готовые скрипты, позволяющие искать в интернете устройства со слабыми паролями или вовсе без парольной защиты. Мы рекомендуем следить за безопасностью конфигураций, использовать стойкие пароли и двухфакторную аутентификацию для доступа к важным ресурсам.

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.

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. Наше 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.

В рамках отчета каждая массовая атака (в ходе которой злоумышленники проводят, например, фишинговую рассылку на множество адресов) рассматривается как одна отдельная, а не как несколько. Термины, которые мы используем в исследовании, приведены в гlossарии на сайте ptsecurity.com.

О компании

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

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникнуть в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте ptsecurity.com.