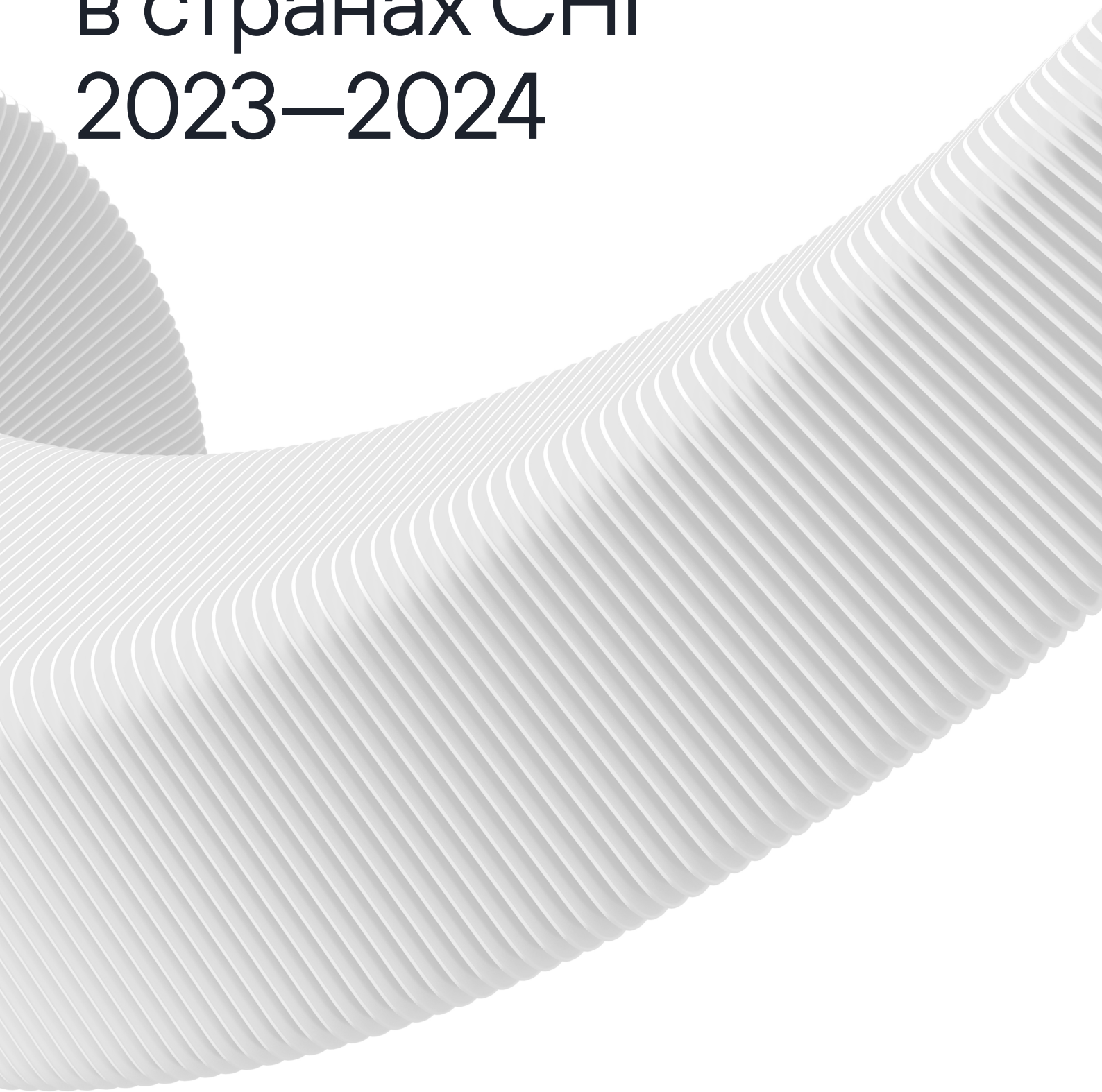
Актуальные киберугрозы в странах СНГ 2023–2024



Москва
2024

ptsecurity.com

Содержание

Об исследовании ... 3

Резюме ... 3

Цифровой статус СНГ ... 4

Основные очаги киберпреступности ... 6

Жертвы и последствия атак ... 11

Кто и как атакует СНГ ... 16

- Использование вредоносного ПО ... 17
- Атаки кибершпионских групп ... 20
- Атаки хактивистов ... 29
- Атаки финансово мотивированных операторов шифровальщиков ... 31
- Фишинговые атаки и скам ... 34
- Анализ теневых площадок ... 43

Выводы и рекомендации ... 48

Об исследовании

В отчете представлены результаты исследования актуальных киберугроз для Содружества Независимых Государств (СНГ) в 2023-м и первой половине 2024 года. В СНГ входят: Азербайджан, Армения, Беларусь, Казахстан, Кыргызстан, Молдавия, Россия, Таджикистан и Узбекистан. Туркменистан входит в СНГ на правах ассоциированного члена. Исследование выполнено с целью обратить внимание компаний, интересующихся современным состоянием информационной безопасности, на ландшафт киберугроз в этих странах.

Данные и выводы, представленные в отчете, основаны на собственной экспертизе Positive Technologies, а также на анализе общедоступных ресурсов, включая публикации правительственных и международных организаций, научно-исследовательские работы и отраслевые доклады. 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. В нашем отчете каждая массовая атака (в ходе которой злоумышленники проводят, например, фишинговую рассылку на множество адресов) рассматривается как одна отдельная, а не как несколько атак. Термины, которые мы использовали в исследовании, приведены в глоссарии на сайте Positive Technologies.

Резюме

- Количество атак на страны СНГ растет: во II квартале 2024 года зафиксировано в 2,6 раза больше атак по сравнению с аналогичным периодом в 2023 году.
- Почти три четверти (73%) атак, направленных против организаций в СНГ, пришлось на долю России. На втором и третьем месте — Казахстан (8%) и Беларусь (7%).
- Наибольшему числу атак в странах СНГ подверглись госучреждения (18%), промышленность (11%) и телекоммуникации (10%). На них нацелены злоумышленники самых разных категорий — начиная с продавцов данных на теневых рынках и заканчивая прогосударственными кибершпионами.
- Основными методами кибератак в странах СНГ, как и во всем мире, являются использование вредоносного ПО и социальная инженерия. В то же время доля DDoS-атак на организации в СНГ существенно выше общемирового показателя — 18% в СНГ против 8% в мире.
- Основными последствиями успешных атак на организации стали утечка конфиденциальной информации (41%) и нарушение основной деятельности (37%). Атаки на частных лиц заканчивались утечкой конфиденциальной информации в 69% случаев и прямыми финансовыми потерями в 32% случаев. Более половины от общего объема похищенных у организаций данных составили персональные данные и коммерческая тайна (30% и 29% соответственно).
- Одна из основных угроз для стран СНГ — атаки кибершпионских групп. Их доля составляет 18% от общего числа успешных атак. Наибольшее число жертв — среди госучреждений, промышленных предприятий, в сфере науки и образования.
- Четверть (26%) кибератак против организаций СНГ были совершены хактивистами. Цели большинства из них — кража данных и DDoS-атаки.

- В странах СНГ каждая пятая (22%) атака на организации с использованием ВПО приходится на долю шифровальщиков, из них 88% имеют финансовую мотивацию. Наиболее часто жертвами вымогателей становятся промышленные и производственные предприятия — 21% от всех атак шифровальщиков.
- На теневых рынках растет доля объявлений, связанных со странами СНГ: в первом полугодии 2024 года было опубликовано на 35% больше объявлений, чем за аналогичный период в 2023 году. Большая часть сообщений связана с базами данных (40%), при этом в 79% из них базы данных раздаются бесплатно.

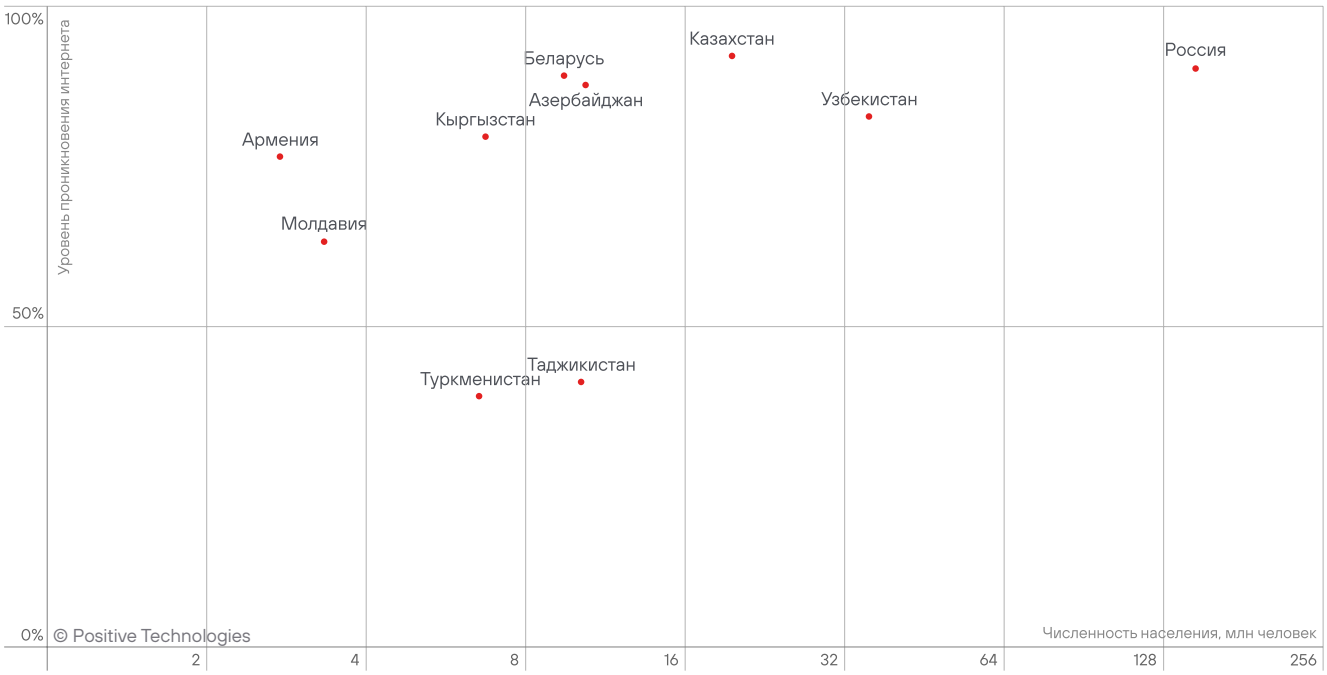
Цифровой статус СНГ

Содружество Независимых Государств (СНГ) создано в декабре 1991 года с целью сотрудничества между рядом стран, входивших в состав СССР. В настоящее время оно объединяет Азербайджан, Армению, Беларусь, Казахстан, Кыргызстан, Молдавию, Россию, Таджикистан и Узбекистан, а также Туркменистан, который имеет статус ассоциированного члена.

В регионе интенсивными темпами идет процесс диджитализации. Во многих странах появляются собственные государственные стратегии и программы цифровизации. На сегодняшний день в большинстве стран СНГ уровень проникновения интернета превышает отметку в 70%. Для сравнения: согласно отчету Digital 2024: Global Overview Report, среднемировой показатель составляет 66,2%. Уровень проникновения интернета остается ниже среднемирового только в Молдавии, Таджикистане и Туркменистане.

[1] Источник данных: datareportal.com

Рисунок 1. Соотношение численности населения и уровня проникновения интернета[1]



Цифровой трансформации стран СНГ способствуют инвестиции, которые регион привлекает благодаря своему географическому положению и политическому значению. Например, Китай активно сотрудничает со странами Центральной Азии для реализации проектов в рамках программы «Цифровой Шелковый путь», включающих строительство новых линий передачи данных, центров хранения и обработки данных, развитие спутниковой навигации и сетей 5G, а также обмен знаниями в области передовых технологий. Европейский Союз также инвестирует в регион. Так, Армения, Азербайджан и Молдавия являются участниками флагманской инициативы Европейского союза EU4Digital по поддержке цифровой трансформации и экономического роста в странах Восточного партнерства ЕС. В начале 2024 года Молдавия присоединилась к программе Digital Europe, что позволит государству получать финансирование от ЕС на проекты в области цифровизации. Всемирный банк оказывает финансовое содействие странам Центральной Азии в рамках программы Digital CASA (Digital Central Asia — South Asia). Она направлена на расширение доступа к высокоскоростному интернету, привлечение частных инвестиций и развитие электронных государственных услуг.

Обратная сторона интенсивных темпов цифровизации — рост уровня киберпреступности. В условиях политической неопределенности и нестабильности вопросы развития кибербезопасности имеют для большинства стран СНГ большое значение. В целом обеспечение кибербезопасности среди стран СНГ коррелирует с уровнем их экономического развития. Сегодня, согласно индексу NCSI[2], по уровню кибербезопасности среди стран СНГ лидирует Россия. Наиболее низкие индексы кибербезопасности среди стран СНГ имеют Таджикистан и Туркменистан.

[2] Рейтинг, отражающий готовность стран предотвращать киберинциденты и противостоять киберугрозам на национальном уровне.

Рисунок 2. Соотношение индекса кибербезопасности (NCSI) и ВВП страны



Основные очаги киберпреступности

Интерес злоумышленников к странам СНГ увеличивается из квартала в квартал. Так, во II квартале 2024 года было зафиксировано в 2,6 раза больше атак, чем в аналогичный период 2023 года (см. рисунок 3). По нашим данным, 73% всех атак, направленных против организаций СНГ, пришлось на долю России. На втором и третьем месте — Казахстан (8%) и Беларусь (7%). Интерес злоумышленников к этим государствам подтверждается, в том числе, большим количеством объявлений в дарквебе о продаже, раздаче и покупке данных и услуг, связанных с Россией, Беларусью и Казахстаном. Подробнее об этом читайте в разделе «Анализ теневых площадок».

Рисунок 3. Распределение успешных кибератак по кварталам

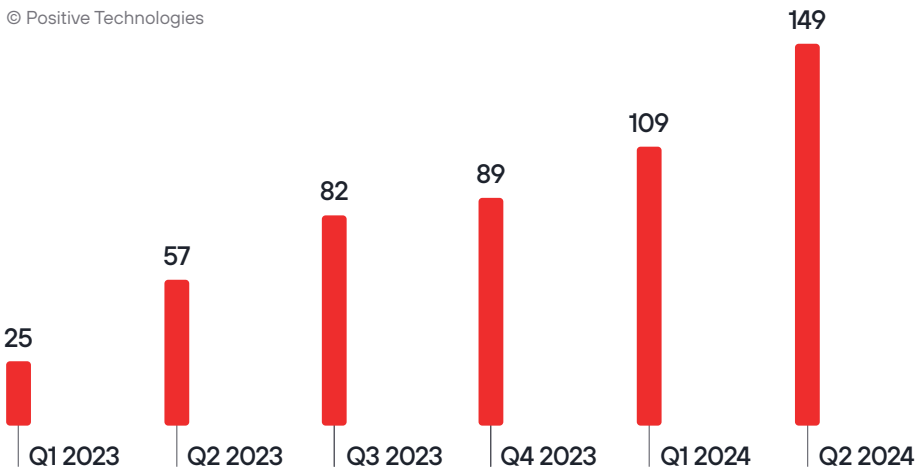


Рисунок 4. Распределение успешных кибератак по странам



Россия

Россия активно выступает за международное сотрудничество в сфере кибербезопасности, заключает соглашения с другими странами, в том числе и со странами СНГ. В стране созданы и функционируют центры по реагированию на инциденты (CERT), планируется создание такого центра в области искусственного интеллекта. В ноябре 2023 года была утверждена Стратегия развития отрасли связи до 2035 года, которая предусматривает переход на доверенные сертифицированные в РФ средства защиты информации, развитие государственного центра обнаружения, предупреждения и ликвидации последствий компьютерных атак, развитие единой централизованной системы защиты от DDoS-атак и другие инициативы, связанные с развитием в области кибербезопасности.

Как уже было отмечено выше, 73% всех атак на страны СНГ в 2023 и первой половине 2024 года пришлось именно на Россию. Большое количество атак на российские компании начиная с 2022 года обусловлено геополитической ситуацией. Сегодня российские организации атакуются десятками кибершпионских, хактивистских и финансово мотивированных групп.

Наибольшее количество атак было совершено на промышленность (11%), телекоммуникации (10%), госучреждения (9%) и IT-компании (7%). Среди методов атак превалирует социальная инженерия (56%), в каждой второй атаке использовалось вредоносное ПО, в каждой третьей злоумышленники эксплуатировали уязвимости. В 40% всех атак с применением ВПО использовались инфостилеры, в 31% — трояны для удаленного управления, а в каждой четвертой атаке с использованием ВПО злоумышленники пытались заразить жертв шифровальщиками. Каждая вторая (49%) атака заканчивалась утечкой конфиденциальной информации, 31% атак привел к нарушению основной деятельности организаций.

Рисунок 5. Сводная статистика по атакам на Россию



Россия

375 атак
2023–H1 2024

Топ категорий жертв:

Промышленность	11%
Телекоммуникации	10%
Госучреждения	9%
IT-компании	7%

Топ методов атак:

Социальная инженерия	56%
Использование ВПО	51%
Эксплуатация уязвимостей	30%
DDoS	10%

Топ объектов атак:

Компьютеры, серверы и сетевое оборудование	69%
Люди	56%
Веб-ресурсы	21%

Топ последствий атак:

Утечка конфиденциальной информации	49%
Нарушение основной деятельности	31%
Прямые финансовые потери	9%

*Доля от общего числа атак на страну за указанный период

© Positive Technologies

Казахстан

На сегодняшний день Казахстан занимает 78-е место в рейтинге NCSI, уступая позиции Беларуси, Молдавии, Азербайджану и России. В стране предпринимаются меры для повышения киберустойчивости. В марте 2023 года правительство республики Казахстан утвердило Концепцию цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023—2029 годы, согласно которой планируется дальнейшее развитие Национального координационного центра кибербезопасности, созданного ранее в рамках программы «Киберщит Казахстана». В рамках этой программы планируется также создание киберполигона для обучения специалистов по информационной безопасности.

