Актуальные киберугрозы: III квартал 2022 года

Positive Technologies

ptsecurity.com

Содержание

Резюме

Итоги III квартала 2022 года:

- Количество атак увеличилось на 10% по сравнению со II кварталом 2022 года и на треть относительно аналогичного периода прошлого года.

- Доля атак на частных лиц составила 18%. Продолжается рост доли использования шпионского ПО в таких атаках (46%).

- Значительных изменений в типах используемого ВПО не наблюдается: шифровальщики остаются наиболее популярным типом вредоносов в атаках на организации. Отмечаются рост доли использования вредоносного ПО для Linux (на 18 процентных пунктов по сравнению с прошлым кварталом) и появление новых сложных фреймворков для проведения атак.

- Активность шифровальщиков остается на уровне предыдущего квартала. Вымогатели в атаках на организации больше полагались на проникновение в корпоративные системы с помощью компрометации RDP-соединений, путем эксплуатации уязвимостей или посредством услуг брокеров доступа. Наблюдался повышенный интерес операторов шифровальщиков к организациям топливно-энергетического комплекса, научным и образовательным учреждениям.

- Злоумышленники частично переключаются с нарушения основной деятельности на кражу конфиденциальной информации, преимущественно учетных данных: их доля среди остальных типов украденных данных составила 17% в атаках на орагнизации, увеличившись на 8 п. п. по сравнению с результатами II квартала 2022 года.

- Растет популярность комплектов для фишинга в атаках, направленных на сбор учетных данных. Такие комплекты включают готовые фишинговые страницы и поддельные формы ввода, скрипты для рассылки сообщений жертвам и для отправки украденных данных злоумышленникам. Активно распространяется модель «фишинг как услуга». Преступники создают платформы для распространения фишинговых наборов, и провести атаку может даже злоумышленник с низким уровнем квалификации.

- В связи с повсеместным использованием многофакторной аутентификации преступники переходят на использование обратных прокси-серверов для ее обхода.

- В III квартале мы отметили массовые атаки на веб-ресурсы: злоумышленники используют известные уязвимости популярных CMS для компрометации сайта, а также внедряют веб-скиммеры и применяют фишинговые комплекты для атак на пользователей.

Для защиты от кибератак мы прежде всего советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. Мы советуем следить за актуальностью версий используемого ПО и устанавливать обновления безопасности. Учитывая особенности третьего квартала, рост популярности фишинговых комплектов и массовые атаки с использованием методов социальной инженерии, также следует быть внимательнее при получении писем, особенно если отправитель не является доверенным лицом. Необходимо своевременно информировать сотрудников о новых схемах фишинга, тактиках и техниках мошенников. При совершении покупок или других платежей онлайн убедитесь, что используете легитимную платформу. Укрепить безопасность веб-ресурсов на периметре компании можно с помощью современных средств защиты (например, межсетевых экранов уровня приложений (WAF)). Чтобы предотвратить заражение устройства вредоносным ПО, мы советуем использовать песочницы, которые анализируют поведение файлов в виртуальной среде и выявляют вредоносную активность.

Сводная статистика

В III квартале 2022 года количество кибератак по сравнению с аналогичным периодом 2021 года увеличилось на треть, а относительно прошлого квартала — на 10%. Этот рост обусловлен продолжающимся противостоянием в киберпространстве, деятельностью хактивистов, появлением на сцене новых шифровальщиков и обновлением уже известных. С активностью шифровальщиков связана выросшая на 6 п. п. доля атак на компьютеры, серверы и сетевое оборудование организаций. Кроме того, мы отмечаем рост числа массовых атак на 4% относительно прошлого квартала.

В начале второго полугодия фокус внимания злоумышленников сместился с нарушения основной деятельности на похищение учетных данных, развитие фишинговых инструментов и подходов для проведения атак по каналам социальной инженерии.

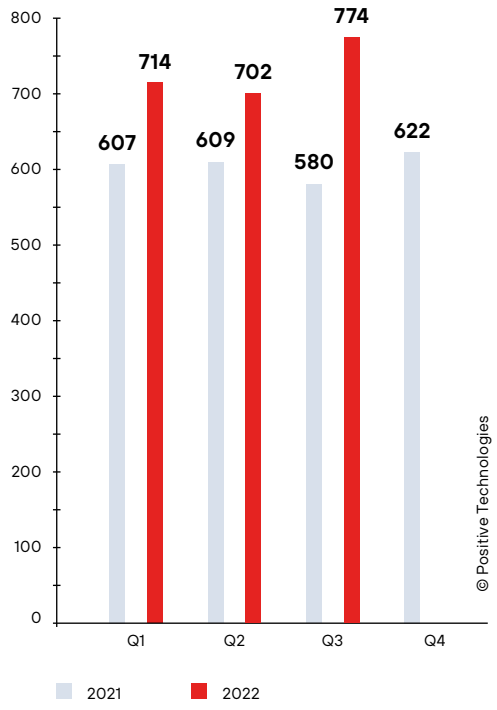

Рисунок 1. Количество атак в 2021 и 2022 годах (по кварталам)

Рисунок 2. Категории жертв среди организаций

18% атак были направлены на частных лиц

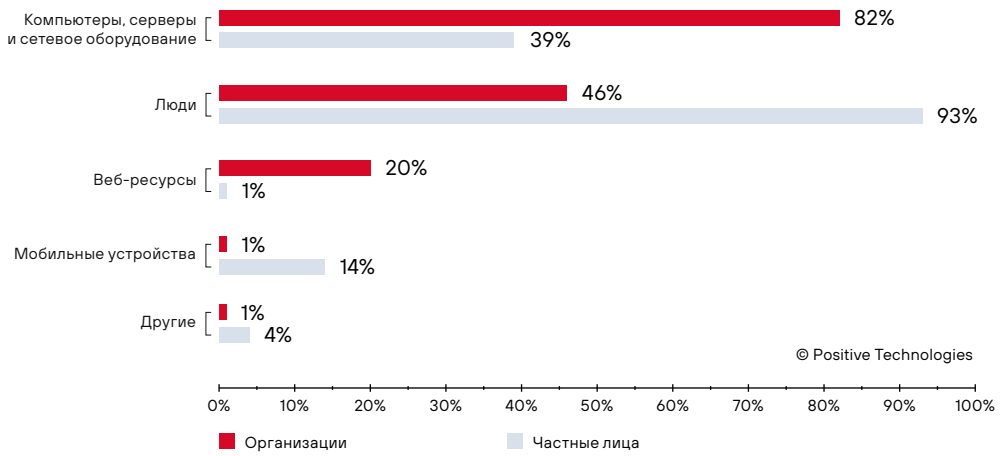

Рисунок 3. Объекты атак (доля атак)

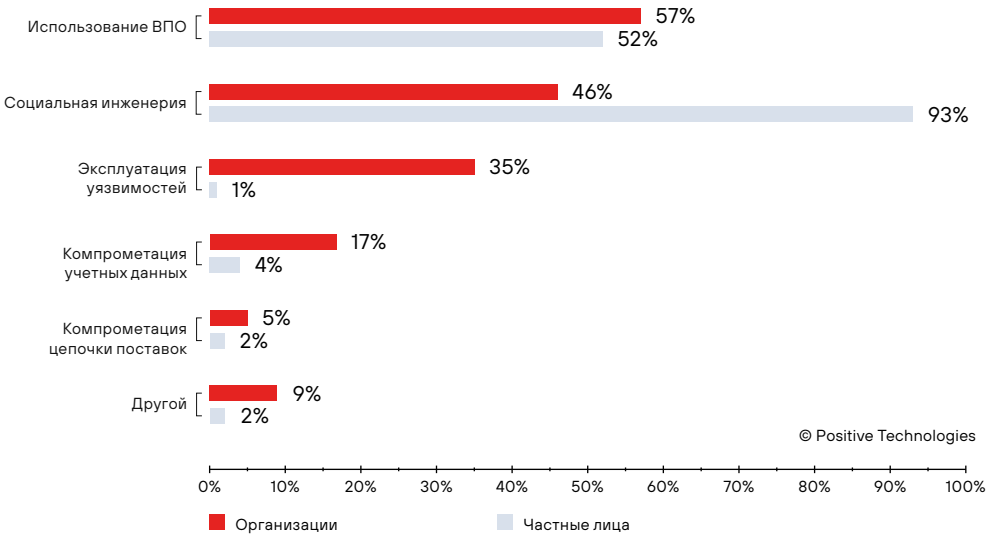

Рисунок 4. Методы атак (доля атак)