Наиболее часто жертвами киберпреступлений в Казахстане в 2023 и 2024 годах становились СМИ (19%), госучреждения (12%), финансовые организации (12%) и телекоммуникации (7%). Высокая доля атак на СМИ обусловлена тем, что на казахстанские СМИ с ноября 2023 года обрушилась волна DDoS-атак. Кибератаки были направлены как минимум на девять независимых СМИ и на аккаунты нескольких журналистов в мессенджерах и социальных сетях. Для решения проблемы роста числа атак на казахстанские СМИ в конце декабря 2023 года был организован круглый стол на тему «Информационная безопасность СМИ: как обеспечить защиту журналистики от хакерских атак».

Две трети всех атак на Казахстан (65%) были связаны с использованием вредоносного ПО, а в каждой второй (53%) применялись методы социальной инженерии. Более трети атак (35%) заканчивались утечкой конфиденциальной информации. Наибольшим спросом пользовались персональные и учетные данные. Эксперты национальной службы реагирования на компьютерные инциденты KZ-CERT назвали инфостилеры, с помощью которых злоумышленники похищали персональные данные. В их число вошли ReadLine, Vidar, Raccoon и Azorult.

Рисунок 6. Сводная статистика по атакам на Казахстан



Казахстан

43 атаки
2023–H1 2024

Топ категорий жертв:	
СМИ	19%
Госучреждения	12%
Финансовые организации	12%
Телекоммуникации	7%

Топ методов атак:	
Использование ВПО	65%
Социальная инженерия	53%
Эксплуатация уязвимостей	28%
DDoS	19%

Топ объектов атак:	
Компьютеры, серверы и сетевое оборудование	74%
Люди	53%
Веб-ресурсы	21%

Топ последствий атак:	
Утечка конфиденциальной информации	35%
Нарушение основной деятельности	35%
Прямые финансовые потери	12%

*Доля от общего числа атак на страну за указанный период

© Positive Technologies

Беларусь

Беларусь занимает 70-е место в рейтинге NSCI, уступая среди стран СНГ только Молдавии, Азербайджану и России. В феврале 2023 года Беларусь совместно с Россией утвердила постановление о сотрудничестве в сфере информационной безопасности, целью которого стала защита от внешних угроз, обеспечение информационной безопасности и укрепление системы безопасности Союзного государства. Также в феврале 2023 года президентом Беларуси был подписан Указ № 40 «О кибербезопасности», согласно которому создается национальная система обеспечения кибербезопасности. Уже около 14 лет в стране работает Национальный центр обмена трафиком (НЦОТ), одна из основных задач которого — развитие единой республиканской сети передачи данных. За время своего существования НЦОТ стал одним из самых конкурентоспособных игроков на телекоммуникационном рынке Европы и в настоящее время работает над расширением географии своего присутствия.

Каждая пятая кибератака (22%) в Беларуси была направлена на госучреждения, на втором месте по числу атак — промышленность (14%). Три четверти атак (76%) совершались с использованием ВПО, каждая вторая (57%) заканчивалась утечкой конфиденциальных данных.

Наибольшую угрозу для белорусских организаций представляют кибершпионские группы XDSpy, Sticky Werewolf, Lazy Koala и некоторые другие (см. рисунок 20). В начале 2024 года Avast, компания-владелец программы для очистки компьютера CCleaner, прекратила оказывать услуги в России и Беларуси, в связи с чем программа перестала работать на территории этих государств. Инфоповодом воспользовались злоумышленники из группы Sticky Werewolf, организовав фишинговую кампанию, направленную на белорусские организации. В ходе этой кампании под видом программы CCleaner распространялся троян Ozone RAT.

Помимо кибершпионажа еще одна существенная угроза для белорусских организаций — атаки группировки «Киберпартизаны». «Киберпартизаны» — это хактивисты, относящие себя к оппозиционному движению в Беларуси. В конце 2023 года они заявили о взломе сайта госагентства БелТА, сообщив о краже 90 Гбайт конфиденциальной информации, включая личные данные сотрудников. В апреле 2024 года хактивисты заявили об атаке на крупнейшего в стране государственного производителя удобрений «Гродно Азот» в связи с его предполагаемой причастностью к политическим репрессиям, уклонению от санкций и нарушениям прав человека. Злоумышленники выложили доказательства атаки в своем Telegram-канале. Они утверждают, что могли полностью остановить работу завода, но воздержались от этого.

Рисунок 7. Сообщение хактивистов с доказательствами взлома белорусского завода по производству удобрений «Гродно Азот» в апреле 2024 года

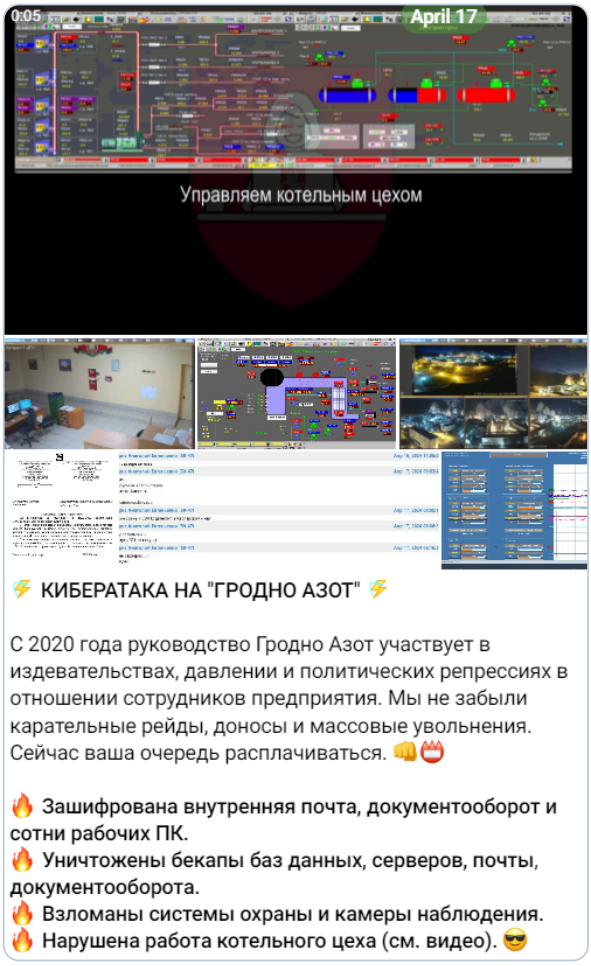


Рисунок 8. Сводная статистика по атакам на Беларусь





Беларусь

37 атак
2023–H1 2024

Топ категорий жертв:

Госучреждения	22%
Промышленность	14%
Финансовые организации	11%
Наука и образование	8%

Топ методов атак:

Использование ВПО	76%
Социальная инженерия	68%
Эксплуатация уязвимостей	32%

Топ объектов атак:

Компьютеры, серверы и сетевое оборудование	86%
Люди	68%
Веб-ресурсы	14%

Топ последствий атак:

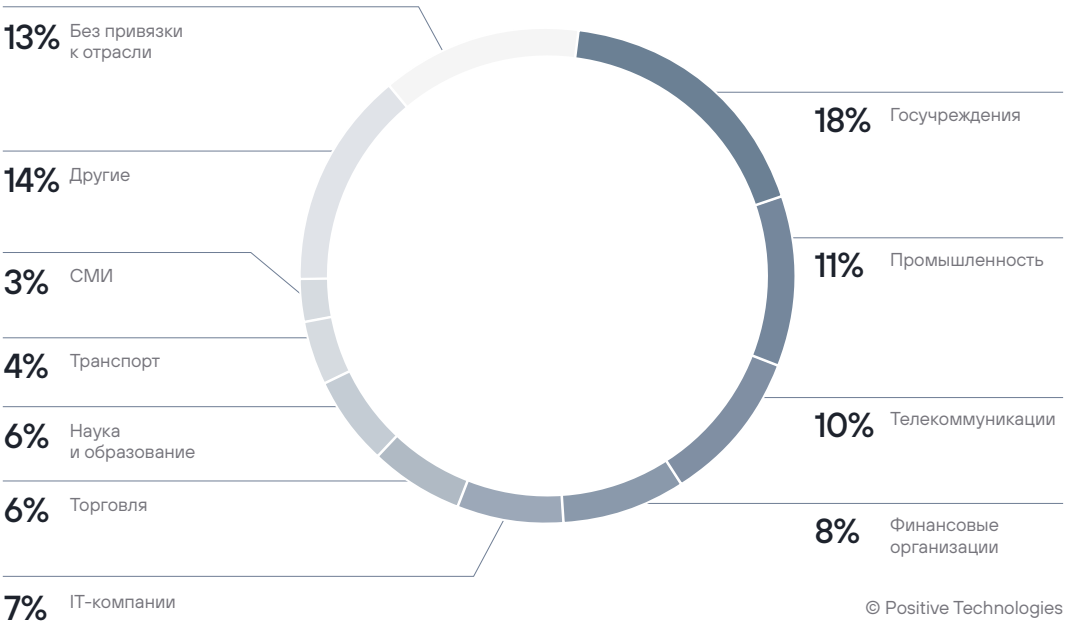
Утечка конфиденциальной информации	57%
Нарушение основной деятельности	16%
Прямые финансовые потери	8%

© Positive Technologies

Жертвы и последствия атак

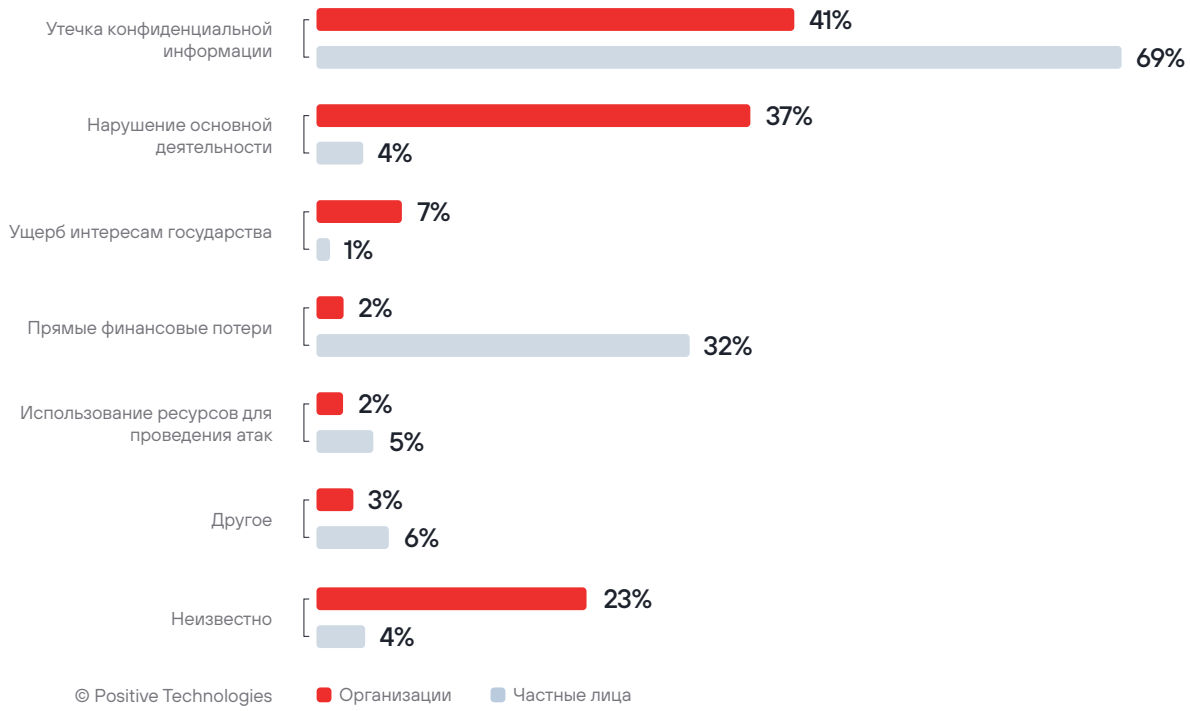
В 2023-м и первой половине 2024 года максимальному числу атак в странах СНГ подверглись госучреждения (18%), промышленность (11%) и телекоммуникации (10%). Эти три отрасли представляют наибольший интерес для злоумышленников по ряду причин. Во-первых, организации из этих сфер имеют стратегически важное значение для экономики страны, и поэтому в условиях геополитической напряженности они в первую очередь подвергаются кибератакам. Во-вторых, в государственных, промышленных и телекоммуникационных компаниях хранятся большие объемы конфиденциальной информации, прежде всего персональные данные и коммерческая тайна. На них нацелены злоумышленники самых разных категорий — начиная с продавцов данных на теневых рынках и заканчивая прогосударственными кибершпионами, собирающими разведданые.

Рисунок 9. Категории жертв среди организаций



Основные последствия успешных атак на организации — утечка конфиденциальной информации (41%) и нарушение основной деятельности (37%). Атаки на частных лиц заканчивались утечкой конфиденциальной информации в 69% случаев и прямыми финансовыми потерями в 32% случаев.

Рисунок 10. Последствия атак (доля атак)



Персональные данные и коммерческая тайна в совокупности составили более половины от общего объема похищенных у организаций данных (30% и 29% соответственно).

Рисунок 11. Типы украденных данных (в успешных атаках на организации

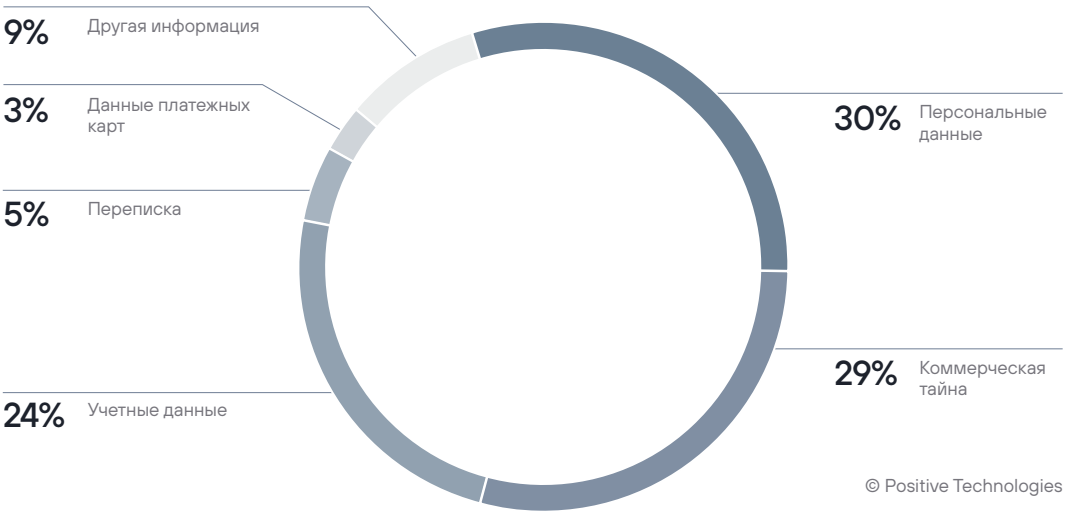
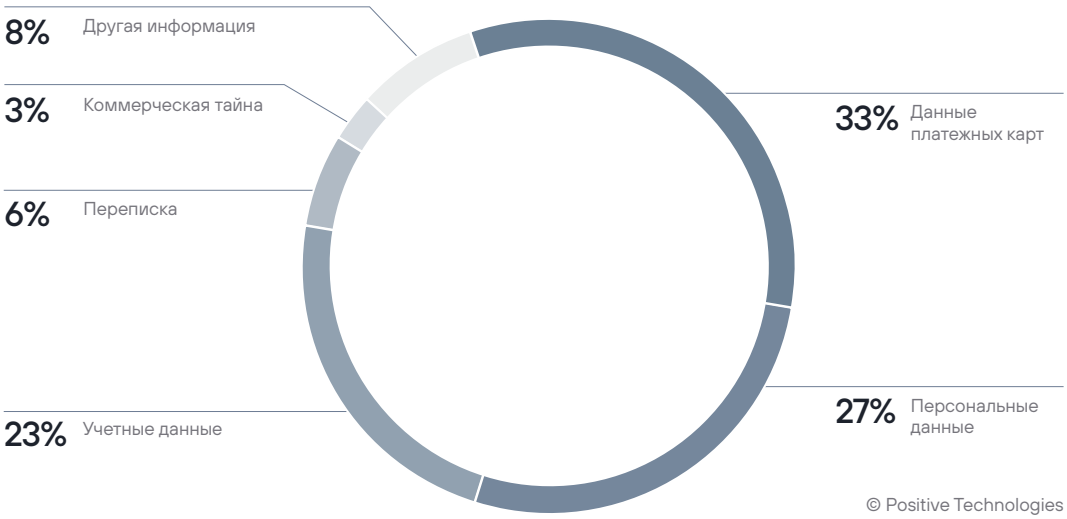


Рисунок 12. Типы украденных данных (в успешных атаках на частных лиц)



Госучреждения

На долю госучреждений пришлось 18% от всех атак на организации СНГ. Почти две трети (62%) успешных атак на госучреждения в СНГ совершены с использованием вредоносного ПО, в 57% атак применялись методы социальной инженерии. Каждая пятая атака на госучреждения (19%) — это DDoS. Как правило, DDoS-атаки усиливаются накануне или в день значимого политического или социального события. К примеру, в день начала акции «Диктант Победы» наблюдалось большое количество DDoS-атак на сервисы «Единой России». Во время выборов президента России также отмечалось большое количество попыток DDoS-атак на правительственные ресурсы. Например, атака на портал видеонаблюдения за выборами привела к его краткосрочной недоступности.