67% атак имели целенаправленный характер

Категории жертв

	Распределение кибератак по метрикам (мотивы, методы, объекты атак) и категориям жертв	Госучреждения	Промышленность	Наука и образование	Сфера услуг	IT-компании	Медицинские учреждения	Финансовые организации	Другие	Без привязки к отрасли	Частные лица
	Всего атак	**115**	**51**	**52**	**44**	**38**	**52**	**30**	**122**	**132**	**138**
Объект	Компьютеры, серверы и сетевое оборудование	90	48	49	29	33	44	27	93	111	54
	Веб-ресурсы	45	4	10	17	4	2	4	35	9	2
	Люди	48	23	30	15	16	28	16	43	76	129
	Мобильные устройства	1					1	1		3	20
	Другие			1		1			2	3	5
Метод	Использование ВПО	64	35	44	12	22	25	19	55	89	72
	Социальная инженерия	48	23	30	15	16	28	16	43	76	129
	Компрометация учетных данных	18	12	12	8	14	16	2	17	6	6
	Эксплуатация уязвимостей	27	26	8	15	11	16	11	48	63	2
	Компрометация цепочки поставок или доверенных каналов связи	5	1	5	2	2	2	1	6	5	3
	Другие	22	2	1	7	3		3	15	7	3
Последствие	Утечка конфиденциальной информации	42	31	34	24	28	44	20	57	55	88
	Нарушение основной деятельности	64	26	38	14	14	18	5	43	15	4
	Прямые финансовые потери	3	2		3	3	2	2	15	13	28
	Ущерб интересам государства	39	6						9		2
	Использование ресурсов компании или частных лиц для проведения атак	2	1	1	7	5	1	3	7	14	2
	Другое		1				1			8	11
	Неизвестно	22	5	3	4	3	1	5	20	47	21

© Positive Technologies

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

Последствия атак

В III квартале 2022 года более чем в каждой второй атаке организации сталкивались с утечкой конфиденциальной информации: доля этого типа последствий выросла на 13 п. п. Если во II квартале 2022 года конфиденциальная информация была украдена в 40% атак, то теперь в 53%. При этом мы можем заметить снижение доли атак, в результате которых была нарушена основная деятельность организаций, с 50% до 37%. Злоумышленники частично переключаются на кражу конфиденциальной информации.

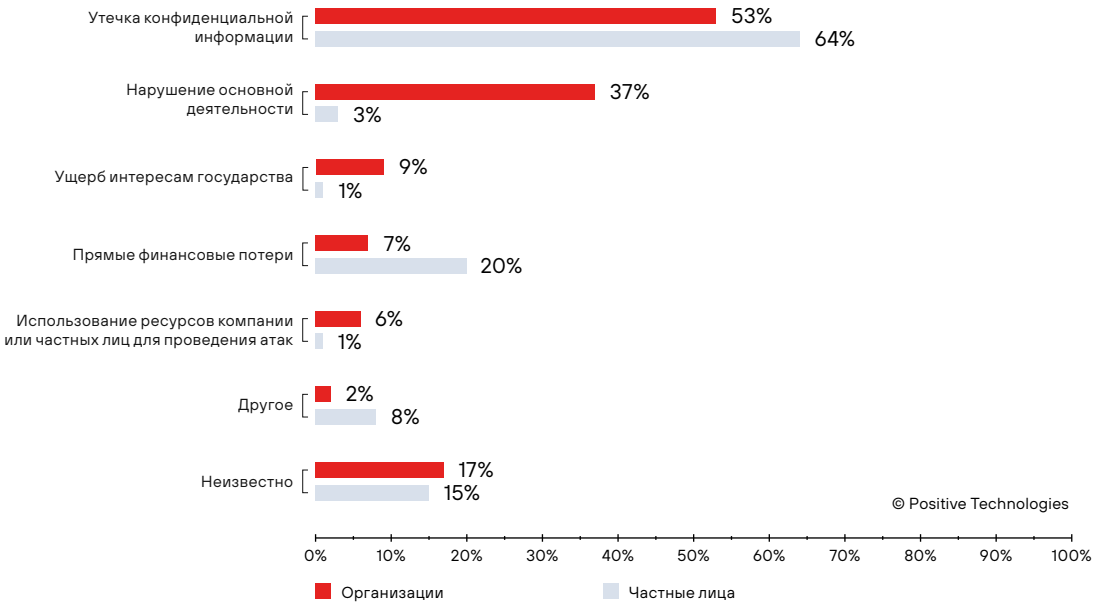

Рисунок 5. Последствия атак злоумышленников (доля атак)

Охота на учетные данные

Среди украденных данных мы отмечаем увеличение доли учетных данных с 9% до 17%. Такой рост вызван распространением наборов для проведения фишинговых атак, которое привело к многочисленным кампаниям по сбору учетных данных.

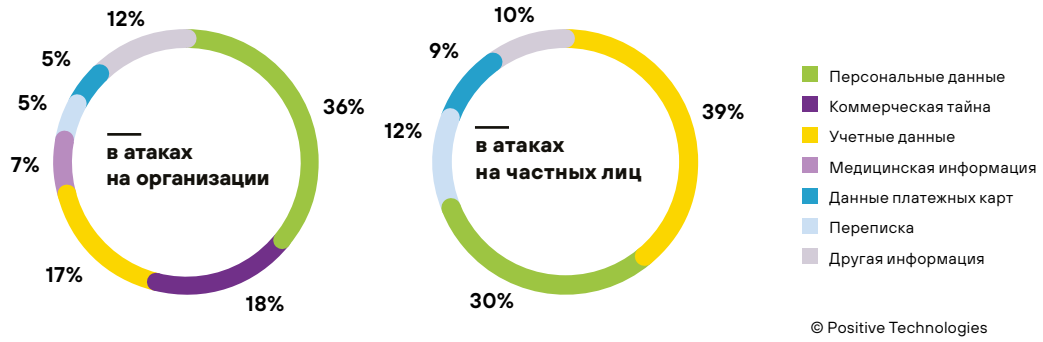

Рисунок 6. Типы украденных данных

Злоумышленники не перестают пользоваться слабостью и доверчивостью людей. Доля атак с использованием социальной инженерии остается стабильно высокой, и III квартал не стал исключением: в 93% атак был задействован человеческий фактор. Это можно объяснить: средства защиты постоянно совершенствуются, и получить доступ к инфраструктуре организации, при этом оставшись незамеченным, становится сложнее. Так, в одном из интервью участник печально известной группировки Conti[1], из-за атак которой в Коста-Рике было объявлено чрезвычайное положение, пояснил, что киберпреступники не могут победить в противостоянии технологий, поскольку это означает соперничество с многомиллиардными компаниями. Однако злоумышленники все еще могут использовать человеческий фактор в корыстных целях.

[1] Группа объявила о завершении своей деятельности, отключила свои серверы и закрыла сайт с данными о жертвах.

Данные в открытом доступе и на продажу

Рынок киберпреступных услуг увеличивает масштабы, и в ряде случаев компании могут узнать о взломе своих систем только спустя время — когда украденная информация начинает распространяться за большие суммы на теневом рынке. С такой ситуацией столкнулось подразделение популярной сети кофеен Starbucks в Сингапуре: атака была раскрыта в сентябре, когда злоумышленник разместил объявление о продаже базы, включающей персональные данные более 219 000 клиентов.

С крупными утечками столкнулись граждане Индонезии: на одном из теневых форумов пользователь выставил на продажу архив, содержащий набор данных о 105 миллионах человек — это почти 40% населения страны. Предполагается, что информация была украдена из Всеобщей избирательной комиссии. Архив содержит полные имена, даты рождения и другую личную информацию, а назначенная злоумышленником цена составляет 5000 $. Ранее преступник также выложил архив, содержащий регистрационные данные около 1,3 миллиарда SIM-карт, — номера телефонов, удостоверения личности, — стоимостью 50 000 $.

В этом же квартале мы наблюдали волну атак группировки Desorden, ранее известной как chaoscc, сопровождавшуюся активностью на криминальных форумах. Впервые под новым названием группа злоумышленников была замечена в 2021 году в атаках на азиатские организации. В основном преступники целятся на компании с высоким доходом, требуя выкуп за неразглашение украденной конфиденциальной информации.

Вредоносное ПО: число атак на Linux растет

В III квартале доля атак с использованием ВПО не претерпела значительных изменений и осталась на уровне показателей прошлого квартала: доля атак, в которых использовались вредоносы, составила 57% для организаций, для частных лиц — 52%. Шифровальщики все еще остаются наиболее используемым типом ВПО в атаках на организации, а частные лица чаще сталкивались с программами-шпионами (46%).