В государственных учреждениях хранятся огромные объемы конфиденциальных данных, начиная с личной информации граждан и заканчивая информацией, касающейся государственной безопасности. Утечка конфиденциальных данных происходила в 42% атак на госучреждения. Прежде всего госучреждения привлекают внимание кибершпионских групп — почти все они хотя бы раз атаковали государственные организации. Подробнее о том, какие кибершпионские группы действуют на территории СНГ, мы расскажем далее.

В 27% атак на госучреждения объектами атак становились веб-ресурсы. У сайтов правительственных организаций высокая посещаемость, поэтому они интересуют различные группы злоумышленников. Хактивисты, например, нередко проводят дефейс государственных сайтов с целью размещения на них политических или иных лозунгов. APT-группировки могут использовать веб-ресурсы госучреждений для атак watering hole. Так, летом 2023 года APT-группа YoroTrooper взломала несколько сайтов госучреждений Таджикистана и разместила на них вредоносное ПО.

В 28% атак был нанесен ущерб интересам государств, а 22% привели к нарушению деятельности госучреждений. Так, например, в феврале 2024 года в результате кибератаки на «Почту Молдовы» почтовые и финансовые услуги госпредприятия были недоступны около суток, что привело к образованию очередей в почтовых отделениях. В апреле 2023 года кибератака на Федеральную

таможенную службу России привела к сбоям в работе электронных сервисов таможни и затруднению таможенных операций — в частности, было приостановлено оформление таможенных деклараций. Подобные инциденты являются недопустимыми событиями для госучреждений, поскольку подрывают доверие граждан и усиливают социальную напряженность в стране.

Рисунок 13. Сводная статистика по госучреждениям



Промышленность

Промышленный сектор из года в год остается в зоне повышенного риска кибератак, и страны СНГ не исключение. На долю промышленных и производственных предприятий здесь приходится 11%. В восьми из десяти атак на промышленность (79%) было задействовано вредоносное ПО. В 42% из них использовались инфостилеры, в 37% — ВПО для удаленного управления, в 26% — шифровальщики.

Основные цели киберпреступников, атакующих отрасль, — промышленный шпионаж, вымогательство денег и нарушение технологических процессов. Попытки проникнуть в инфраструктуру промышленных предприятий совершали 73% APT-группировок, действующих в СНГ. В качестве начального вектора проникновения чаще всего они выбирают фишинговые письма с вредоносными вложениями. Приманками, как правило, служат различные служебные документы — фейковые заказы, договоры, счета-фактуры, акты сверки. Иногда киберпреступники проникают через уязвимости на сетевом периметре. Осенью 2023 года наши специалисты из команды PT CSIRT расследовали инцидент ИБ в российской энергетической компании. Эксперты выяснили, что злоумышленники попали в инфраструктуру через шлюз удаленного доступа к сети Citrix NetScaler Gateway. Предположительно, это было сделано путем эксплуатации уязвимости CVE-2023-3519.

Помимо кибершпионов через уязвимые публичные сервисы в инфраструктуру промышленных предприятий проникали финансово мотивированные киберпреступники, например группировка вымогателей Shadow, известная также как Comet и DARKSTAR. Злоумышленники шифровали инфраструктуру с помощью известного шифровальщика LockBit Black и требовали за восстановление данных суммы в размере от 1 млн долларов США.

По результатам ежегодного исследования Sophos, в 2023 году с атаками шифровальщиков столкнулись 56% промышленных компаний, а в 2024 году этот показатель вырос до 65%. Атаки шифровальщиков и политически мотивированных киберпреступников, настроенных на уничтожение инфраструктуры, представляют особую опасность для промышленности, поскольку могут стать причиной сбоя в производстве и даже выхода из строя оборудования. К примеру, в июле 2023 года появилась информация о кибератаке на систему регионального склада фармацевтической компании в Приморском крае, в результате которой во Владивостоке перестали отпускать любые лекарства крупной аптечной сети, в том числе льготные лекарственные препараты.

Рисунок 14. Сводная статистика по промышленности



Телекоммуникации

В каждой десятой атаке, направленной против организаций, жертвами становились телекоммуникационные компании. Основная угроза для телекома в СНГ — это DDoS-атаки (43% от всех атак на отрасль). Поток DDoS-атак на телеком связан, прежде всего, со стремлением политически мотивированных хактивистов препятствовать предоставлению качественных услуг связи основным геополитическим игрокам. Вот только несколько примеров за последнее время. Весной 2024 года компания МТС подверглась мощной DDoS-атаке, которая велась одновременно из пяти стран. Атаку удалось отразить, однако в случае ее успеха без интернета остались бы абоненты МТС целого региона. В июне 2024 года российский оператор связи ПАКТ сообщил о массированной DDoS-атаке на свою инфраструктуру, которая продолжалась двое суток. Во время атаки сервисы для некоторых клиентов компании были недоступны.

В результате 68% атак на телеком происходили нарушения в основной деятельности атакованной компании. Сбои в работе провайдеров связи влияют на миллионы абонентов, приводят к нарушению бизнес-процессов на стороне клиентов атакованного оператора. Так, в июне 2023 года проукраинская группировка Cyber.Anarchy.Squad заявила об атаке на российского оператора связи «Инфотел», который предоставляет услуги связи между коммерческими банками и Центральным банком России. По утверждению злоумышленников, атака привела к повреждению сетевого оборудования и прекращению работы более чем на сутки. Также в июне 2023 года

другая группа злоумышленников заявила об атаке на российского оператора спутниковой связи «Дозор-Телепорт», услугами которого пользуются топливно-энергетические компании. Киберпреступники утверждают, что смогли вывести из строя часть спутниковых терминалов, перезагрузить сетевое оборудование и уничтожить информацию, хранящуюся на серверах компании, а также они разместили на своих ресурсах 700 файлов, похищенных у жертвы. Подобного рода атаки влекут за собой значительные финансовые и репутационные потери, а на восстановление жертве может потребоваться от нескольких суток до нескольких месяцев.

Важно также отметить, что на серверах телекоммуникационных компаний хранятся и обрабатываются большие объемы данных. В результате каждой четвертой атаки на телеком происходила утечка конфиденциальной информации. Злоумышленники могут контролировать захваченную инфраструктуру провайдера в течение месяцев и даже лет, регулярно выгружая из нее ценные сведения. Так, в феврале 2024 года после публикации на GitHub конфиденциальных данных китайской компании iSoon выяснилось, что злоумышленники имели полный доступ к инфраструктуре казахстанских операторов связи в течение более двух лет. В руках злоумышленников оказались огромные объемы различной информации, включая персональные и учетные данные абонентов.

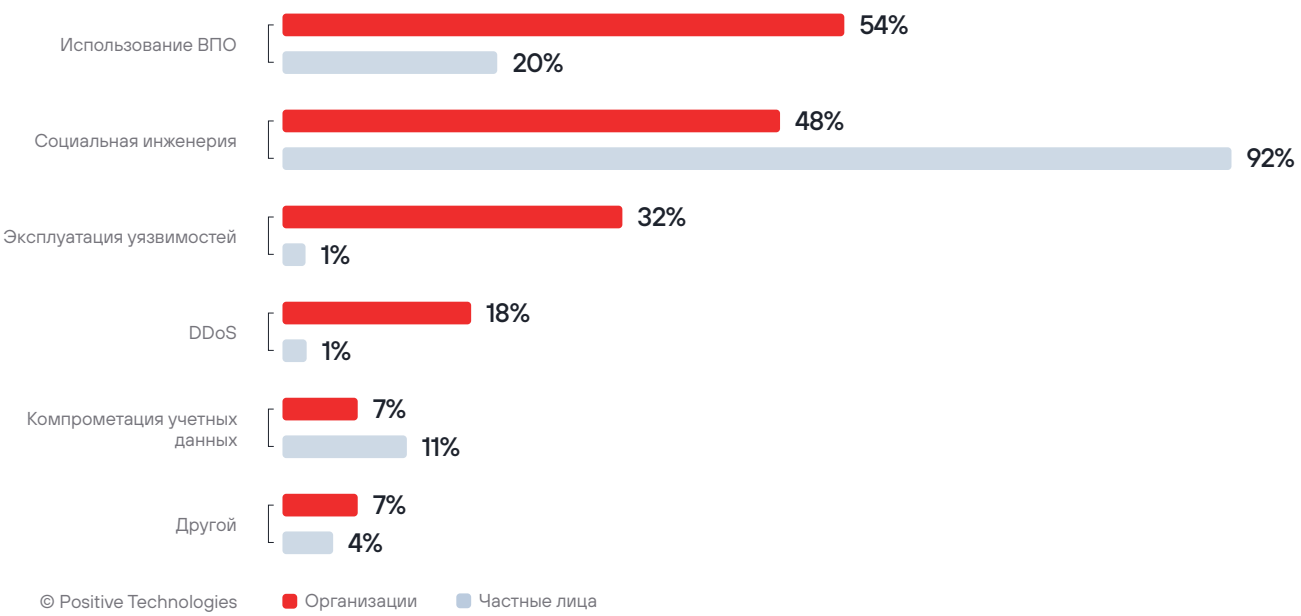
Рисунок 15. Сводная статистика по телекоммуникациям



Кто и как атакует СНГ

Основными методами кибератак в странах СНГ, как и во всем мире, являются использование вредоносного ПО и социальная инженерия. Однако мы выделяем характерную для региона особенность: доля DDoS-атак на организации в СНГ существенно выше общемирового показателя — 18% в СНГ против 8% в мире. Такое отличие в ландшафте киберугроз связано с напряженной текущей геополитической обстановкой. Она служит поводом для образования большого количества новых хактивистских группировок, объединяющихся в альянсы для проведения массовых DDoS-атак, прежде всего на организации в России.

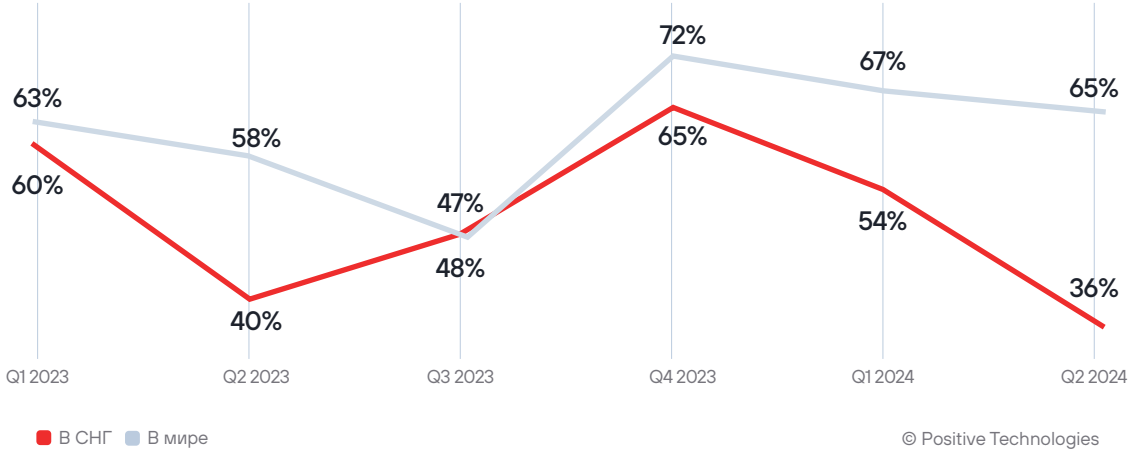
Рисунок 16. Методы атак на страны СНГ



Использование вредоносного ПО

На протяжении 2023-го и в первой половине 2024 года преобладали атаки с использованием ВПО. Мы отмечаем всплески атак с использованием ВПО в начале и в конце 2023 года. В I квартале 2023 года это преимущественно было связано с деятельностью вымогателей-шифровальщиков, в то время как в IV квартале фиксировалась высокая активность кибершпионских групп. Прежде всего речь идет о группах XDSpy, Core Werewolf, Sticky Werewolf, Cloud Atlas и Hellhounds, о которых мы расскажем далее.

Рисунок 17. Доля атак с использованием ВПО

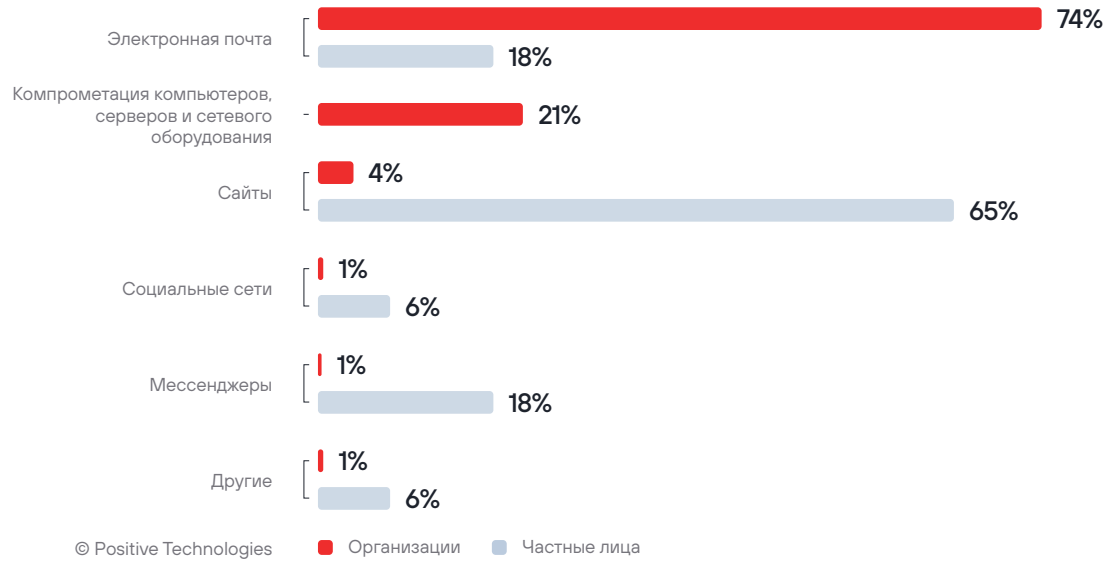


Наиболее распространенный сценарий в атаках на организации — рассылка фишинговых писем с вредоносными вложениями. Именно так доставлялись вредоносы в 74% случаев. В качестве приманок злоумышленники нередко использовали документы, связанные с актуальными полити-

ческими событиями. Так, в середине 2023 года APT-группа APT28 для доставки бэкдора Headlace рассылала в азербайджанские организации фишинговые письма с 15-страничным планом мероприятий по развитию сотрудничества между Беларусью и Азербайджаном. Темой фишинговых писем становились также конфликты, вызванные территориальными спорами. Например, для привлечения внимания получателей писем в Азербайджане и Армении киберпреступники активно используют конфликт между этими государствами, вызванный спором за контроль над регионом Нагорного Карабаха. Так, в августе 2023 года лаборатория FortiGuard Labs зафиксировала вредоносную рассылку в азербайджанские организации, в которой использовались фальшивые фотографии сцен агрессии со стороны Армении. При просмотре изображений на компьютер жертвы загружалось шпионское ПО. В сентябре 2023 года международные аэропорты и госорганы Армении подверглись вредоносным рассылкам электронных писем якобы от Службы национальной безопасности с сообщением, что страна стоит перед опасностью новой войны с Азербайджаном. На компьютеры жертв этой рассылки доставлялось ВПО для удаленного управления AsyncRAT.

На устройства частных лиц вредоносные программы в основном попадают при посещении пользователями зараженных сайтов (65%), а также через фишинговые сообщения в электронной почте (18%) и мессенджерах (18%).

Рисунок 18. Способы распространения вредоносного ПО (доля успешных атак с использованием ВПО)

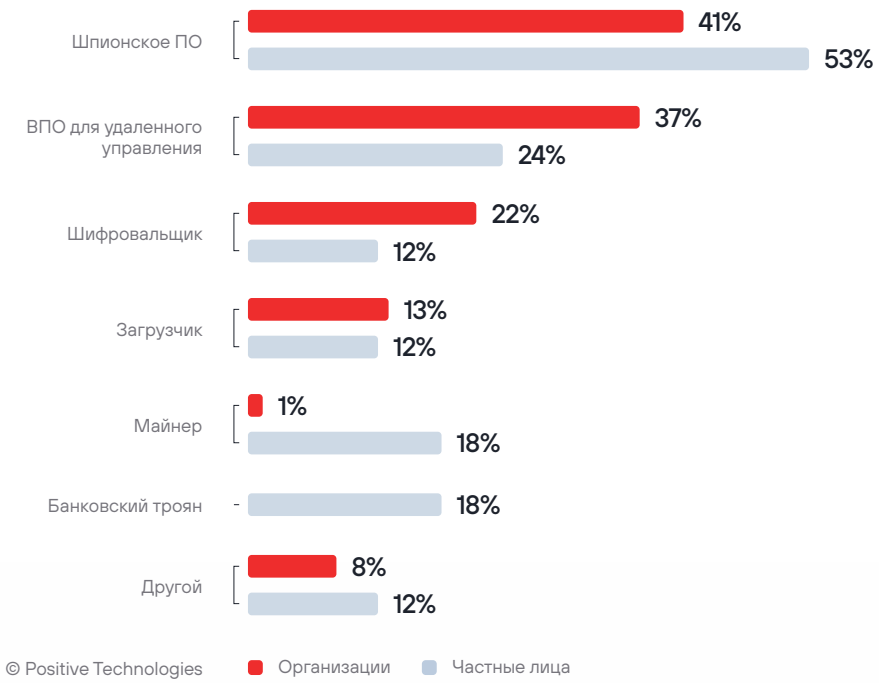


В атаках на СНГ с использованием ВПО наиболее часто применялось шпионское ПО: в 41% атак на организации и 53% атак на частных лиц. Среди распространенных семейств инфостилеров — Agent Tesla, XDigo, Azorult, Raccoon, Formbook, RedLine. По данным сервиса ANY.RUN, во II квартале 2024 года инфостилер RedLine занял первое место по частоте встречаемости. В СНГ RedLine и его форк MetaStealer используются в атаках кибершпионских групп ReaverBits и Sticky Werewolf и финансово мотивированной группы VasyGrek (также известна как Fluffy Wolf).

Злоумышленники также часто используют трояны для удаленного управления. В атаках с использованием ВПО на организации их доля составила 37%, в атаках на частных лиц — 24%. Пример

распространенного ВПО для удаленного управления — троян Remcos, или Remote Control and Surveillance. Это изначально легитимная программа, которая сейчас используется многими злоумышленниками в качестве инструмента для удаленного доступа. По числу загрузок на ANY.RUN троян Remcos занимает лидирующие позиции. Специалисты департамента Threat Intelligence (TI-департамента) экспертного центра безопасности Positive Technologies (PT Expert Security Center, PT ESC) регулярно фиксируют фишинговые рассылки, нацеленные на доставку Remcos в организации в странах СНГ. Например, в январе 2024 года была выявлена фишинговая рассылка, адресатами которой стали организации в Молдавии и Беларуси. К письмам был прикреплен документ, маскирующийся под платежный документ SWIFT. Он содержал в себе VBS-макрос, который в результате нескольких итераций запускал бэкдор Remcos. Помимо Remcos в атаках на СНГ также активно использовались бэкдоры njRAT, DarkCrystal, NetWire, Quasar.

Рисунок 19. Типы вредоносного ПО (доля успешных атак с использованием ВПО)



Атаки кибершпионских групп

На фоне непростой геополитической обстановки атаки кибершпионских групп, в том числе APT-группировок, — одна из острых угроз для стран СНГ. Их доля составляет 18% от общего числа успешных атак. Наиболее часто жертвами становятся госучреждения, промышленность, сфера науки и образования. В организациях из этих отраслей злоумышленники могут получить максимальное количество ценной информации, поэтому они становятся лакомыми целями кибершпионов.

В 2023 и 2024 годах в регионе продолжали деятельность кибергруппировки, известные на протяжении многих лет, например XDSpy и Cloud Atlas. Однако в добавление к давно известным группам в течение последних двух лет появились новые, например Lazy Koala, YoroTrooper, Sticky Werewolf, Hellhounds, (Ex)Cobalt. Ниже приведен краткий обзор 15 кибершпионских групп, наиболее активно атаковавших страны СНГ в указанный период.

Рисунок 20. Кибершпионские группы, наиболее активные в странах СНГ в 2023 и 2024 годах

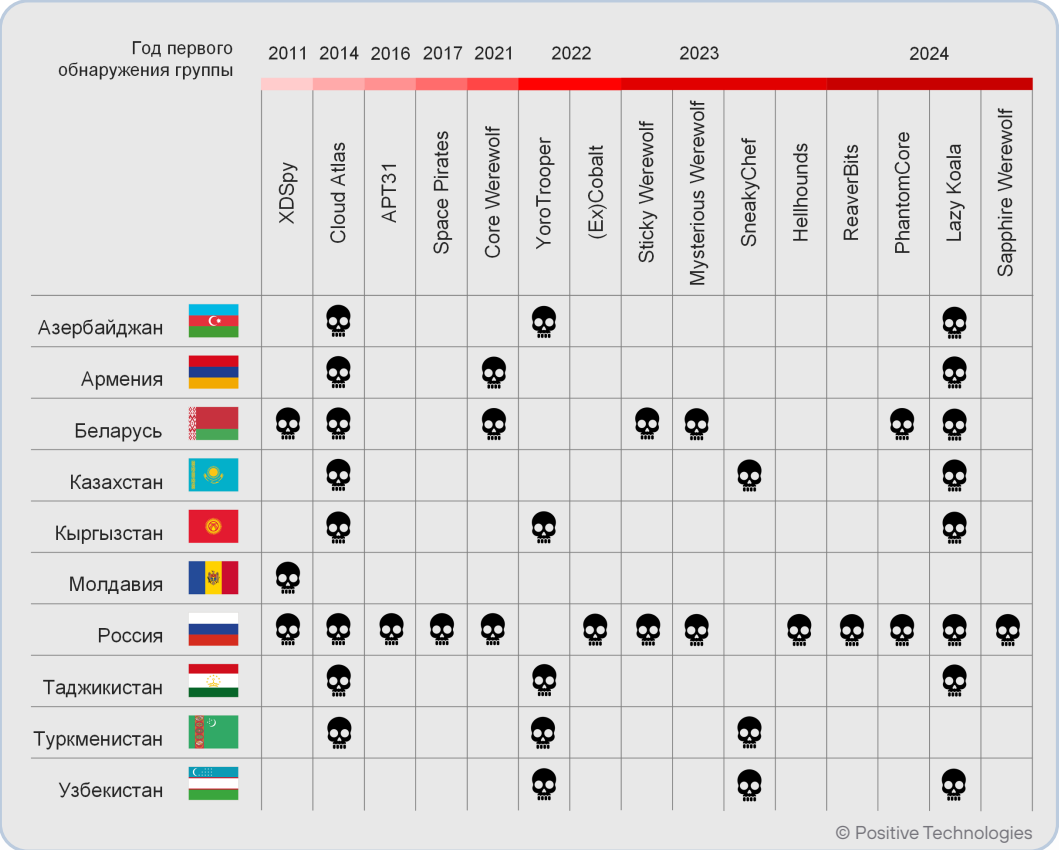
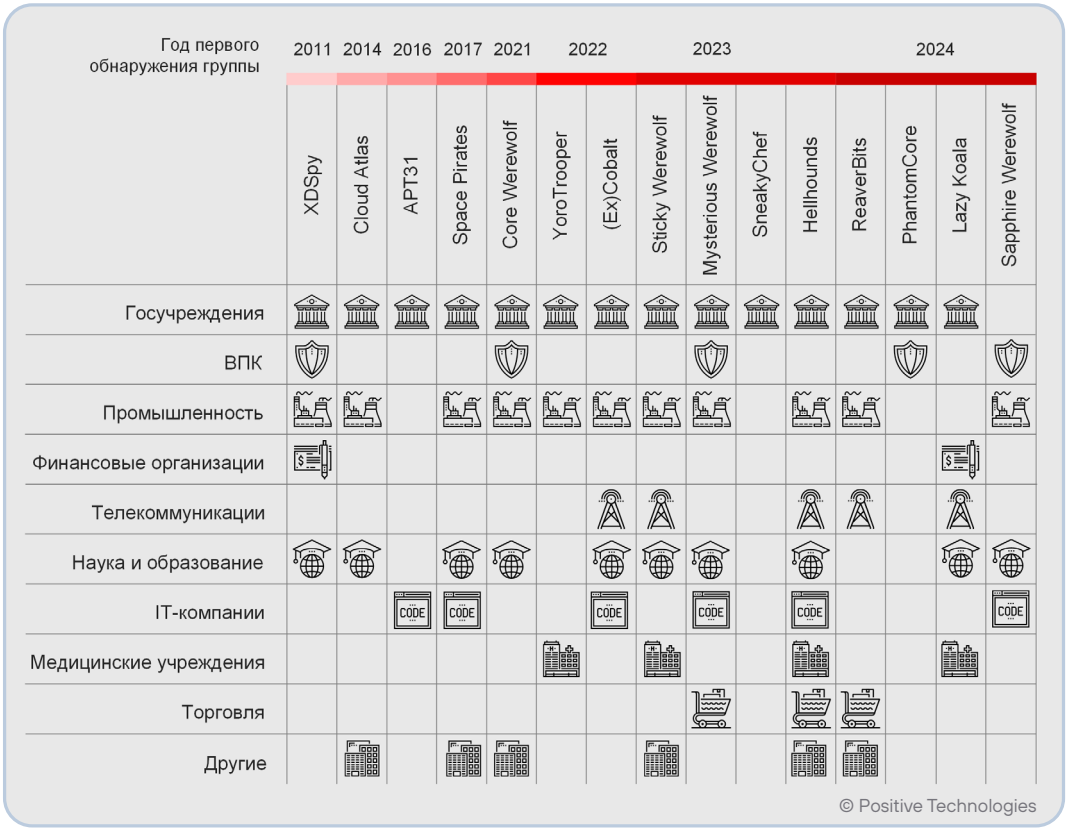


Рисунок 21. Отрасли, атакуемые кибершпионскими группами в странах СНГ в 2023 и 2024 года



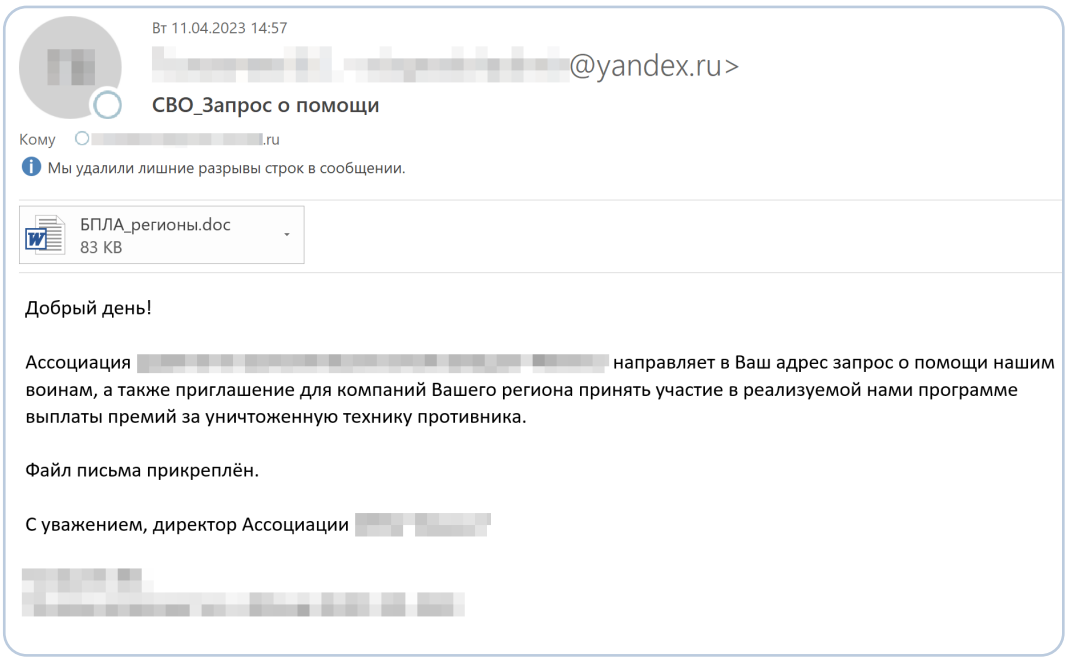
XDSpy

Группа XDSpy активна как минимум с 2011 года. В СНГ она атакует организации из самых разных отраслей преимущественно в России, Беларуси и Молдавии. В атаках использует одноименный инфостилер, для распространения которого делает фишинговые рассылки. Примеры вредоносных вложений из таких рассылок мы публиковали в одном из наших ежеквартальных отчетов.

Cloud Atlas

Злоумышленники из группы Cloud Atlas действуют как минимум с 2014 года. Они атакуют множество отраслей и стран по всему миру, включая страны СНГ. Специалисты TI-департамента PT ESC регулярно фиксируют фишинговые кампании этой группы. В апреле 2023 года злоумышленники рассылали письма в крупные российские организации под видом просьбы о помощи в СВО. В документе использовалась техника Template Injection, о ней наши эксперты уже рассказывали ранее. В конце 2023 года коллеги зафиксировали фишинговые рассылки Cloud Atlas в адрес российской исследовательской госкомпании и агропромышленного предприятия. С февраля по март 2024 года группа совершила не менее пяти атак на госучреждения в России и Беларуси. В ходе этих атак рассылались фишинговые письма с вложениями, которые загружали вредоносные шаблоны с удаленного сервера.

Рисунок 22. Фишинговое письмо группы Cloud Atlas под видом просьбы помощи в СВО



APT31

Группа известна с 2016 года. В разное время атаковала организации в Европе, Канаде и США. Весной и летом 2024 года были зафиксированы кибершпионские кампании, направленные против организаций в России. В ходе операций киберпреступники использовали множество различных инструментов, в том числе новый бэкдор CloudSorcerer. В рамках весенней кампании в качестве основных командных серверов для бэкдора применялись публичные облачные службы. В июле киберпреступники использовали троян, известный с 2021 года, обновленный бэкдор CloudSorcerer и ранее неизвестный имплант, код которого схож с кодом бэкдора Clambling группы APT27.

Space Pirates

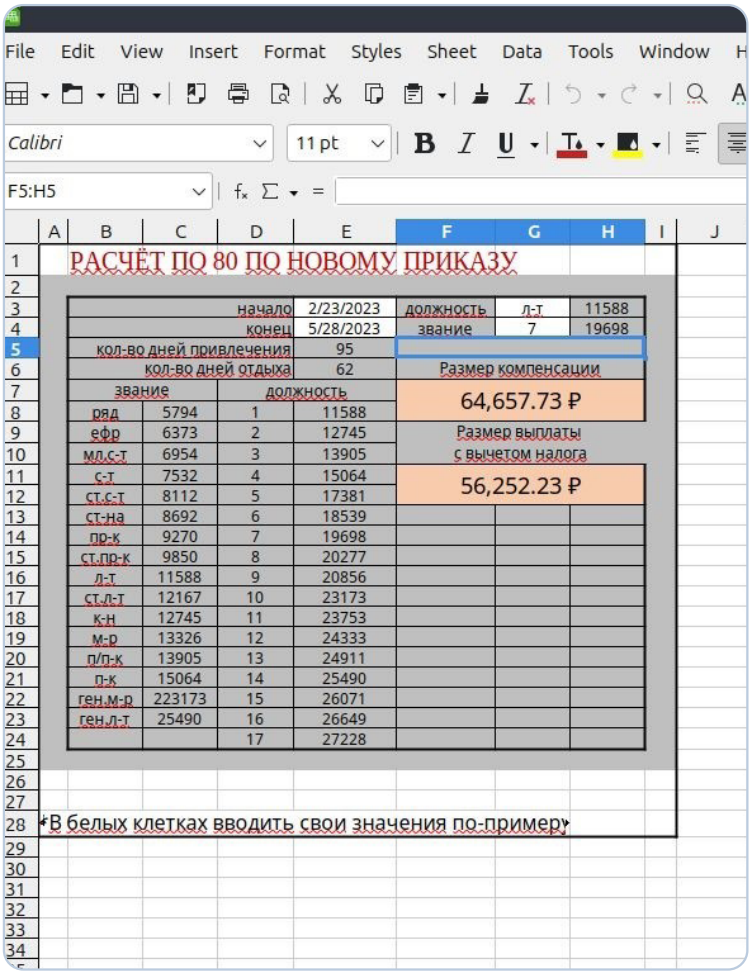
Space Pirates были обнаружены специалистами PT ESC в конце 2019 года. Группа активна как минимум с 2017 года. На протяжении 2023 года злоумышленники усиливали свою активность в отношении российских компаний. Специалисты TI-департамента PT ESC отмечают, что с момента обнаружения группировка практически не изменила свои тактики и техники, однако разработала новые инструменты и улучшила старые. Среди жертв в 2023 году специалисты TI-департамента PT ESC выявили государственные и образовательные учреждения, охранные предприятия, промышленные предприятия и предприятия топливно-энергетического комплекса, а также компании, занимающиеся информационной безопасностью.

Core Werewolf

О группе Core Werewolf впервые стало известно в 2021 году. Ее целью являются российские организации военно-промышленного комплекса, объекты критической информационной инфраструктуры.

Злоумышленники рассылают фишинговые письма с вредоносными вложениями, маскирующимися под различные документы — приказы, резюме, методические указания. К примеру, в конце 2023 года во время расследования одного инцидента команда PT CSIRT обнаружила письмо с фишингового домена fstec[.]support якобы от имени ФСТЭК. В качестве вложения к письмам прилагается самораспаковывающийся архив с клиентом ПО для удаленного доступа UltraVNC.

Рисунок 23. Вредоносное вложение из фишинговой рассылки Core Werewolf, выявленное специалистами TI-департамента PT ESC в I квартале 2024 года



YoroTrooper

Группа YoroTrooper впервые попала на радары специалистов по кибербезопасности в середине 2022 года. На сегодняшний день география ее целей ограничена странами СНГ. В период с мая по август 2023 года злоумышленники взломали несколько государственных веб-сайтов и завладели учетными записями, принадлежащими важным государственным лицам этих стран. Группа прикладывает усилия, чтобы скрыть свое происхождение, разместив большую часть инфраструктуры в Азербайджане.