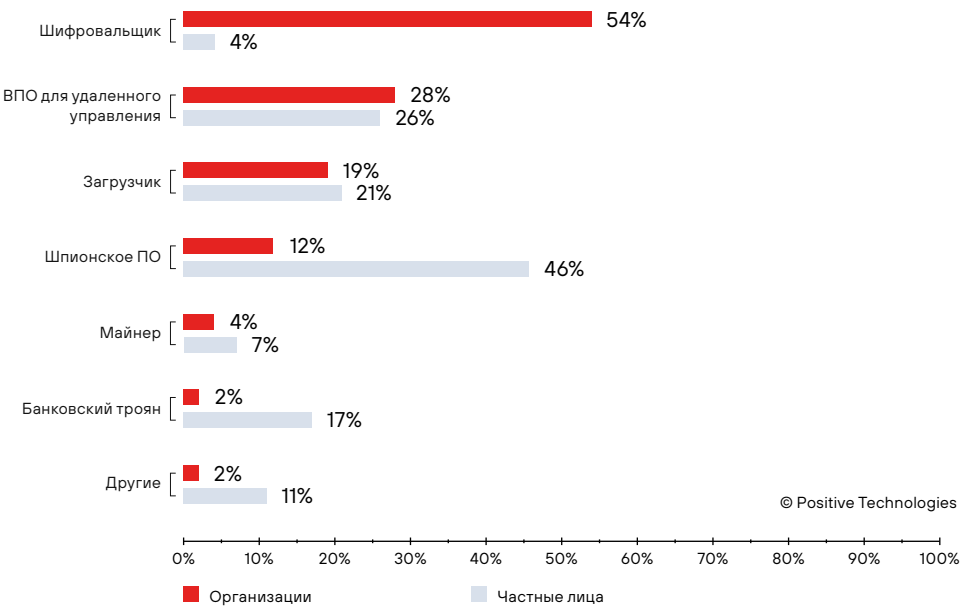

Рисунок 7. Типы вредоносного ПО (доля атак с использованием ВПО)

Шпионские штучки

Со второй половины 2021 года мы отмечаем продолжающийся рост числа атак на частных лиц с использованием шпионского ПО: злоумышленники все чаще нацелены на похищение персональных и учетных данных с личных устройств жертв, а с ростом удаленной занятости и использования личных устройств в рабочих целях это может приводить к компрометации корпоративных систем. После некоторого затишья один из популярных среди киберпреступников шпионов Raccoon Stealer возвращается с обновлениями, которые делают его более производительным и затрудняют его обнаружение.

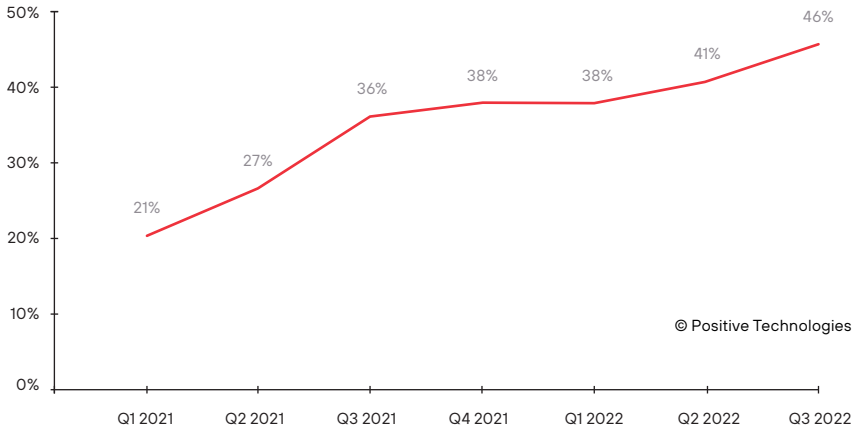

Рисунок 8. Использование шпионского ПО (доля атак на частных лиц с использованием ВПО)

По сравнению с прошлым кварталом, в атаках на организации с использованием ВПО ситуация со способами доставки вредоносов поменялась незначительно: злоумышленники все так же часто полагались на фишинговые рассылки, а также компрометировали системы с помощью уязвимостей и подбора учетных данных.

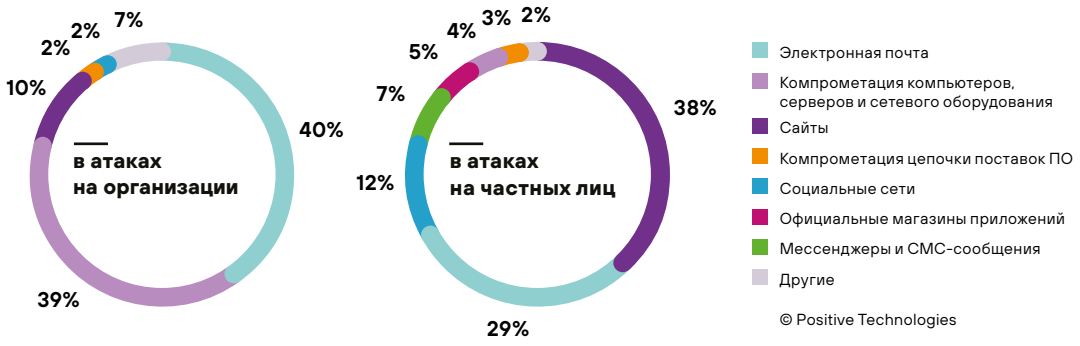

Рисунок 9. Способы распространения вредоносного ПО

В атаках на частных лиц вредоносное ПО чаще распространялось злоумышленниками через различные сайты (38%). Исследователями был обнаружен интересный экземпляр набора вредоносных программ, который распространялся в виде самораспаковывающегося архива. Основной полезной нагрузкой был стилер RedLine, но самое интересное начиналось во время его распаковки: один из исполняемых файлов скачивал видео и текстовый файл с описанием к нему и вредоносными ссылками, а второй файл с помощью API для Chrome загружал это видео на YouTube, обеспечивая тем самым самораспространение вредоносного ПО.

Linux в опасности

Множество решений виртуализации и облачных технологий базируются на системах под управлением Linux. Ландшафт атак на подобные решения расширяется с каждым днем, а последствия становятся только серьезнее из-за повсеместного внедрения виртуализации и облачных технологий в бизнес-процессы. В III квартале произошел заметный рост доли атак с использованием ВПО, которые затрагивали Linux, с 12 до 30% по сравнению с прошлым кварталом.

Исследователи Intezer в своем отчете рассказали о новой вредоносной программе Lightning, которая представляет собой модульный вредонос с обширной функциональностью — возможностью установки руткитов и других видов полезной нагрузки, активной и пассивной коммуникации с управляющим сервером по защищенному каналу. Распространение языка программирования Rust, который позволяет разрабатывать кроссплатформенное ПО, привело к появлению и обнаружению исследователями Cisco Talos нового фреймворка Manjusaka, который был протестирован в реальных атаках. Фреймворк опасен тем, что его можно использовать в атаках на системы Windows и Linux, а новая система коммуникации с управляющим сервером и свежие кроссплатформенные вредоносные импланты позволяют обходить средства защиты. Кроссплатформенные фреймворки, такие как Manjusaka, становятся новой и более опасной угрозой, чем давно известный Cobalt Strike. Распространение таких инструментов на черном рынке, как это было из-за утечки взломанной версии Brute Ratel, облегчает работу злоумышленников и кибершпионов, может вызвать значительный рост количества кибератак на самые распространенные операционные системы.

По данным исследования IBM Security X-Force, число новых шифровальщиков для Linux-систем увеличилось в 2,5 раза относительно прошлого года, и в III квартале был замечен еще один случай адаптации шифровальщика к Linux: печально известная группировка Hive, атаковавшая в прошлом квартале систему здравоохранения Коста-Рики, обзавелась свежей версией шифровальщика для систем Linux. В новой версии она получила улучшенный алгоритм шифрования, большую скрытность от обнаружения и поддержку параметров командной строки для удаленного управления.

Такое сложное, хорошо продуманное ВПО для Linux стало появляться все чаще, что должно заставить пользователей задуматься о своей безопасности. Не стоит переходить по подозрительным ссылкам и открывать непроверенные вложения. Не следует скачивать программное обеспечение из неофициальных или неавторитетных источников: это может привести к компрометации устройств. Разработчикам нужно с осторожностью относиться к загружаемым библиотекам, фреймворкам, надстройкам, а также проверять удаленные репозитории, к которым они обращаются.