Рисунок 24. Вредоносное вложение из фишинговой рассылки YoroTrooper, выявленное специалистами TI-департамента PT ESC в 2023 году



THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Повестка дня Технического консультативного совещания высокого уровня по сектору здравоохранения в Таджикистане

Национальный музей (3-ий этаж), г. Душанбе, 16 февраля 2023 г., 15:00-17:00

Время	Сессии	Докладчики
15:00-15:20	***Вступительное слово*** *Правительство Таджикистана (5 мин)* *Министерство здравоохранения и социальной защиты населения (5 мин)* *Всемирный банк (5 мин)* *ВОЗ (5 мин)*	*Г-жа Матлюбахон Сатториен, Заместитель Премьер-министра по социальным вопросам (участие подлежит подтверждению)* *Г-н Джамолиддин Абдуллозода, Министр здравоохранения и социальной защиты населения Республики Таджикистан* *Г-н Озан Севимли, Постоянный представитель Всемирного банка в Республике Таджикистан и Туркменистан* *Г-н Виктор Олшавски, Глава офиса ВОЗ в Таджикистане*
15:20-15:30	***Вступительная презентация:*** *Результаты мероприятий по охране здоровья в Республике Таджикистан* *Воздействие ситуации после пандемии COVID-19 и после кризиса на результаты мероприятий по охране здоровья в Республике Таджикистаню. Реформы здравоохранения в Республике Таджикистан. Достижения и незавершенная повестка. Приоритеты Правительства Республики Таджикистан в секторе здравоохранения, включая Инвестиционный план для финансирования приоритетных направлений.*	*Г-н Джамолиддин Абдуллозода, Министр здравоохранения и социальной защиты населения Республики Таджикистан*
15:30-15:40	***Человеческий капитал начинается со здравоохранения*** *Повестка Всеобщего охвата услугами здравоохранения до 2030 года и Глобальные приоритеты здравоохранения. Опыт реформ в регионе ЕЦА. Возможности совершенствования сектора*	*Г-жа Таня Дмитраченко, Руководитель глобальной практики в области «Здравоохранения, питания и народонаселения», Европа и Центральная Азия, Всемирный банк*

1

(Ex)Cobalt

Название (Ex)Cobalt было присвоено группе Cobalt, известной с 2016 года, после того как несколько лет назад киберпреступники сменили свою деятельность с финансово-мотивированных атак на кибершпионаж. За 2023 год специалистами PT ESC были расследованы атаки киберпреступников, нацеленные на российские организации. Также экспертами был обнаружен ранее неизвестный бэкдор GoRed, который использует группа (Ex)Cobalt.

Sticky Werewolf

Как минимум с апреля 2023 года организации в России и Беларуси атакует ранее неизвестная группа Sticky Werewolf. Первые выявленные атаки были направлены против госучреждений, однако впоследствии группа распространила свою деятельность и на другие отрасли. В качестве первоначального вектора злоумышленники осуществляют фишинговые рассылки с вредоносными вложениями, замаскированными под различные документы — предупреждения, заявления, повестки, предписания. Арсенал группы регулярно обновляется. Так, в течение 2023 года на компьютеры

жертв доставлялось ВПО для удаленного управления NetWire, Darktrack, Ozone RAT и инфостилер MetaStealer (разновидность RedLine). В 2024 году группа стала использовать инфостилеры Glory и Rhadamanthys.

Mysterious Werewolf

Об атаках группы Mysterious Werewolf стало впервые известно в 2023 году. В начале октября специалисты TI-департамента PT ESC обнаружили фишинговые письма, эксплуатирующие уязвимость CVE-2023-38831 в WinRAR. При исполнении вредоносных вложений жертвы заражались агентом Athena, который является частью фреймворка Mythic. Эту кампанию описали аналитики из Cyble, а позже, в ноябре, коллеги из BiZone дополнили описание и назвали группу Mysterious Werewolf. Целями группы становятся исключительно российские организации. В одной из последних кампаний злоумышленники использовали собственный бэкдор RingSpy, управляемый через Telegram-бота и предоставляющий удаленный доступ к скомпрометированным устройствам.

SneakyChef

Группа известна с 2023 года. В атаках использует троян SugarGh0st — улучшенная модификация известного трояна Gh0st, исходный код которого оказался в публичном доступе в 2008 году. В ноябре 2023 года исследовательская группа Cisco Talos опубликовала отчет, в котором привела детали кибератаки с использованием SugarGh0st на Министерство иностранных дел Узбекистана. В декабре 2023 года эксперты Национального координационного центра информационной безопасности Казахстана выявили фишинговую рассылку, нацеленную на заражение SugarGh0st казахстанского госоргана. В июне 2024 года эксперты Cisco Talos поделились подробностями новой кампании операторов SugarGh0st, дав им название SneakyChef. Группа атакует государственные организации через фишинговые рассылки. В качестве приманки использует отсканированные документы госорганов, большинство из которых связаны с министерствами иностранных дел и посольствами различных стран.

Hellhounds

В ноябре 2023 года специалисты PT ESC рассказали об атаках ранее неизвестной группировки Hellhounds, нацеленной исключительно на инфраструктуру российских компаний. В атаках использовался доработанный образец бэкдора Decoy Dog, который стал для группы флагманским инструментом. В 2024 году группа продолжила активно атаковать российские компании, и ко второму кварталу число жертв достигло 48. Среди них преимущественно IT-компании, госучреждения и промышленность.

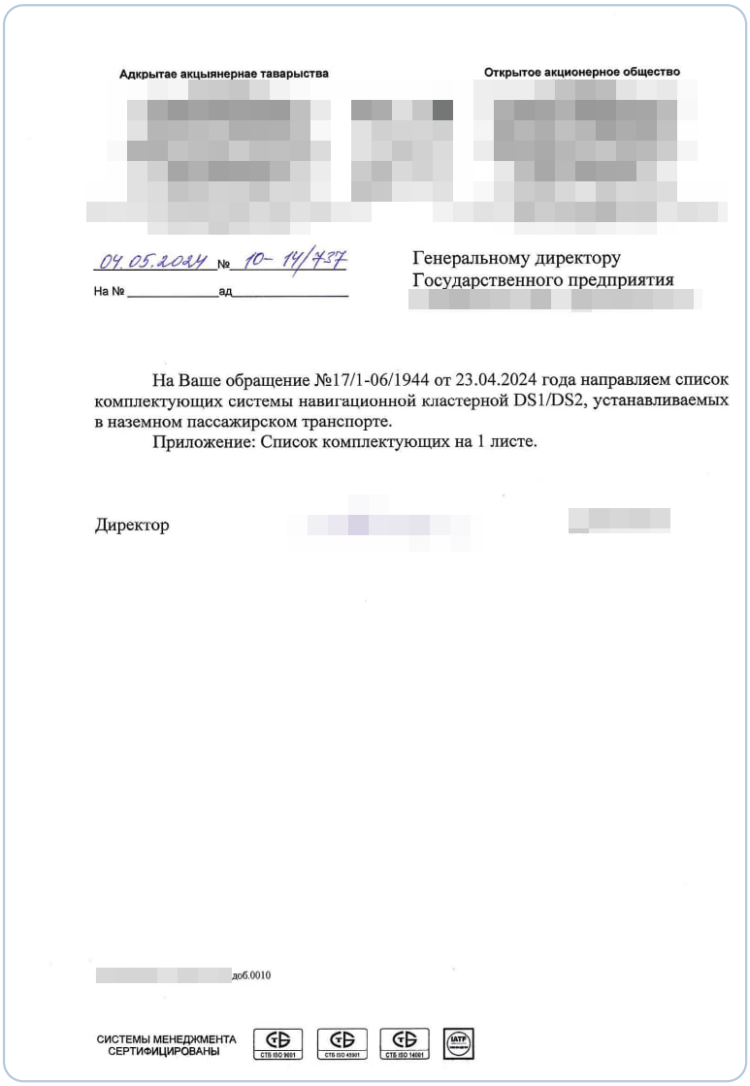
ReaverBits

Группа обнаружена в январе 2024 года. Злоумышленники рассылают фишинговые письма в адрес российских компаний от имени различных организаций, включая министерства. Первые письма датируются декабрем 2023 года. Через фишинговые письма группа распространяет шпионское ПО MetaStealer — форк распространенного в атаках на СНГ инфостилера RedLine.

PhantomCore

С января 2024 года российские компании активно атакует новая группа кибершпионов, получившая название PhantomCore. Злоумышленники рассылают фишинговые письма, эксплуатируя уязвимость CVE-2023-38831, однако вместо ZIP-архивов используются RAR-архивы. Жертвы заражаются ранее не описанным трояном удаленного доступа — PhantomRAT. В качестве приманок используются различные служебные документы — договоры, акты сверки, счета-фактуры. В июне 2024 года эксперты TI-департамента PT ESC зафиксировали фишинговые рассылки PhantomCore в адрес белорусских учреждений.

Рисунок 25. Вредоносное вложение из фишинговой рассылки PhantomCore, выявленной специалистами TI-департамента PT ESC в июне 2024 года



Адкрытае акцыянернае таварыства

Открытое акционерное общество

04.05.2024 № 10- 14/437

На № _____ад_____

Генеральному директору
Государственного предприятия

На Ваше обращение №17/1-06/1944 от 23.04.2024 года направляем список комплектующих системы навигационной кластерной DS1/DS2, устанавливаемых в наземном пассажирском транспорте.

Приложение: Список комплектующих на 1 листе.

Директор

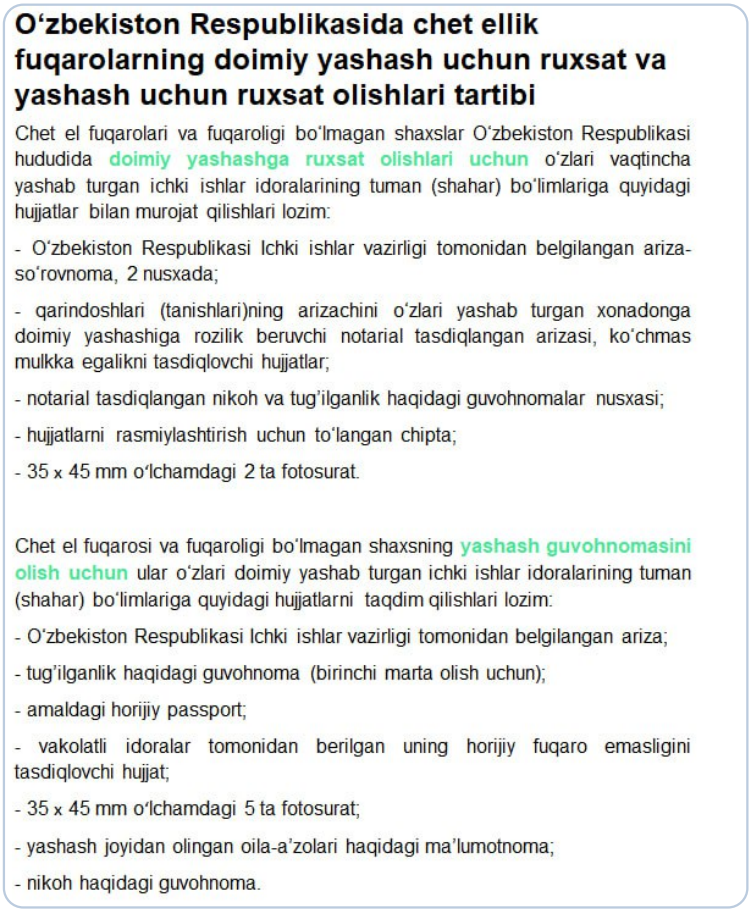
доб.0010

СИСТЕМЫ МЕНЕДЖМЕНТА СЕРТИФИЦИРОВАНЫ

Lazy Koala

Деятельность группы Lazy Koala впервые была выявлена специалистами TI-департамента PT ESC во время расследования серии атак, направленных на государственные структуры ряда стран СНГ в I квартале 2024 года. В ходе фишинговых рассылок группа распространяла вредоносное ПО LazyStealer, предназначенное для кражи учетных данных из браузеров с дальнейшей пересылкой их в Telegram-бот. В круг интересов злоумышленников, помимо госучреждений, входят также финансовая отрасль, медицинские организации, наука и образование. В мае 2024 года эксперты TI-департамента PT ESC зафиксировали новые атаки на Азербайджан, Беларусь и Узбекистан. В атаках на Азербайджан и Беларусь злоумышленники изменили формат отправляемых в бот сообщений и сменили ник с Koala на Capybara, а в атаках на Узбекистан вместо Telegram-бота использовался хостинг.

Рисунок 26. Документ из фишинговой рассылки Lazy Koala, выявленной специалистами TI-департамента PT ESC в мае 2024 года



O‘zbekiston Respublikasida chet ellik fuqarolarning doimiy yashash uchun ruxsat va yashash uchun ruxsat olishlari tartibi

Chet el fuqarolari va fuqaroligi bo‘lmagan shaxslar O‘zbekiston Respublikasi hududida doimiy yashashga ruxsat olishlari uchun o‘zlari vaqtincha yashab turgan ichki ishlar idoralarining tuman (shahar) bo‘limlariga quyidagi hujjatlar bilan murojat qilishlari lozim:

- O‘zbekiston Respublikasi Ichki ishlar vazirligi tomonidan belgilangan ariza-so‘rovnoma, 2 nusxada;
- qarindoshlari (tanishlari)ning arizachini o‘zlari yashab turgan xonadonga doimiy yashashiga rozilik beruvchi notarial tasdiqlangan arizasi, ko‘chmas mulkka egalikni tasdiqlovchi hujjatlar;
- notarial tasdiqlangan nikoh va tug’ilganlik haqidagi guvohnomalar nusxasi;
- hujjatlarni rasmiylashtirish uchun to‘langan chipta;
- 35 x 45 mm o‘lchamdagi 2 ta fotosurat.

Chet el fuqarosi va fuqaroligi bo‘lmagan shaxsning yashash guvohnomasini olish uchun ular o‘zlari doimiy yashab turgan ichki ishlar idoralarining tuman (shahar) bo‘limlariga quyidagi hujjatlarni taqdim qilishlari lozim:

- O‘zbekiston Respublikasi Ichki ishlar vazirligi tomonidan belgilangan ariza;
- tug’ilganlik haqidagi guvohnoma (birinchi marta olish uchun);
- amaldagi horijiy passport;
- vakolatli idoralar tomonidan berilgan uning horijiy fuqaro emasligini tasdiqlovchi hujjat;
- 35 x 45 mm o‘lchamdagi 5 ta fotosurat;
- yashash joyidan olingan oila-a’zolari haqidagi ma’lumotnoma;
- nikoh haqidagi guvohnoma.

Sapphire Werewolf

Группа Sapphire Werewolf активна с марта 2024 года. Совершила уже более 300 атак на российские организации из различных отраслей. Для кражи данных злоумышленники используют Amethyst — инструмент собственной разработки, созданный на базе инфостилера с открытым исходным кодом SapphireStealer. Для его доставки злоумышленники рассылали фишинговые письма, маскируя вредоносные вложения под различные юридические документы.

Тепловая карта тактик и техник кибершпионских групп (MITRE ATT&CK)

Resource Development	Acquire Infrastructure	Compromise Accounts	Compromise Infrastructure	Develop Capabilities	Establish Accounts	Obtain Capabilities	Stage Capabilities																
Initial Access	Exploit Public-Facing Application	Phishing	Supply Chain Compromise	Trusted Relationship	Valid Accounts																		
Execution	Command and Scripting Interpreter	Exploitation for Client Execution	Inter-Process Communication	Native API	Scheduled Task/Job	Shared Modules	System Services	User Execution	Windows Management Instrumentation														
Persistence	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	Create Account	Create or Modify System Process	Event Triggered Execution	Hijack Execution Flow	Scheduled Task/Job	Server Software Component	Valid Accounts														
Privilege Escalation	Abuse Elevation Control Mechanism	Access Token Manipulation	Boot or Logon Autostart Execution	Create or Modify System Process	Exploitation for Privilege Escalation	Process Injection	Scheduled Task/Job																
Defense Evasion	Abuse Elevation Control Mechanism	Access Token Manipulation	BITS Jobs	Debugger Evasion	Deobfuscate/ Decode Files or Information	Execution Guardrails	Exploitation for Defense Evasion	Hide Artifacts	Hijack Execution Flow	Impair Defenses	Indicator Removal	Indirect Command Execution	Masquerading	Modify Registry	Modify System Image	Obfuscated Files or Information	Process Injection	Reflective Code Loading	Rootkit	Subvert Trust Controls	System Binary Proxy Execution	Template Injection	Valid Accounts	Virtualization/ Sandbox Evasion
Credential Access	Brute Force	Credentials from Password Stores	Exploitation for Credential Access	Input Capture	Network Sniffing	OS Credential Dumping	Steal or Forge Kerberos Tickets	Steal Web Session Cookie	Unsecured Credentials														
Discovery	Account Discovery	Application Window Discovery	Browser Information Discovery	Debugger Evasion	Domain Trust Discovery	File and Directory Discovery	Group Policy Discovery	Network Service Discovery	Network Share Discovery	Peripheral Device Discovery	Permission Groups Discovery	Process Discovery	Query Registry	Remote System Discovery	Software Discovery	System Information Discovery	System Location Discovery	System Network Configuration Discovery	System Owner/User Discovery	Virtualization/ Sandbox Evasion				
Lateral Movement	Exploitation of Remote Services	Lateral Tool Transfer	Remote Service Session Hijacking	Remote Services	Taint Shared Content	Use Alternate Authentication Material																	
Collection	Archive Collected Data	Audio Capture	Automated Collection	Clipboard Data	Data from Local System	Data from Network Shared Drive	Data from Removable Media	Data Staged	Email Collection	Input Capture	Screen Capture	Video Capture											
Command and Control	Application Layer Protocol	Data Encoding	Data Obfuscation	Dynamic Resolution	Encrypted Channel	Fallback Channels	Ingress Tool Transfer	Multi-Stage Channels	Non-Application Layer Protocol	Non-Standard Port	Protocol Tunneling	Proxy	Remote Access Software	Web Service									
Exfiltration	Automated Exfiltration	Data Transfer Size Limits	Exfiltration Over Alternative Protocol	Exfiltration Over C2 Channel	Exfiltration Over Web Service	Transfer Data to Cloud Account																	

© Positive Technologies

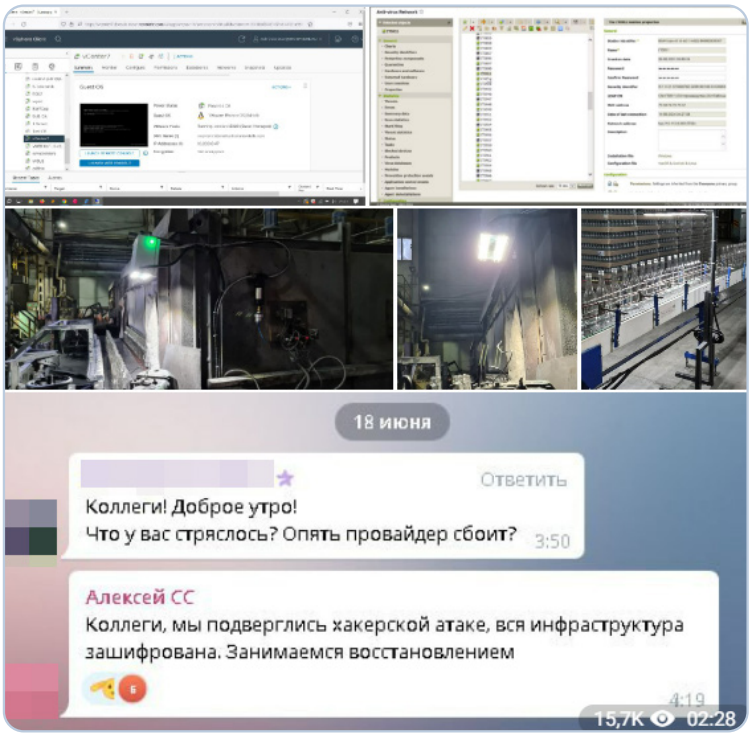
Технику используют:	1–3 группи-ровки	4–6 группи-ровок	7–9 группи-ровок	10–12 группи-ровок	13–15 группи-ровок

Атаки хактивистов

По нашим данным, 26% кибератак против СНГ в 2023 и 2024 годах были совершены хактивистами. Это киберпреступники, которые атакуют, руководствуясь политическими или социальными мотивами. К примеру, в феврале 2023 года проукраинские хактивисты взломали десятки сайтов российских организаций и произвели дефейс, разместив на страницах видеоролики с якобы горящим Кремлем.