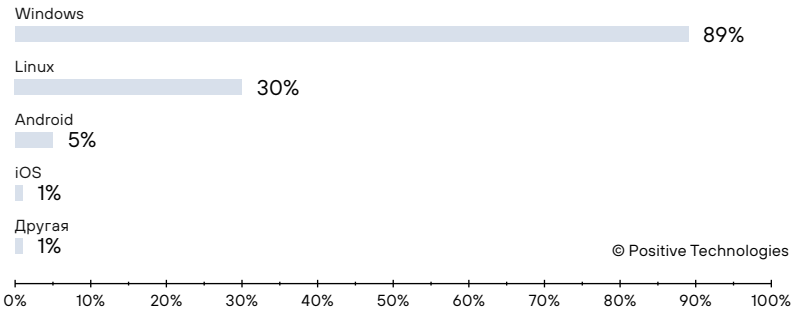

Рисунок 10. Целевые ОС в атаках с использованием ВПО (доля атак)

Новые ботнеты

Появляются и новые игроки: этим летом исследователи Cloudflare сообщили о появлении мощного ботнета, ставшего причиной одной из крупнейших DDoS-атак. Ее пик составил 26 миллионов запросов в секунду, при этом злоумышленники задействовали всего 5067 устройств. Для сравнения: согласно оценке экспертов, в прошлом году ботнет Mēris насчитывал более 200 000 зараженных устройств, при этом его пиковая мощность составила 21,8 миллиона запросов в секунду. Исследователи из Cloudflare дали новому ботнету имя Mantis и в течение нескольких недель наблюдали атаки почти на 1000 своих клиентов. В отличие от знакомых нам ботнетов, использующих устройства IoT, Mantis заражает и эксплуатирует виртуальные машины и мощные серверы: это позволяет использовать большее количество вычислительных ресурсов и увеличивать общую силу атаки.

Шифровальщики: образовательные учреждения под ударом

В III квартале активность шифровальщиков остается высокой, как и в прошлом квартале; это связано с появлением нескольких новых игроков (RedAlert, Luna, Omega), предложениями новых доступов к корпоративным сетям на черном рынке, а также с возвращением кампаний социотехнических атак. Больше половины всех атак на организации (54%) было совершено с использованием вымогательского ПО.

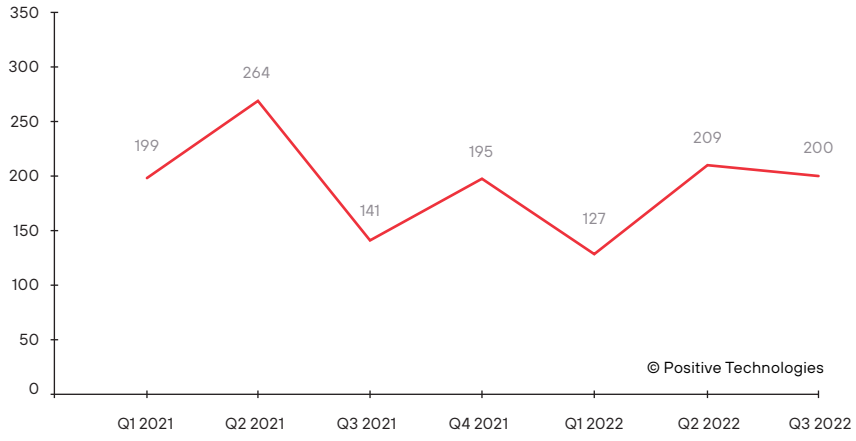

Рисунок 11. Количество атак шифровальщиков

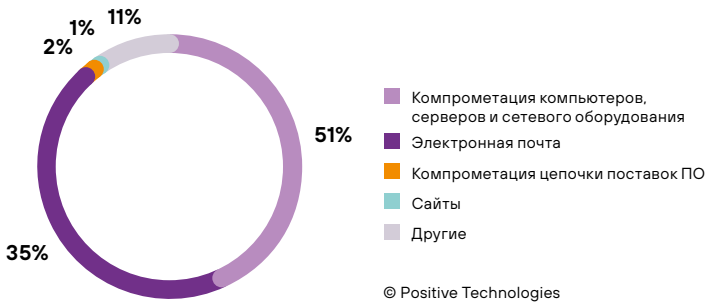

Рисунок 12. Способы распространения шифровальщиков в атаках на организации (доля атак с использованием ВПО)

Доля распространения шифровальщиков по каналам электронной почты продолжает снижаться (на 14 п. п. относительно прошлого квартала), при этом доля компрометации компьютеров и сетевых устройств увеличилась на 3 п. п. с прошлого квартала (51%); одна из причин — брокеры доступа, которые предлагают вымогателям свои услуги по проникновению в скомпрометированные системы. Например, на форуме Exploit злоумышленник утверждал, что имеет доступ к инфраструктуре одного провайдера IT-услуг и ищет тех, кто помог бы ему реализовать его. Подробнее о развитии киберпреступного рынка, продаже доступов к корпоративным сетям и их стоимости вы можете прочитать в другом нашем исследовании.

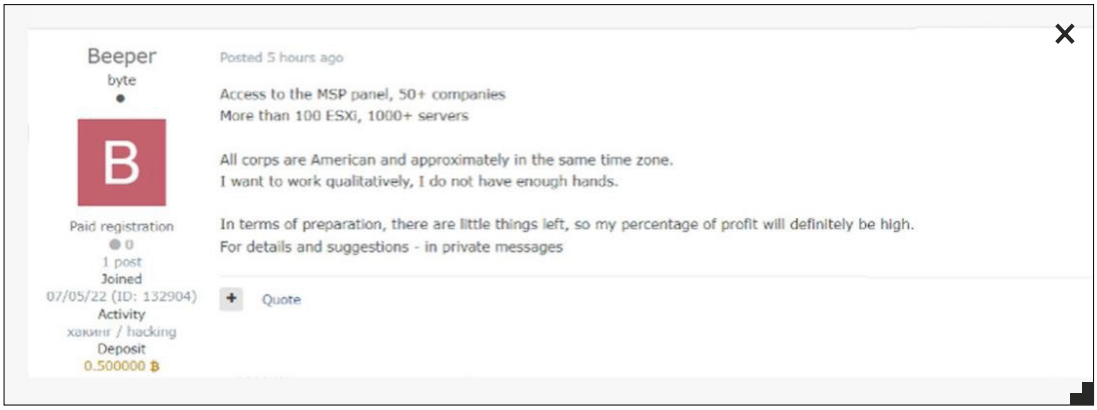

Рисунок 13. Объявление о продаже доступа к инфраструктуре

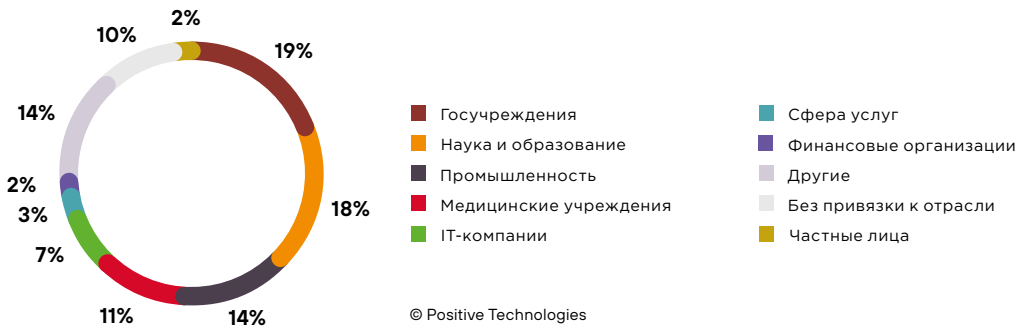

Рисунок 14. Распределение атак программ-вымогателей по отраслям

В III квартале фокус внимания вымогателей значительно сместился в сторону научно-образовательных учреждений: доля атак на эту отрасль составила 18%, что на 7 п. п. больше показателя предыдущего квартала. Группировке Vice Society удалось провести масштабную атаку на Высший совет по научным исследованиям Испании, что привело к отключению от сети более ста отделений совета и утечке идентификационных данных. Атаки с использованием программ-вымогателей не обошли стороной и учебные заведения: из-за атаки шифровальщиков школьный округ Ватерлоо был вынужден заниматься восстановлением большей части своих систем, а также уведомлять учеников, сотрудников и выпускников, которых коснулась утечка персональных данных.