Мы проанализировали методы 24 хактивистских группировок, которые были наиболее активны в странах СНГ в течение последних двух лет. Целью многих групп является полное разрушение скомпрометированной инфраструктуры путем шифрования либо удаления данных.

Рисунок 27. Сообщение хактивистов с доказательствами взлома российского промышленного холдинга летом 2024 года



Восемь хактивистских группировок специализируются на DDoS-атаках. Как правило, основным драйвером для них является геополитика. Однако поводом для атак на отказ в обслуживании могут стать любые события, вызвавшие общественный резонанс. К примеру, в мае 2024 года в Бишкеке после конфликта между киргизскими и иностранными студентами несколько хактивистских групп устроили DDoS-атаки на ресурсы различных организаций в Кыргызстане, предположительно, в знак протеста против притеснения иностранных студентов.

Рисунок 28. Методы хактивистов в странах СНГ (количество группировок)

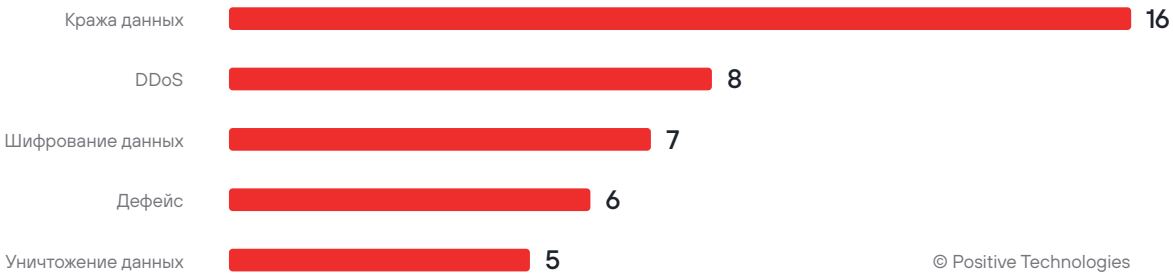
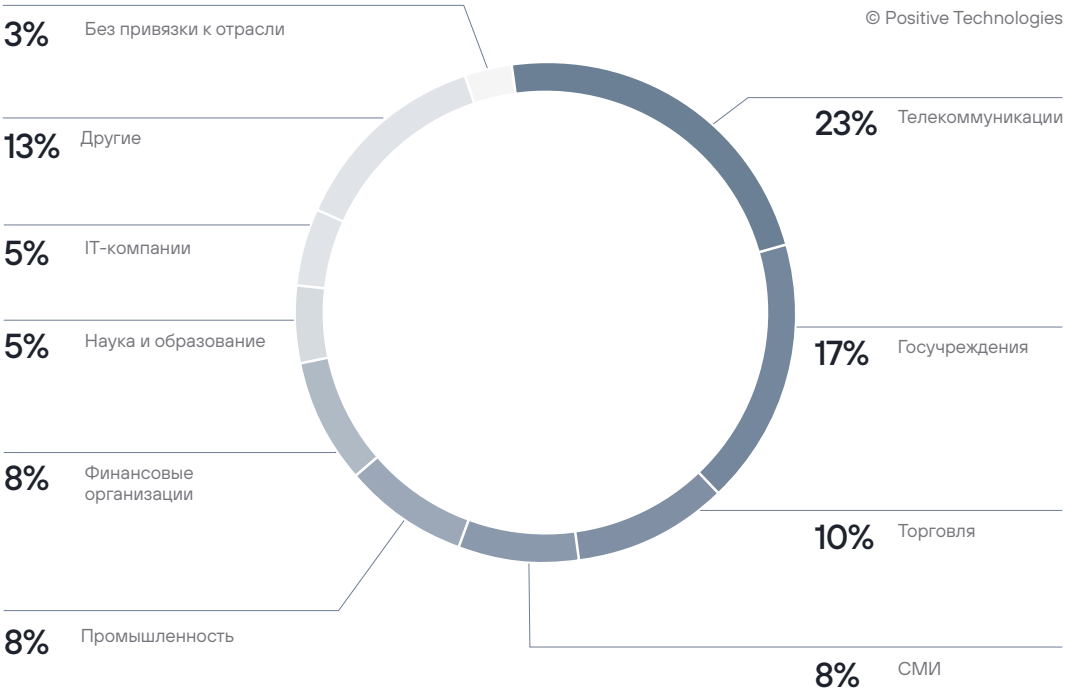
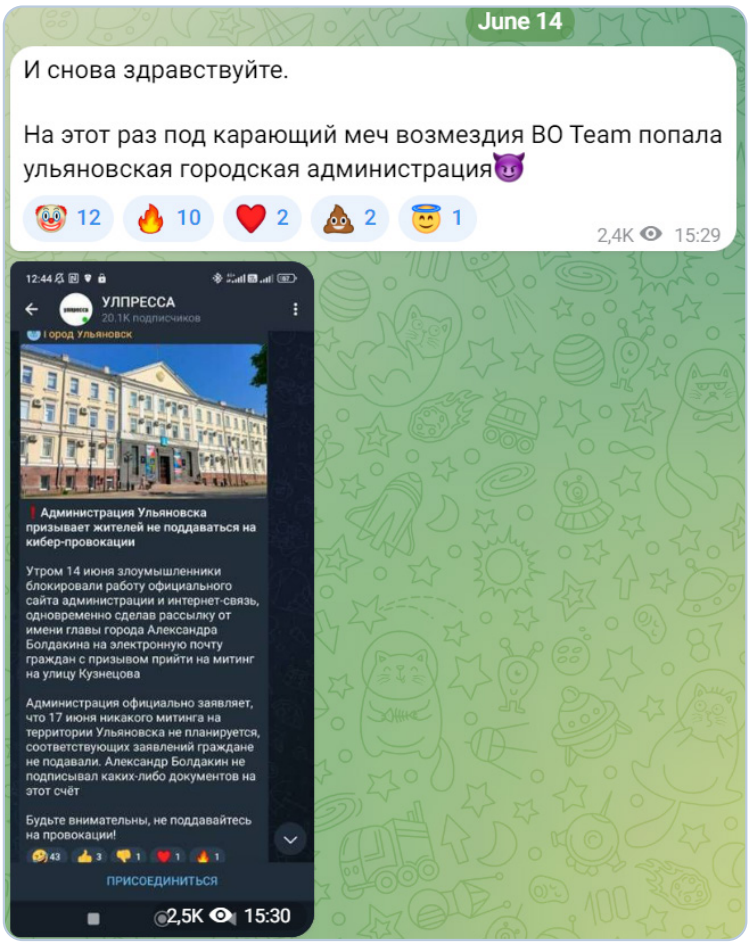


Рисунок 29. Жертвы хактивистов в странах СНГ



Наиболее часто жертвами хактивистов становились телекоммуникационные компании (23%) и госучреждения (17%). Нарушения в работе госорганов способны подорвать общественное доверие и вызвать социальное недовольство. Зачастую кибератаки хактивистов направлены именно на это. К примеру, в июне 2024 года группа хактивистов BO Team атаковала инфраструктуру администрации Ульяновска, заблокировала работу сайта и разослала жителям фейковые приглашения на митинг.

Рисунок 30. Сообщение в Telegram-канале хактивистов BO Team об атаке на администрацию Ульяновска



Как правило, атаки хактивистов на правительственные организации усиливаются накануне знаковых политических событий. Например, группа Nebula заявила об атаке на российскую избирательную инфраструктуру накануне президентских выборов в марте 2024 года.

Атаки финансово мотивированных операторов шифровальщиков

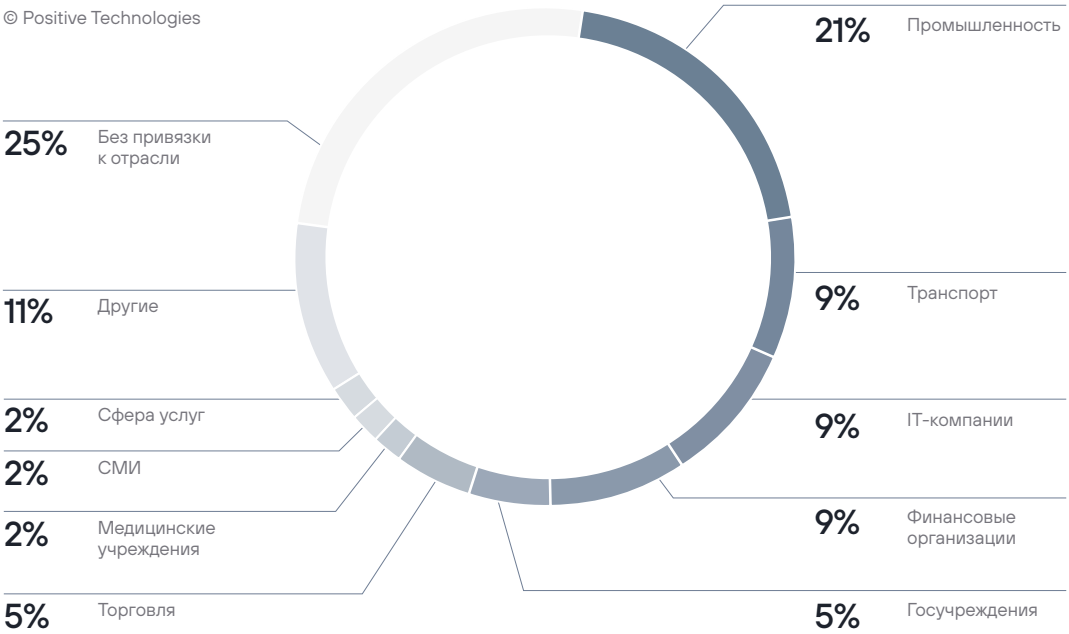
В странах СНГ каждая пятая (22%) атака на организации с использованием ВПО приходится на долю шифровальщиков, 88% этих атак имеют финансовую мотивацию. Это связано с потенциально высокими выкупами, которые можно получить от жертв. Сегодня атаки с помощью программ-вымогателей остаются одной из самых прибыльных форм киберпреступности не только в СНГ, но и во всем мире. Суммы, которые в 2023 и 2024 годах вымогатели запрашивали у скомпрометированных организаций в СНГ, колеблются от нескольких сотен тысяч до нескольких сотен миллионов рублей. Максимальную сумму выкупа в размере 1 млн долларов США злоумышленники требовали у российского банка.

В странах СНГ набирают обороты многофакторные вымогательские кампании (multi-extortion ransomware). В таких атаках злоумышленники используют сразу несколько рычагов давления, чтобы заставить жертву заплатить выкуп. Наиболее часто мы видим двойное воздействие на жертву (double extortion). В таких атаках помимо стандартного требования денег за расшифрование данных злоумышленники угрожают обнародовать либо продать украденную из компании информацию в случае отказа заплатить выкуп.

Наиболее часто жертвами вымогателей становятся промышленные и производственные предприятия — 21% от всех атак шифровальщиков. Один из недавних заметных инцидентов связан с атакой на агрокомплекс им. Н. И. Ткачева — одно из крупнейших сельскохозяйственных предприятий в России. В апреле 2024 года злоумышленники проникли в инфраструктуру компании, вызвали сбои в работе и потребовали выкуп в размере 500 млн рублей.

На втором месте среди жертв финансово мотивированных шифровальщиков — транспорт, финансовые организации и IT-компании (по 9%). Сбои в логистических процессах являются недопустимым событием для транспортной отрасли, поэтому транспортные компании крайне заинтересованы в максимально быстром восстановлении, и у злоумышленников повышается шанс получить выкуп. Финансовые и технологические компании обладают высокой платежеспособностью, поэтому также привлекательны для финансово мотивированных атакующих. Кроме того, IT-компании становятся мишенью из-за возможности атак типа trusted relationship — через подрядчиков IT-услуг у киберпреступников появляется возможность получить доступ в сети их клиентов.

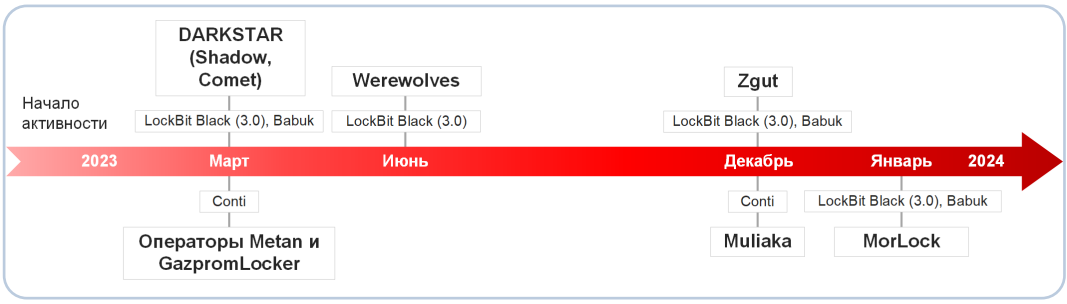
Рисунок 31. Жертвы атак шифровальщиков в странах СНГ



Ряд групп, атакующих СНГ, шифруют данные собственным уникальным ВПО. В то же время несколько лет назад произошли события, которые привели к снижению порога вхождения в кибервымогательство при помощи шифровальщиков. В 2021 году в открытый доступ утекли исходные

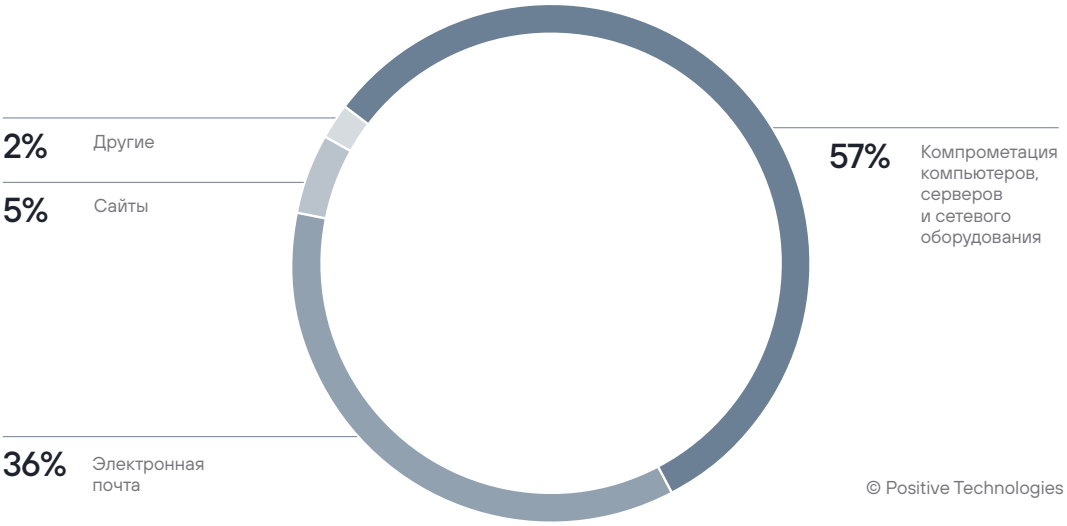
коды программы-вымогателя Babuk, а в 2022 году в публичном пространстве оказались исходные коды Conti и билдер LockBit Black (3.0). Это привело к увеличению атак с использованием шифровальщиков и появлению новых хакерских группировок, специализирующихся на таких атаках.