Атаки на топливно-энергетический сектор

Организации промышленного сектора продолжают подвергаться натиску атак шифровальщиков: на их долю пришлось 14% таких атак. Одной из особенностей деятельности вымогателей в этом квартале является их нацеленность на организации топливно-энергетического комплекса:

- в июне из-за атаки злоумышленников BlackCat оказались недоступными клиентские порталы оператора газового трубопровода и электросети Creos Luxembourg. В результате взлома была похищена техническая документация, сведения о контрактах и данные о клиентах оператора;
- с разницей в несколько дней были совершены атаки на системы итальянского нефтеперерабатывающего гиганта Eni и итальянского энергетического агентства Gestore dei Servizi Energetici. Обе атаки привели к масштабным утечкам конфиденциальной информации, и более того — к недоступности сервисов и сбоям в обслуживании клиентов;
- группировке Ragnar Locker удалось совершить атаку на греческого оператора газовых трубопроводов DESFA, нарушить работу некоторых систем и похитить более 350 ГБ конфиденциальных данных.

Атаки на такие объекты критически значимой инфраструктуры, как организации ТЭК, и сбои в их работе могут привести к серьезным последствиям: в памяти еще свежи воспоминания об атаке на Colonial Pipeline, которая вызвала перебои в поставках и колебания цен на топливо, а атака на Венесуэльскую ГЭС вовсе привела к отключению электроэнергии по всей стране.

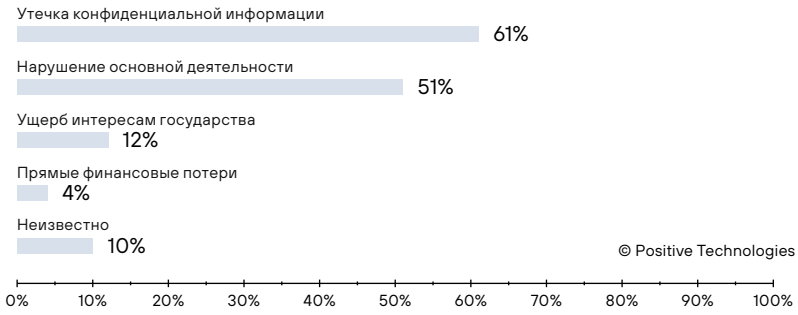

Рисунок 15. Последствия атак злоумышленников на промышленные организации

Социальная инженерия на подъеме

Рост числа массовых атак с использованием социальной инженерии мы наблюдали еще во II квартале 2022 года, однако к третьему кварталу этот тренд набрал силу: злоумышленники проигрывают техническим решениям и переключаются на человеческий фактор.

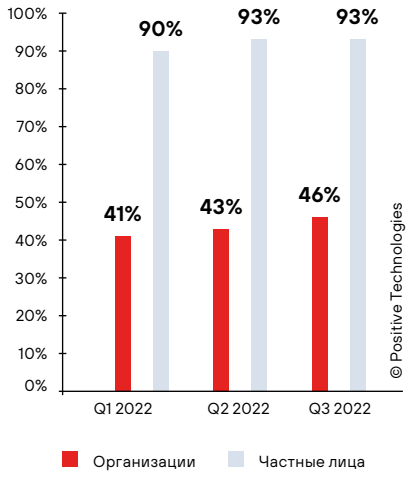

Рисунок 16. Доля атак с использованием социальной инженерии

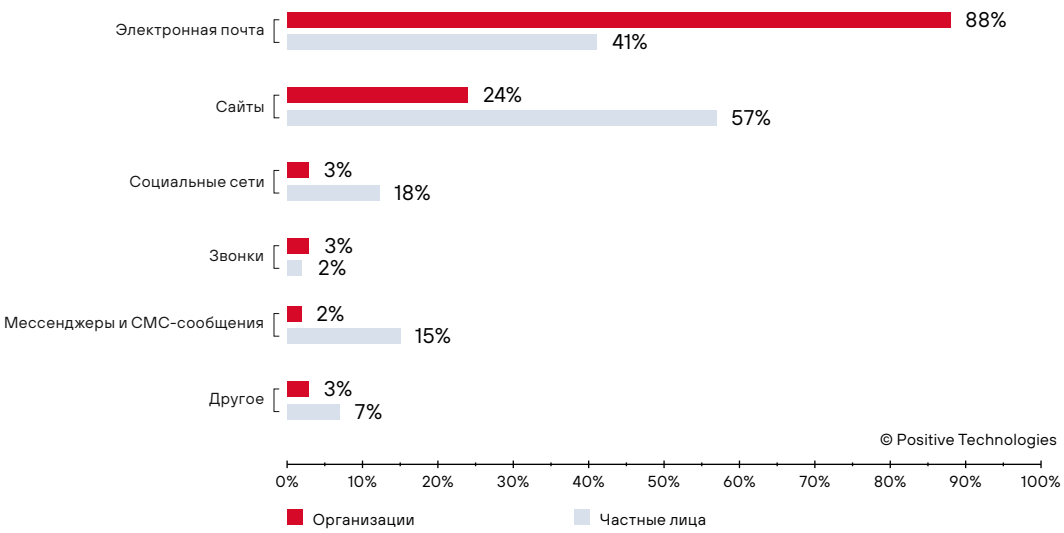

Рисунок 17. Используемые злоумышленниками каналы социальной инженерии

Как правило, чтобы обмануть и пользователей, и антивирусные программы, преступники используют совместно сразу несколько тактик.

Заимствования у операторов шифровальщиков

Чтобы повысить эффективность некоторых методов социальной инженерии, не обязательно придумывать нечто принципиально новое — можно посмотреть, как действуют «товарищи по цеху», например операторы шифровальщиков. В одной из фишинговых атак в середине лета злоумышленники использовали таймер обратного отсчета. Изначально жертвы получали письмо о подозрительной попытке входа в аккаунт. Для подтверждения адреса электронной почты злоумышленники призывали перейти по ссылке, где жертвам предлагалось ввести свои учетные данные в течение часа, иначе якобы аккаунт будет удален. Кроме таймера на странице также случайно генерировался список учетных записей на основе домена целевой организации, якобы удаляющихся в данный момент с сервера.

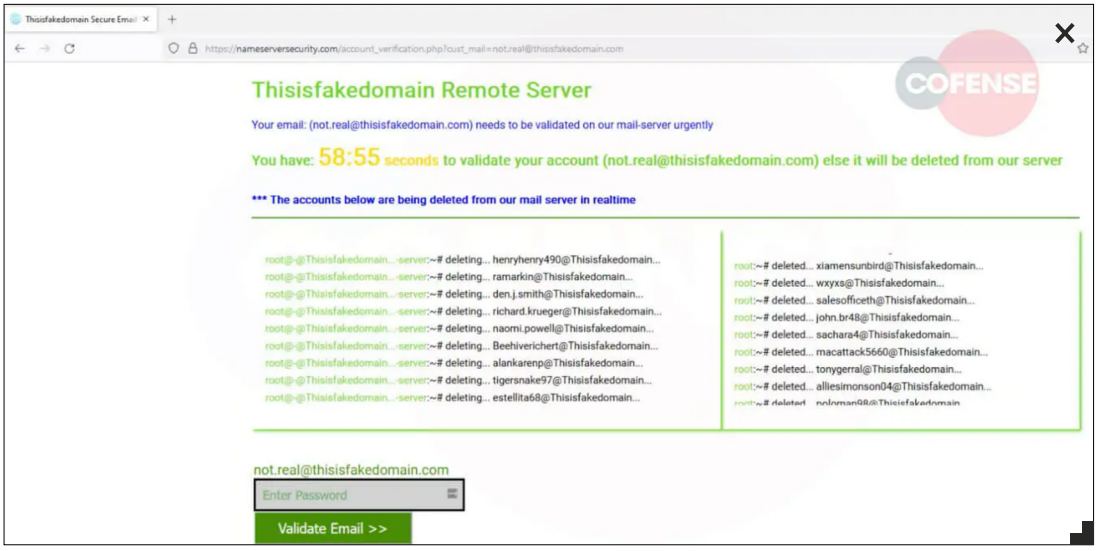

Рисунок 18. Фишинговый сайт

Операторы шифровальщиков также не упускают возможности использования социальной инженерии в атаках: этим летом вернулись атаки BazaCall, о которых мы подробно рассказывали в III квартале 2021 года. Метод BazaCall (или BazarCall) изначально использовался операторами программы-вымогателя Ryuk. Такая атака начиналась с уведомления по электронной почте о том, что скоро с пользователя будет взыматься плата за некую подписку. Также в сообщении был указан номер, по которому необходимо позвонить для ее отмены. При звонке жертва связывалась с подставным оператором кол-центра, который убеждал жертву либо скачать определенный файл, либо начать сеанс удаленного доступа для дальнейшего разрешения проблемы. В результате сеть была скомпрометирована, и злоумышленники могли приступить к развертыванию шифровальщика.

Телеграм-боты для эксфильтрации данных

Если ранее преступники в основном отправляли похищенную информацию на одноразовые почтовые ящики, то теперь используют и Telegram. Зашифрованный характер обмена сообщениями позволяет сохранить данные в секрете, а трафик не будет казаться подозрительным в тех организациях, где используется мессенджер.

В начале 2022 года мы писали о том, как операторы стилера Raccoon использовали Telegram в качестве инструмента контроля и управления. В недавних фишинговых кампаниях злоумышленники стали прибегать к этому же способу передачи украденных данных. Одна из таких атак была направлена на клиентов компании DHL: в июле исследователи Sucuri обнаружили поддельную страницу для отслеживания отправлений, которая повторяла оригинальную, однако персональные и платежные данные отправлялись злоумышленнику в виде HTTP-запроса на URL-адрес API бота Telegram.

«Короткоживущие» и легитимные домены

Чтобы жертва прочитала вредоносное сообщение, в первую очередь необходимо попасть в папку входящих, минуя категорию спама. Злоумышленники используют множество техник, чтобы избежать обнаружения средствами защиты. Например, чтобы вложенные ссылки на фишинговые сайты не казались вредоносными, злоумышленники могут использовать легитимные домены для хостинга вредоносных ресурсов. Так, в августе Avanan сообщили о всплеске числа атак, в которых преступники размещали фишинговые сайты на Amazon Web Services (AWS) — популярном сервисе, используемом в том числе для хостинга. Исследователи назвали этот метод атаки The Static Expressway: дело в том, что службы электронной почты, которые используют статические списки разрешенных или заблокированных источников, не защищены от этих атак, потому что легитимные домены AWS будут помечены как безопасные.

В атаках, направленных на кражу учетных данных пользователей криптовалютной биржи Coinbase, злоумышленники использовали интересную технику: фишинговые домены оставались активными в течение очень короткого периода времени — в среднем большинство страниц были доступны менее двух часов. В большинстве случаев такие страницы не будут архивированы: фишинговый сайт будет закрыт до того, как он будет проиндексирован поисковой системой. В дополнение к этому злоумышленники также устанавливают доступ к сайту для ограниченного круга лиц: например, возможность подключения может остаться только у пользователей с определенной геолокацией или если IP-адрес жертвы входит в диапазон допустимых. Все это усложняет анализ для исследователей безопасности, поскольку даже если одна из фишинговых страниц будет своевременно обнаружена, пока она активна, эксперту потребуется подделать ограничения, чтобы получить доступ к сайту.

В другой атаке, направленной на клиентов индийских банков, злоумышленники использовали функцию хостинг-провайдера создавать предварительные домены: она позволяет просматривать содержимое сайта до того, как он станет общедоступным. Такие фишинговые сайты оставались могли существовать до пяти суток.

Phishing as a service: доступный фишинг

В начале года мы прогнозировали распространение модели «фишинг как услуга», и сейчас можем наблюдать усиление этого тренда. В III квартале 2022 года число массовых кампаний с использованием социальной инженерии увеличилось на 41% в атаках на организации и на 34% в атаках на частных лиц по сравнению с прошлым кварталом. Преимущественно такой рост вызван активным использованием фишинговых комплектов — это готовый набор программ, предназначенный для проведения фишинговой атаки. В комплект могут входить готовые фишинговые страницы и формы ввода данных, скрипты для рассылки сообщений жертвам и скрипты для отправки украденных данных злоумышленникам.

Фишинг как услуга: про бизнес злоумышленников

Фишинговые комплекты просты в использовании, и потому провести фишинговую атаку под силу даже низкоквалифицированному злоумышленнику. Стоимость таких комплектов может составлять от 7 $ (а некоторые репозитории могут быть и в открытом доступе), при этом собранные учетные данные могут стоить в разы дороже.

Злоумышленники развивают бизнес, и мы наблюдаем появление разнообразных площадок для покупки и продажи киберпреступных услуг, в том числе и фишинга. Летом исследователями IronNet была обнаружена масштабная кампания с использованием новой платформы Robin Banks, продающей фишинговые наборы для проведения атак на клиентов известных банков и онлайн-сервисов. Кроме того, пользователи могут не только купить готовый набор, но и создать собственный комплект для фишинга. Доступ к одной странице со всеми обновлениями и круглосуточной поддержкой обойдется на платформе в 50 $ в месяц.

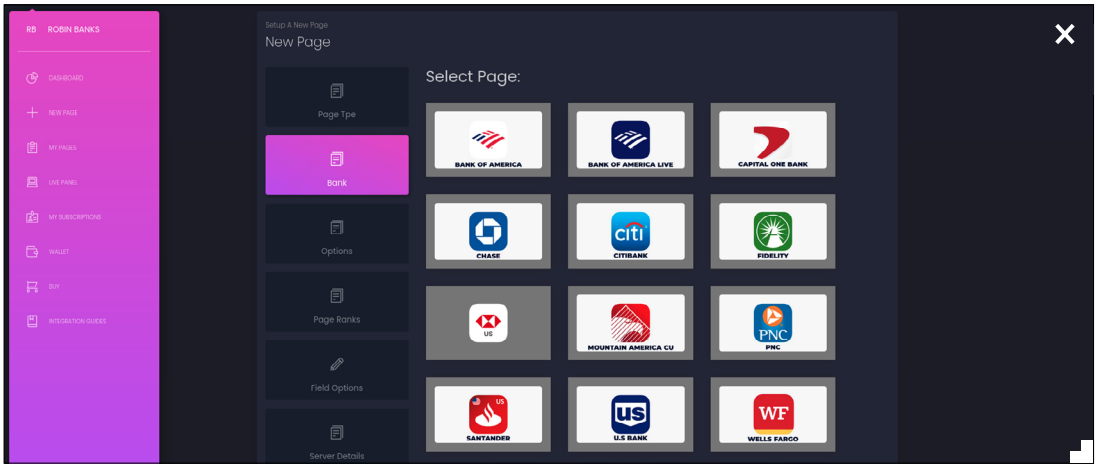

Рисунок 19. Интерфейс платформы Robin Banks

Обновления фишинговых инструментов

Готовые инструменты все чаще используются в фишинговых кампаниях, а их функции постоянно обновляются. Например, в начале августа исследователи Resecurity зафиксировали всплеск числа атак с использованием LogoKit. Этот фишинговый набор использует уязвимости открытого перенаправления[2] в популярных онлайн-сервисах и приложениях. Одна из кампаний, использующих этот набор для фишинга, была зафиксирована в середине июля и была направлена на пользователей Office 365 в США и странах Латинской Америки. Изначально жертва получает уведомление о том, что срок действия пароля скоро истекает. Чтобы оставить текущий пароль, пользователю предлагалось перейти по ссылке ниже в сообщении. Ссылка вела на поддельную форму ввода учетных данных, при этом поле для ввода электронной почты заполнялось автоматически: это создает иллюзию того, что пользователь уже посещал сайт ранее. Примечательно, что при переходе по ссылке LogoKit извлекает из открытых источников логотип компании, автоматически встраивая его в поддельную форму ввода, также создавая видимость легитимности ресурса.

[2] Open Redirect, или открытое перенаправление — это уязвимость, которая с помощью манипуляции параметров в URL позволяет перенаправить пользователя на ресурс, не предусмотренный разработчиком, например на фишинговый сайт.

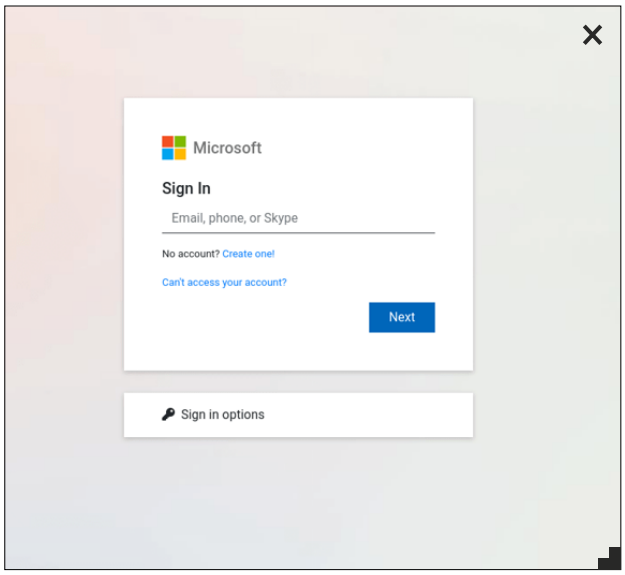

Рисунок 20. Поддельная форма ввода

Из количества в качество

Другой фишинговый комплект нацелен на пользователей PayPal. Для его распространения злоумышленники взламывали легитимные сайты со слабыми паролями, после чего встраивали вредоносный код. Такая атака имеет большой потенциал, поскольку более 400 миллионов частных лиц и компаний используют PayPal в качестве решения для онлайн-платежей.