Рисунок 32. Финансово мотивированные группы, использующие в атаках на СНГ шифровальщики семейств LockBit Black, Babuk и Conti



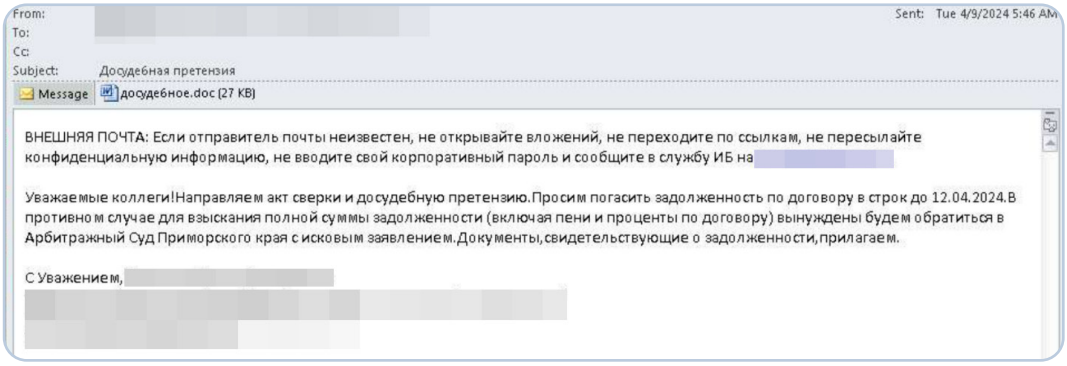
Наиболее распространенный вектор первоначального проникновения шифровальщиков — компрометация сетевого периметра организации (57%). Прежде всего речь идет об эксплуатации уязвимостей в публичных приложениях, к примеру в почтовых серверах Microsoft Exchange и Zimbra. Помимо этого, злоумышленники попадают в инфраструктуру через службы удаленного доступа, например RDP, VPN, используя легитимные учетные данные, приобретенные на теневых площадках.

Рисунок 33. Способы распространения шифровальщиков в СНГ



Более трети (36%) атак шифровальщиков начинаются с фишинговых писем. Так, в I квартале 2024 года группа Werewolves проводила массовые фишинговые кампании, рассылая в российские организации вредоносные документы под видом досудебных претензий и актов сверок. Письма отправлялись в промышленные, финансовые и телекоммуникационные организации.

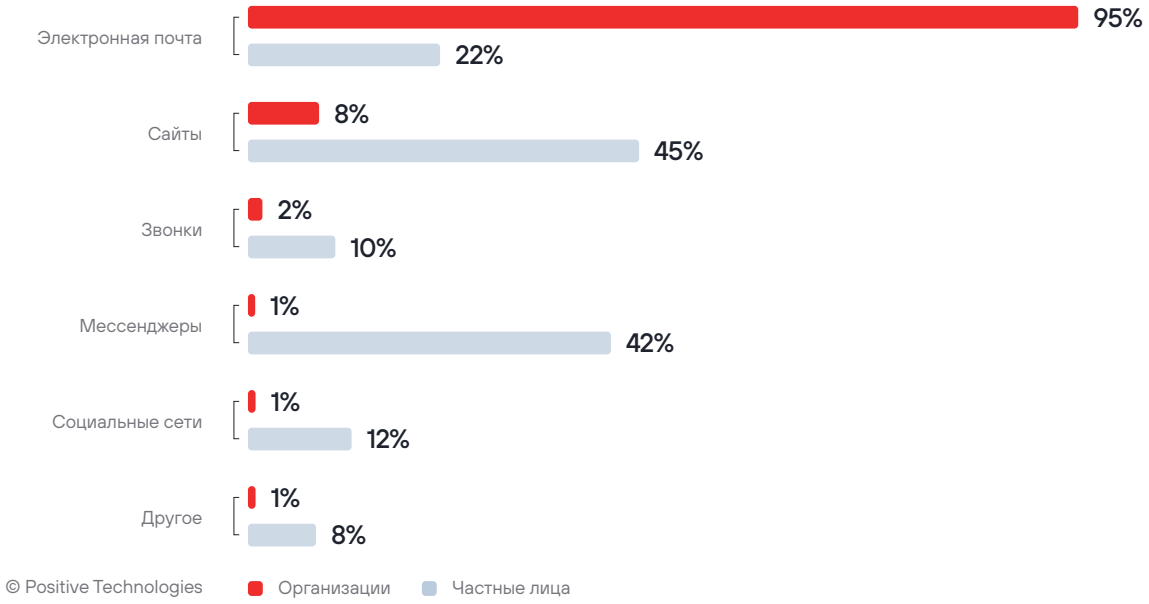
Рисунок 34. Документ из фишинговой рассылки Werewolves, выявленной специалистами TI-департамента PT ESC в апреле 2024 года



Фишинговые атаки и скам

В 48% атак на организации и в 92% атак на частных лиц использовались методы социальной инженерии. Частные лица преимущественно становились жертвами социальной инженерии, посещая мошеннические сайты (45%), либо сталкивались со злоумышленниками в мессенджерах (42%). Согласно отчету Банка России, только в 2023 году регулятор направил операторам связи информацию о более чем 575 тысячах телефонных номеров, использованных злоумышленниками для кражи денег у граждан, и инициировал блокировку почти 43 тысяч мошеннических веб-ресурсов и страниц в соцсетях. Мошенники регулярно модернизируют известные схемы обмана и придумывают новые.

Рисунок 35. Используемые злоумышленниками каналы социальной инженерии



Кража учетных данных через фишинговые письма

Специалисты TI-департамента PT ESC регулярно фиксируют фишинговые кампании, нацеленные на сбор учетных данных сотрудников различных организаций в СНГ. Рассмотрим несколько примеров. В них мы расскажем про наиболее интересные фишинговые рассылки, направленные в адрес организаций в СНГ, которые эксперты TI-департамента PT ESC фиксировали в первой половине 2024 года.

В январе специалисты TI-департамента PT ESC обнаружили фишинговое письмо, направленное в банк Армении, с просьбой подписать документы. В нем была кнопка для просмотра документов, при нажатии на которую жертва перенаправлялась на фишинговую страницу с формой для ввода учетных данных. В форме уже был введен логин жертвы и оставалось ввести только пароль.

Рисунок 36. Фишинговое письмо для кражи учетных данных, отправленное сотруднику банка в Армении

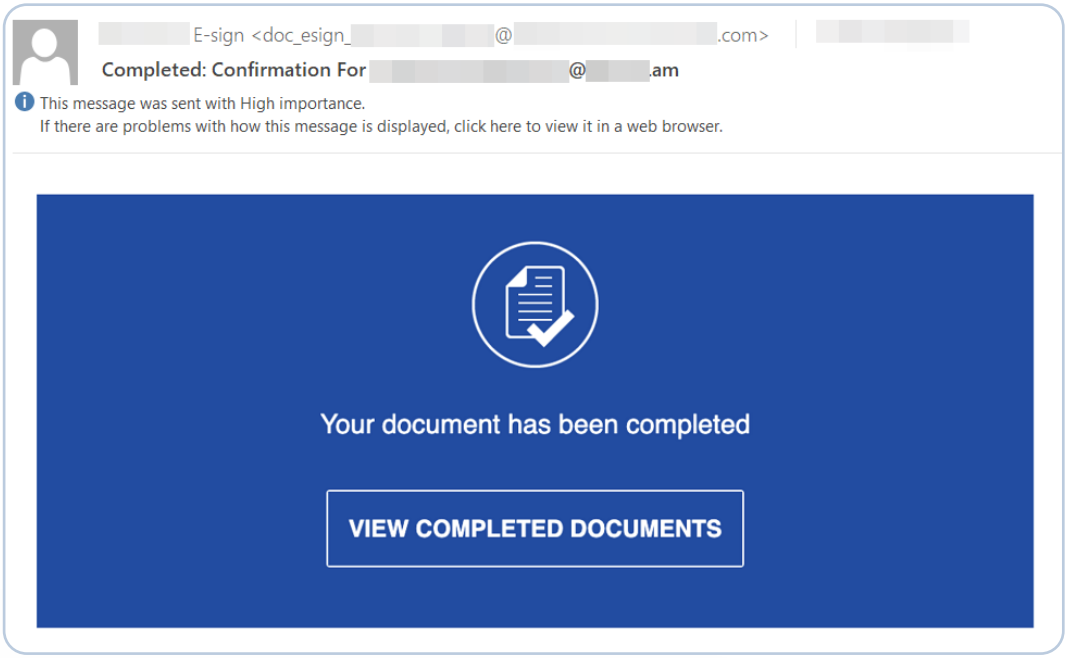
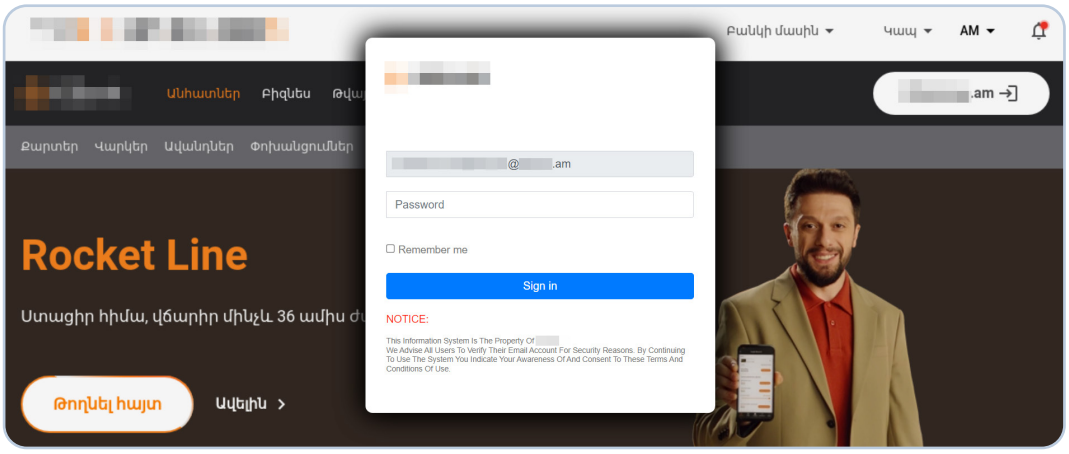
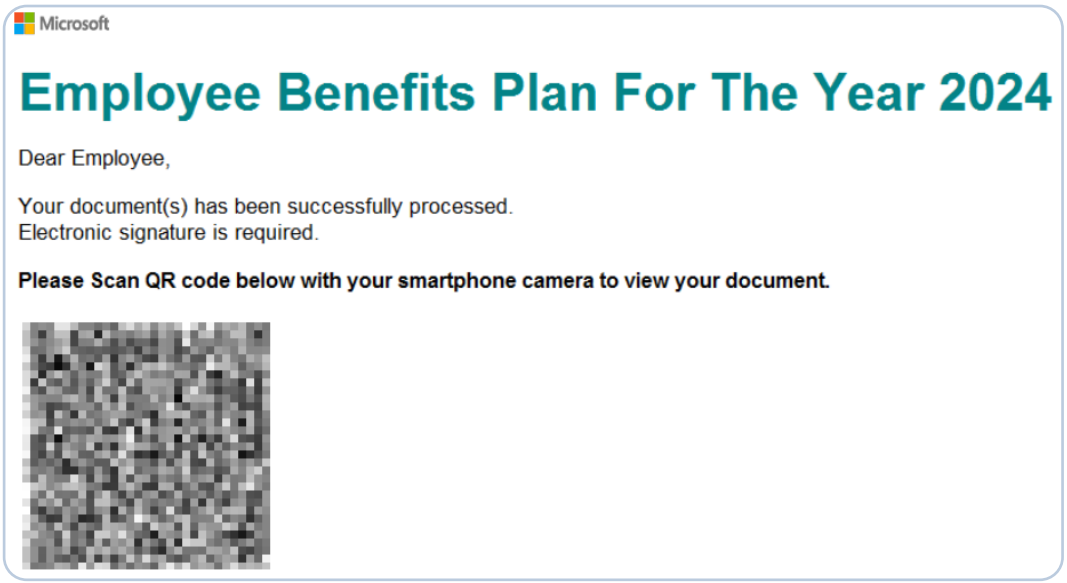


Рисунок 37. Поддельная форма для ввода учетных данных, маскирующаяся по ресурс банка в Армении



В феврале и марте фиксировались аналогичные фишинговые кампании, направленные против российских организаций. В них также были просьбы подписать документы через DocuSign. Фишинговые ссылки были «зашиты» в QR-коды, при переходе по которым открывались фейковые формы авторизации с уже введенным логином жертвы.

Рисунок 38. Фишинговое письмо с QR-кодом



Во II квартале 2024 года были обнаружены два письма, направленные в банки в Беларуси. Оба письма содержали файлы в формате PDF с миниатюрами документов, в которых были ссылки на фишинговые страницы с фейковыми формами для ввода логина, пароля и номера телефона.

Рисунок 39. Фишинговое письмо для кражи учетных данных, отправленное сотруднику банка в Беларуси

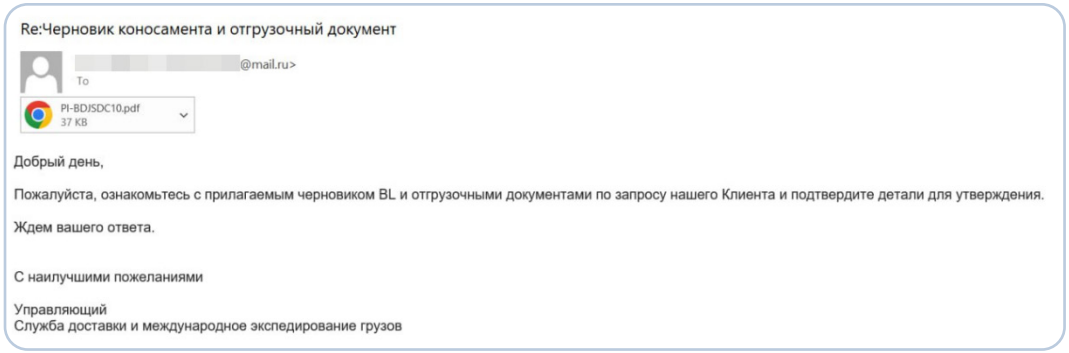


Рисунок 40. Поддельная форма для ввода учетных данных и номера телефона (пример 1)

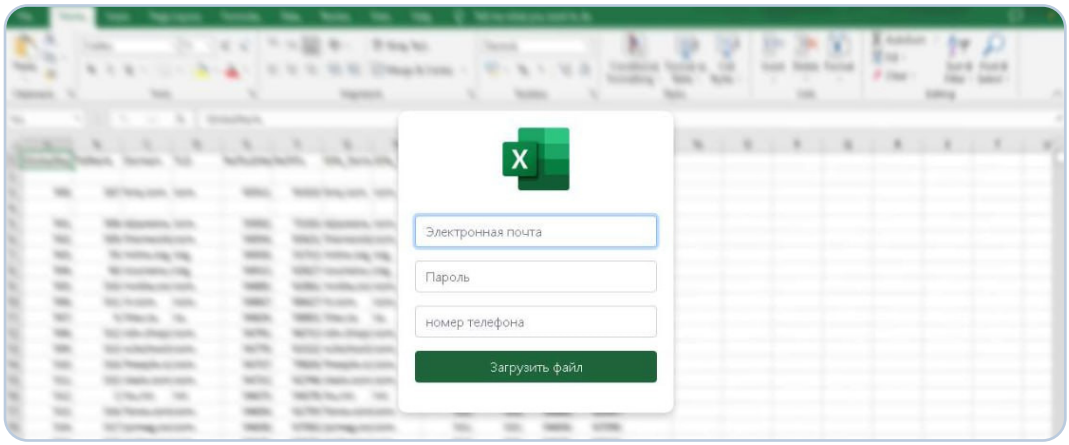
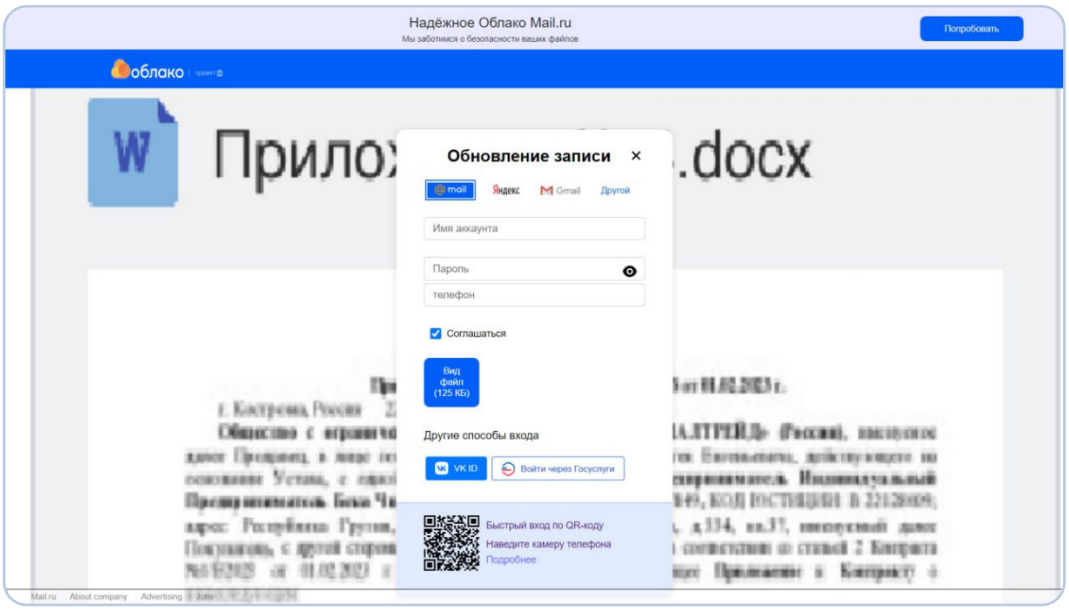
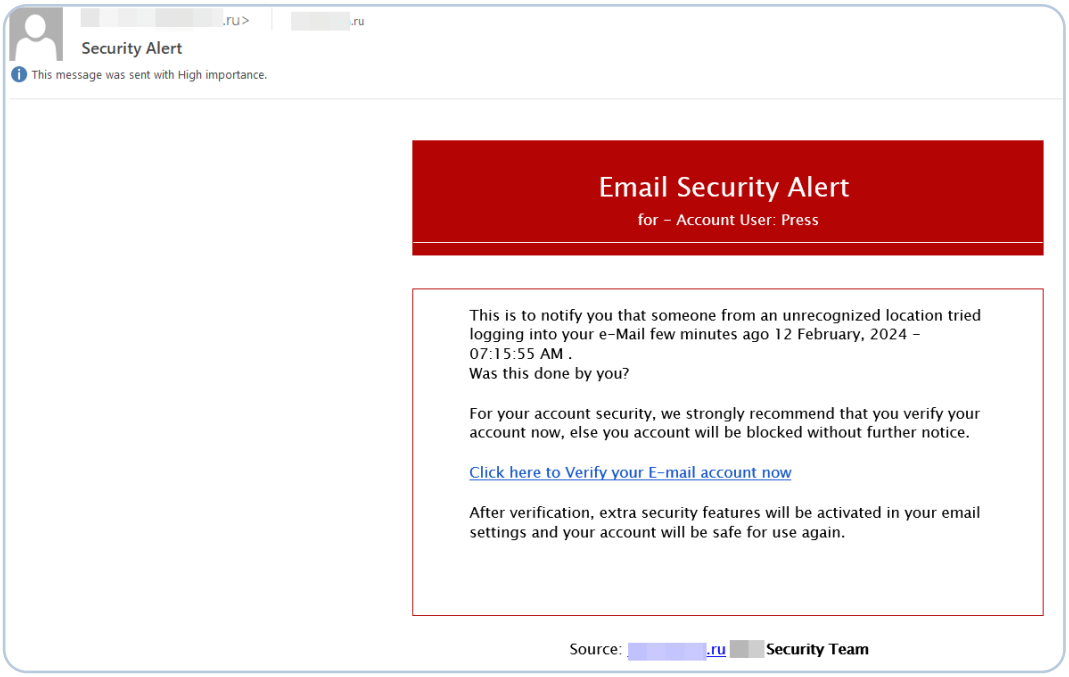