Масштабы этой кампании впечатляют еще и объемами украденных данных: злоумышленники могли скомпрометировать как учетные данные, так и паспорта, водительские удостоверения, что необычно для фишинговых наборов. Кража данных начиналась с предъявления CAPTCHA — такой ход усиливает видимость защищенности веб-ресурса. Далее пользователю предлагалось войти в учетную запись PayPal, введя в поддельную форму ввода адрес электронной почты и пароль. При входе жертву уведомляют о «необычной активности» учетной записи и просят предоставить дополнительную информацию для проверки: это персональные и платежные данные, физический адрес и даже девичья фамилия матери. На этом злоумышленники не останавливались: пользователю предлагалось связать свой аккаунт PayPal с учетной записью электронной почты, а также загрузить документы, удостоверяющие личность (например, паспорт или водительское удостоверение).

Чтобы не оказаться в числе жертв злоумышленников, мы советуем совершать покупки только в надежных магазинах и внимательно проверять ссылки в адресной строке браузера. Если вы получили уведомление о подозрительной активности в вашем аккаунте на каком-либо ресурсе, лучше не переходить по ссылке, а проверить информацию на этом ресурсе самостоятельно.

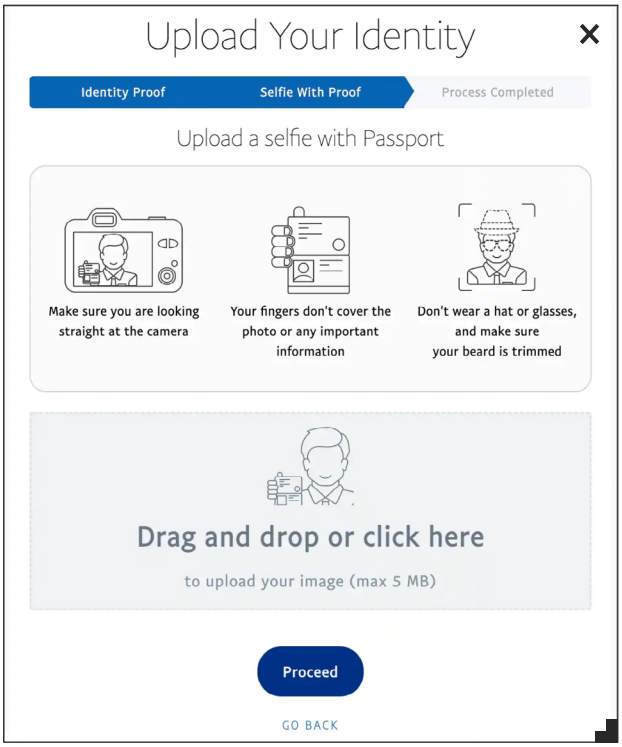

Рисунок 21. Поддельная форма загрузки данных

Обход многофакторной аутентификации

Нескольких факторов входа в учетную запись теперь может быть недостаточно: замечены масштабные кампании по сбору учетных данных с возможностью обхода многофакторной аутентификации. Начиная с июня исследователи Zscaler ThreatLabZ отметили всплеск количества атак, использующих фишинговые комплекты на основе обратных прокси-серверов. Кампания все еще продолжается, и новые фишинговые домены регистрируются почти ежедневно.

Такая техника с использованием обратных прокси-серверов называется adversary in the middle (man in the middle), или «противник посередине»: злоумышленник может находиться как бы посередине между жертвой и сервером провайдера электронной почты. При переходе на фишинговую страницу обратный прокси-сервер отображает легитимную форму ввода. Когда жертва вводит свои учетные данные и одноразовый пароль, информация перенаправляется на сервер фактической платформы, где пользователь вошел в систему, и возвращается куки-файл сеанса. Злоумышленник может украсть его и использовать для входа в учетную запись от лица скомпрометированного пользователя, минуя средства многофакторной аутентификации.

Использование многофакторной аутентификации все чаще становится частью корпоративной политики безопасности, и потому все больше злоумышленников используют обратные прокси-серверы. При этом киберпреступный бизнес растет: появляется платформа для фишинга EvilProxy, предлагающая способы обхода многофакторной аутентификации в Apple, Google, Facebook, Microsoft, Twitter, GitHub, GoDaddy и даже PyPI. Такие инструменты позволяют украсть плохо защищенные аккаунты даже низкоквалифицированному злоумышленнику, которому не по силам настроить прокси-сервер самостоятельно. При этом EvilProxy также предлагает подробные обучающие руководства и большой набор фишинговых страниц, имитирующих популярные ресурсы.

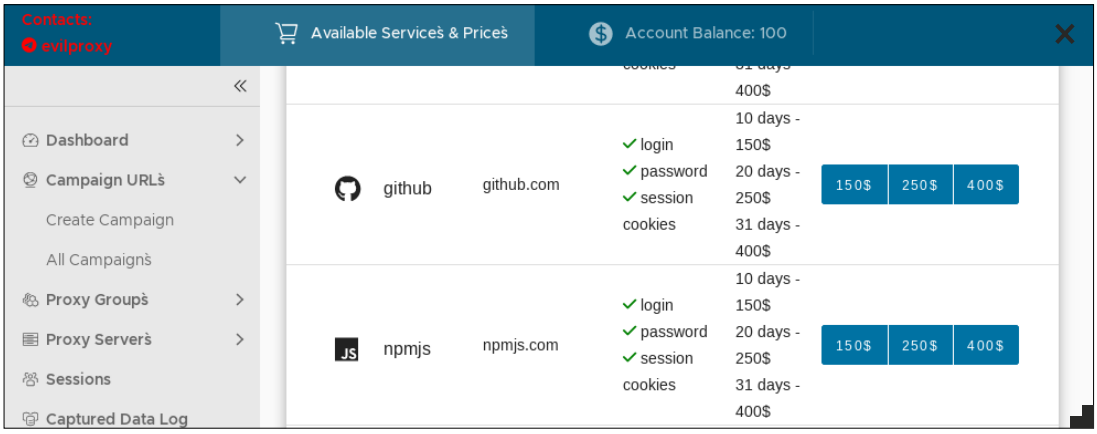

Рисунок 22. Выбор параметров для проведения фишинговой кампании

Массовые атаки на веб-приложения

Уязвимые сайты всегда представляют интерес для злоумышленников: количество атак с использованием эксплуатации веб-уязвимостей выросло на 67%. Эксплуатируя недостатки веб-приложений, преступники могут получить доступ к внутренней сети и продолжить атаку в инфраструктуре организации, украсть базу данных клиентов онлайн-магазина, провести массовую атаку на посетителей сайта. В III квартале массовые атаки на веб-ресурсы охватывают все большее количество жертв: исследователи обнаруживают уязвимости в популярных CMS, а атаки в основном направлены на клиентов скомпрометированных сайтов.

Популярные уязвимости

Публикация информации о новых уязвимостях, а тем более эксплойты для них всегда вызывают ажиотаж среди злоумышленников, тем более если они найдены в широко используемых CMS.

В сентябре исследователи Wordfence Threat Intelligence предупредили о массовых атаках, нацеленных на веб-сайты, использующие премиум-плагин WPGateway. Уязвимость, отслеживаемая как CVE-2022-3180, позволяет не прошедшему проверку подлинности злоумышленнику добавить нового пользователя с правами администратора и получить контроль над веб-ресурсом. За 30 дней исследователи обнаружили более 4,6 миллиона атак злоумышленников, пытающихся проэксплуатировать новую уязвимость, на более чем 280 000 сайтов.

Однако нередко внезапную, на первый взгляд, популярность могут обрести и обнаруженные ранее уязвимости. Это может быть связано с открытым распространением эксплойтов на теневых площадках, в результате которого большее количество злоумышленников может ими воспользоваться. Так, в июле исследователи обнаружили внезапный всплеск числа атак, нацеленных на веб-сайты, использующие уязвимый плагин Kaswara Modern WPBakery Page Builder. Сама уязвимость была раскрыта ранее и отслеживается как CVE-2021-24284. Она позволяет неавторизованному злоумышленнику загружать произвольные файлы, например вредоносный веб-шелл, что приводит к выполнению кода и полному контролю над сайтом. И поскольку плагин был закрыт без исправления, все его версии подвержены этой уязвимости. Начиная с 4 июля злоумышленники сканировали в среднем 443 868 сайтов в сутки, пытаясь обнаружить плагин и эксплуатировать уязвимость.

Кроме того, в III квартале 2022 года аналитики Sansec зафиксировали всплеск количества атак, нацеленных на эксплуатацию CVE-2022-24086, критически опасной уязвимости платформы Magento. Она связана с некорректной проверкой ввода в процессе оформления заказа, в результате которой злоумышленник может выполнить произвольный код. Исследователи обнаружили три варианта атаки с использованием этой уязвимости для внедрения трояна удаленного доступа.

Своевременное обновление используемого ПО, включая CMS и многочисленные плагины, поможет снизить риск компрометации веб-ресурса. Мы советуем придерживаться официальных рекомендаций вендора о том, как обезопасить сайт в условиях массового использования новых уязвимостей. Также следует использовать межсетевые экраны уровня приложений (WAF), которые защищают веб-приложения от атак, в том числе от эксплуатации уязвимостей, для которых пока нет патчей от производителей.

В преддверии распродаж

Исследователи экспертного центра безопасности Positive Technologies (PT Expert Security Center) обнаружили более 12 тысяч скомпрометированных сайтов под управлением Bitrix, в коде страниц которых злоумышленники разместили ссылку на вредоносный JavaScript. Если пользователь попадал на скомпрометированный ресурс, скрипт проверял, посещал ли пользователь в этот день другие скомпрометированные страницы и пришел ли он из поисковой системы. При выполнении обоих условий скрипт перенаправлял пользователя по вредоносной ссылке, и в результате посетитель скомпрометированного сайта оказывался на одной из фишинговых страниц, имитирующих легитимные, например известные онлайн-магазины. В конечном итоге злоумышленник получал данные платежных карт жертв.

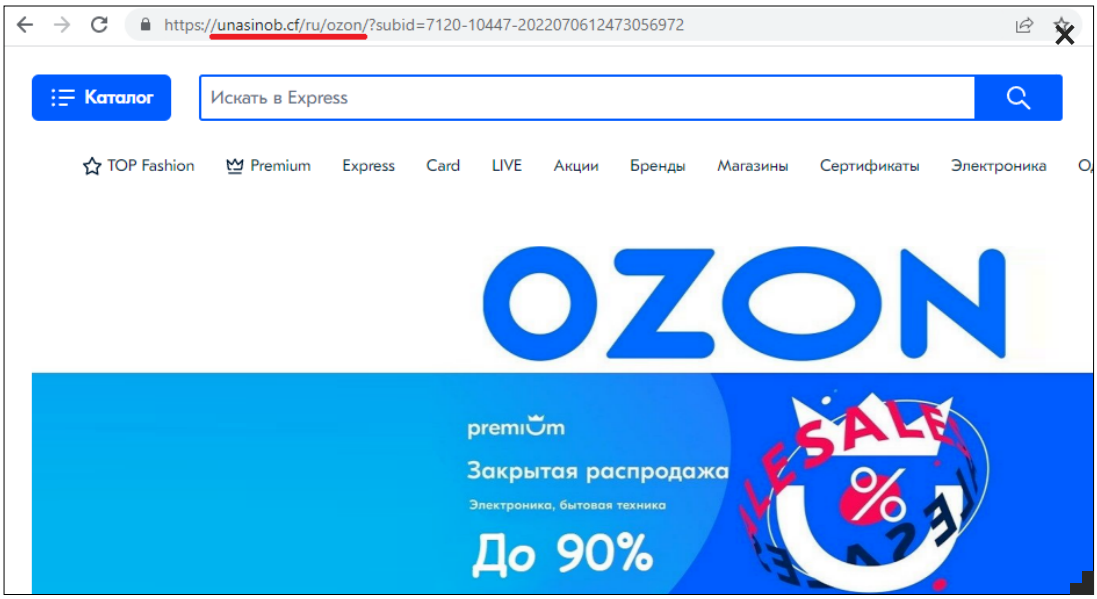

Рисунок 23. Фишинговая страница

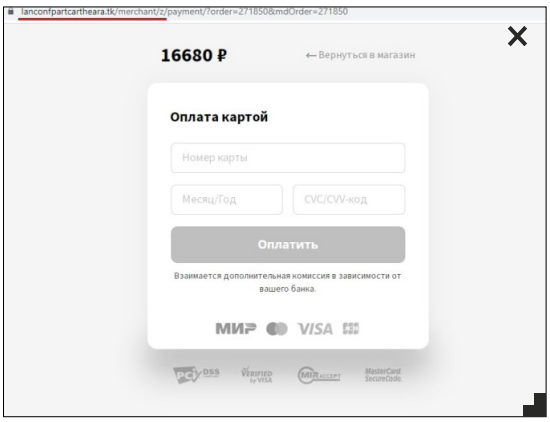

Рисунок 24. Фишинговая форма для оплаты

В другой серии атак злоумышленники эксплуатировали уязвимости Magento, чтобы получить доступ к исходному коду сайта и внедрить веб-скиммер. Такой скрипт предназначен для кражи данных из платежных форм ввода, страниц оформления заказа. Примечательно, что сам скрипт был обфусцирован и при выполнении вредоносного кода проверял, открыты ли в данный момент в браузере инструменты разработчика. Для видимости легитимности злоумышленники также проводили дополнительные проверки на правильность формата введенных данных, например длины номера карты.

Для внедрения скиммеров злоумышленники могут использовать легитимные инструменты, которые добавляются в код страницы. Например, Google Tag Manager (GTM) часто используется для интернет-маркетинга, отслеживания и анализа поведения посетителей на сайте. Еще в 2021 году исследователи из Recorded Future обнаружили вредоносные скрипты в GTM, выполняющие функции скиммера или загрузчика для его установки, и в июле 2022 года были обнаружены новые, обфусцированные варианты вредоносного кода. Активное заражение новых доменов наблюдалось и в августе, а в сентябре на теневых площадках было обнаружено более 165 000 записей о платежных картах жертв, пользующихся услугами скомпрометированных веб-ресурсов. Используя такие легитимные инструменты, как GTM, злоумышленники могут обновлять вредоносные сценарии без доступа к взломанному сайту, что позволяет избежать обнаружения.

Помимо веб-скиммеров злоумышленники также массово внедряют в уязвимые сайты фишинговые комплекты для кражи данных пользователей. В разделе, посвященном модели PhaaS, мы уже рассказывали об одной из таких атак: для распространения набора для фишинга, направленного на пользователей PayPal, преступники взламывали сайты со слабыми паролями на WordPress, после чего устанавливали плагин управления файлами, который далее использовался для загрузки фишингового комплекта. Такое распространение веб-скиммеров и инструментов для фишинга может быть подготовительной активностью злоумышленников в преддверии «черной пятницы» и других сезонных распродаж: чем больше сайтов будет заражено, тем больше пользовательских данных удастся собрать.

Мы рекомендуем пользователям совершать покупки только в известных и надежных интернет-магазинах, перепроверять ссылки в адресной строке браузера. Прежде чем вводить платежные и персональные данные, необходимо убедиться, что страница действительно принадлежит магазину или банку, что используется безопасное подключение. Не стоит переходить по подозрительным ссылкам, а также открывать вложения в письмах, если вы не уверены в надежности отправителя. Для шопинга мы рекомендуем заводить отдельную карту, например виртуальную, и хранить на ней небольшие денежные суммы, а также устанавливать лимиты на покупки в интернете.

Об исследовании

Данный отчет содержит информацию об общемировых актуальных угрозах информационной безопасности, основанную на собственной экспертизе компании Positive Technologies, результатах расследований, а также на данных авторитетных источников.

По нашей оценке, большинство кибератак не предается огласке из-за репутационных рисков. В связи с этим подсчитать точное число угроз не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. Наше исследование проводится с целью обратить внимание компаний 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 глоссарии на сайте Positive Technologies.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — ведущий разработчик решений для информационной безопасности. Уже 21 год наша основная задача — предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики.

Наши технологии и сервисы используют более 2900 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI).

Следите за нами в соцсетях (Telegram, ВКонтакте, Twitter, Хабр) и в разделе «Новости» на сайте ptsecurity.com, а также подписывайтесь на телеграм-канал IT's positive investing.