Рисунок 41. Поддельная форма для ввода учетных данных и номера телефона (пример 2)



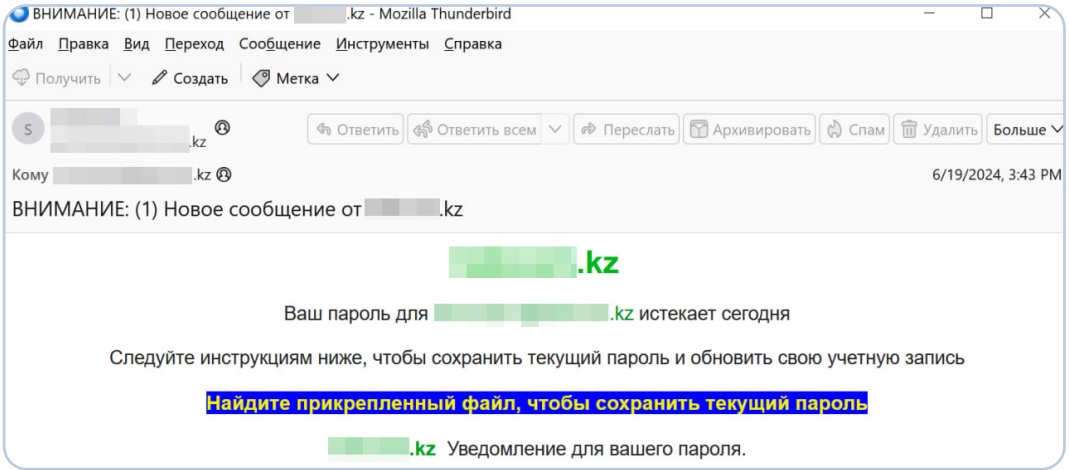
Распространенная тема фишинговых писем, направленных на кражу учетных данных, — это требование сменить пароль под предлогом окончания его срока действия. В феврале специалисты TI-департамента PT ESC обнаружили подобное письмо в адрес российской организации. Ссылка из письма вела на фишинговую страницу, копирующую страницу входа Roundcube Webmail.

Рисунок 42. Фишинговое письмо в адрес российской организации с требованием сменить пароль



В июне 2024 года специалисты TI-департамента PT ESC обнаружили фишинговое письмо с требованием обновить пароль, направленное в организацию в Казахстане. Форма обновления пароля находилась в прикрепленном к письму HTML-файле, который должен открыть пользователь. Данные, введенные жертвой в эту форму, отсылаются на URL легитимного сервиса formspark.io для заполнения разного рода форм и попадают в руки злоумышленников.

Рисунок 43. Фишинговое письмо в адрес организации в Казахстане с требованием сменить пароль



Еще один пример — фишинговое письмо в адрес российской топливно-энергетической организации. К письму была приложена фишинговая HTML-страница Maersk Line Shipping Document.XLS.html. Открыв файл, жертва видит перед собой фейковую страницу с формой для ввода учетных данных. Она замаскирована под ресурс датской логистической компании Maersk Line, специализирующейся на морских контейнерных перевозках. Введенные на странице данные отправляются на адрес сервиса для сбора данных с помощью форм.

Рисунок 44. Фишинговое письмо для кражи учетных данных в адрес организации в России

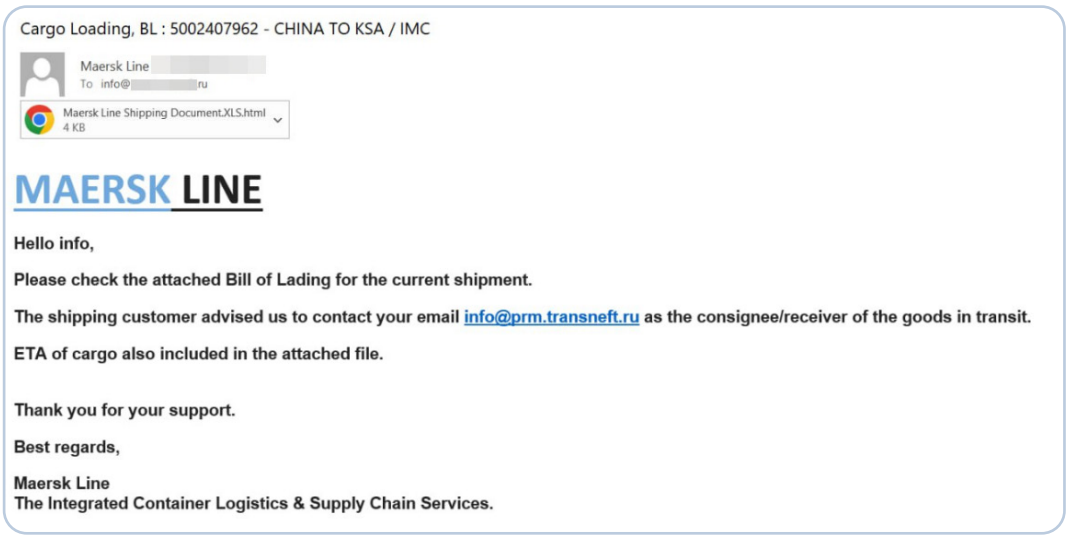
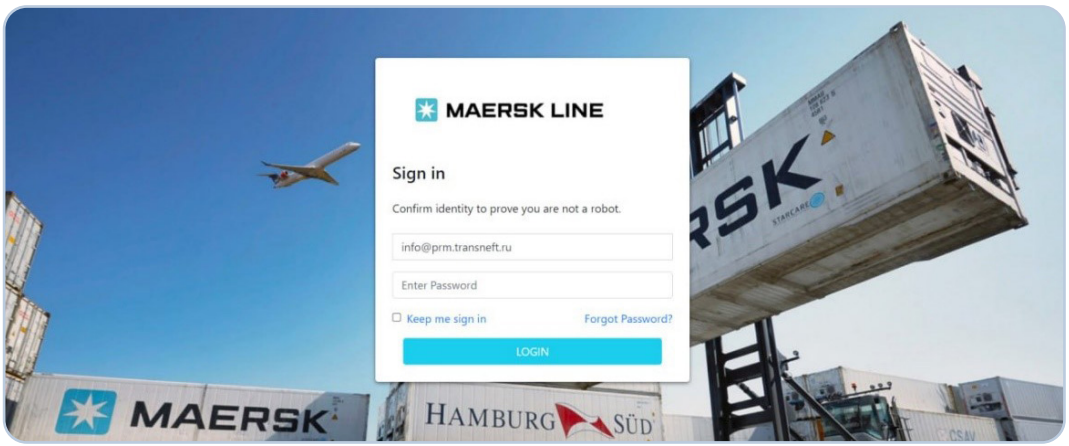


Рисунок 45. Поддельная форма для ввода учетных данных



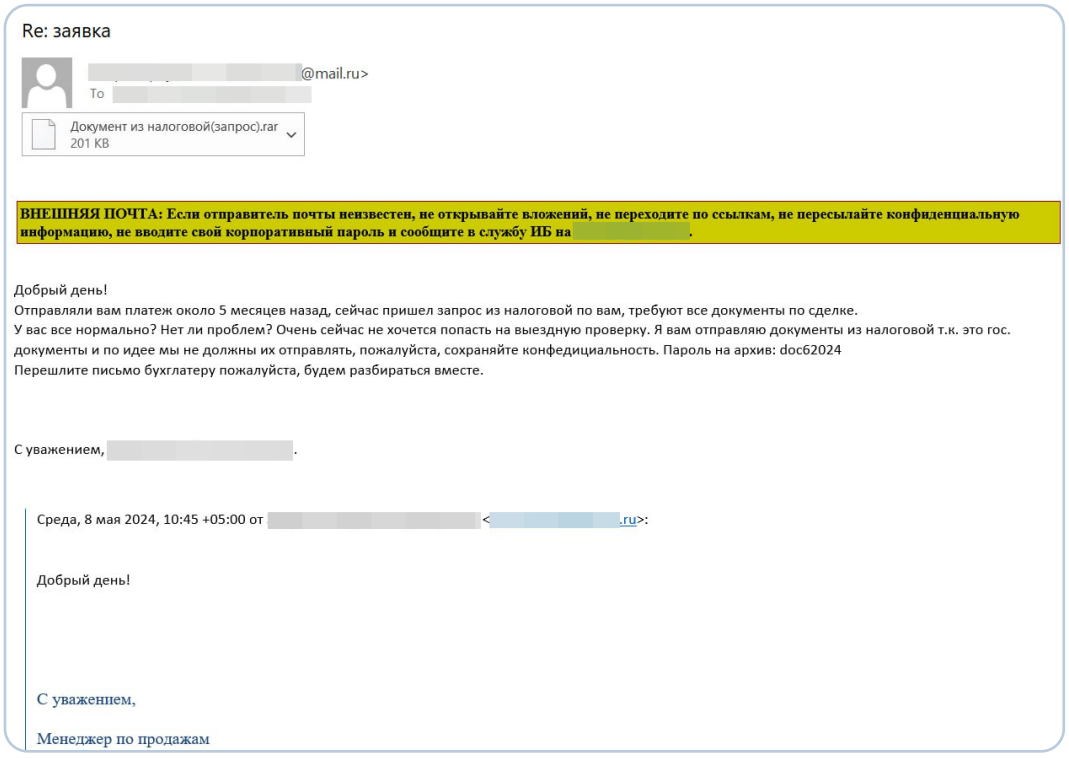
(Не)уплаченные налоги

Одна из старых, но все еще работающих тем для социальной инженерии, — уплата налогов. Мошенники могут обещать вернуть уплаченные налоги или уведомлять о задолженности. Выдавая себя за представителей налоговых органов или сотрудников банков, они выманивают персональные, учетные или банковские данные, угрожая штрафами и заморозкой счетов. В августе 2023 года Министерство по налогам и сборам Республики Беларусь информировало об участившихся случаях мошеннических звонков якобы от сотрудников министерства с целью уточнения паспортных данных. О волне фишинговых рассылок в январе текущего года уведомляла ФНС России. В феврале россиян предупредили еще об одной волне фишинга. На этот раз мошенники рассылали письма о необходимости уплаты несуществующего налога на СВО.

Стоит отметить, что «налоговые» схемы кибермошенники используют не только против частных лиц, но и в атаках на юрлица. В начале года в организации Казахстана по электронной почте стали поступать фейковые предупреждения о налоговых нарушениях. Фишинговая кампания была приурочена к завершению в стране моратория на налоговые проверки малого и среднего бизнеса. Письма содержали вредоносный PDF-документ, загружающий на компьютеры жертв ВПО для удаленного управления.

Во II квартале 2024 года специалисты TI-департамента PT ESC выявили фишинговые рассылки финансово мотивированной хакерской группировки Hive0117. Для нее характерно распространение бэкдора DarkWatchman. В июне злоумышленники рассылали в российские компании дроппер этого ВПО под видом программы «Налогоплательщик ЮЛ» (NalogUL.exe). Помимо этого, специалисты TI-департамента PT ESC зафиксировали фишинговую рассылку в адрес производственного предприятия с вредоносным архивом, содержащим DarkWatchman, замаскированный под исполняемый файл «Документ из налоговой(запрос).exe». Отметим особенности этого фишингового письма. Оно отправлено с реального почтового адреса (ранее он был замечен как минимум в семи утечках) генерального директора строительной компании. Текст письма сформирован как ответ на другое письмо, ранее отправленное жертвой. Все это сделано с целью вызвать у получателя доверие. Использование пароля для архива оправдано тем, что документы якобы конфиденциальные. Наконец, несмотря на то что срочность письма не обозначена явно, подразумевается, что налоговая проверка якобы проходит прямо сейчас. Эти факторы многократно увеличивают шанс на открытие вредоносного вложения.

Рисунок 46. Фишинговое письмо от Hive0117, выявленное специалистами TI-департамента PT ESC



Обращаем ваше внимание, что подобные схемы мошенничества, как правило, приурочены к событиям в налоговом календаре. Особую бдительность стоит проявлять в периоды уплаты налогов. Важно помнить, что налоговые инспекторы не присылают на электронную почту требования об уплате налогов. Подобные уведомления рассылают либо через личный кабинет налогоплательщика, либо по обычной почте.

Кража учетных данных в мессенджерах: фальшивые голосования

Схемы с массовыми рассылками сообщений с просьбой проголосовать в конкурсе все еще продолжают «пользоваться успехом». Обычно целью таких рассылок является кража учетных данных или получение прямой финансовой прибыли. Так, например, армянская организация по кибербезопасности CyberHUB-AM недавно опубликовала исследование фишинговой кампании, проводившейся в 2023 и 2024 годах, которая была нацелена на пользователей Telegram в Армении и Узбекистане. Жертвам рассылались сообщения с ссылками на фейковую страницу с голосованием, где для авторизации пользователей просили ввести свой номер телефона и указать код безопасности для входа в Telegram-аккаунт. Отметим, что это не первое расследование подобной схемы компанией CyberHUB-AM. В июле прошлого года специалисты сообщали о фейковых голосованиях, призывы к которым рассылались с помощью рекламного бота Post Bot.

Российские пользователи популярных мессенджеров и соцсетей также регулярно подвергаются атакам через фейковые опросы и голосования. Весной и летом 2023 года пользователям Telegram и WhatsApp активно рассылались сообщения с просьбами принять участие в голосованиях

за победителей в различных детских конкурсах. Ссылки в этих сообщениях вели на фишинговые страницы с опросами, где требовалось ввести учетные данные. К концу лета 2023 года наши коллеги обнаружили более 2000 подобных фишинговых сайтов для угона аккаунтов. В начале декабря 2023 года коллеги наблюдали новую волну мошенничества с темой фейковых голосований, направленных на угон аккаунтов в популярных мессенджерах. На этот раз тематика детского творчества сменилась на темы, связанные с семьей и профессиональными навыками. В марте 2024 года была выявлена очередная волна угона аккаунтов через фишинг с опросами. На этот раз злоумышленники предлагали принять участие в голосовании за номинацию лучшего менеджера или специалиста по связям с общественностью. Чтобы проголосовать, жертвам предлагалось авторизоваться в Telegram через QR-код или цифровой код, отправленный на телефон. Далее происходил угон, и жертвы теряли доступ к аккаунту и ко всей информации из него. Как правило, во всех схемах после кражи аккаунта фишинговое сообщение отправлялось списку контактов, делая жертву новым распространителем мошеннических сообщений.

Легкие коины: атаки криптоскамеров

Киберпреступники наживаются на людях, желающих заработать на криптовалюте. В середине июня 2023 года компания Trend Micro поделилась результатами расследования крупного мошенничества, связанного с созданием фейковых криптовалютных площадок. Не менее пяти лет киберпреступная группа Impulse Team руководила мошеннической партнерской кампанией, направленной против жителей СНГ, интересующихся торгами на криптобиржах. За это время было создано множество площадок, куда через социальные сети заманивали жертв, предлагая им вознаграждения. За вывод призов пользователей просили внести определенную плату, которая шла в кошельки злоумышленников.

В апреле 2024 года наши коллеги рассказали еще об одной мошеннической схеме заработка на русскоязычных пользователях, желающих заполучить «легкие» деньги на схемах с криптовалютами. На этот раз злоумышленники предлагали заработать Toncoin. Пользователей убеждали зарегистрировать криптокошелек в неофициальном боте для хранения криптовалюты в Telegram, перевести на него деньги, а затем пригласить минимум пять друзей через реферальные ссылки, за что якобы полагалась комиссия. На деле комиссия не выплачивалась, и все вложенные пользователями деньги оказывались безвозвратно утеряны.

В мае 2024 года стала набирать популярность Telegram-игра Hamster Kombat. В ней пользователь выполняет роль директора криптовалютной биржи, зарабатывая игровую валюту многократными кликами на виртуального хомяка. Злоумышленники не упустили возможность нажиться на популярности игры. Пользователям, которые ищут способы вывести заработанные средства, стоит быть внимательными и осторожными. Новость о премаркет-торговле токенами Hamster Kombat была анонсирована в начале июля, однако криптоскамеры уже давно предлагают собственные приложения для снятия криптовалюты, к которым необходимо привязать TON-кошелек. Таким образом мошенники получают доступ к проведению любых операций с кошельком жертвы. Еще одна угроза состоит в краже Telegram-аккаунтов. Например, жертву вынуждают выполнить вход в аккаунт под предлогом авторизации для запуска бота. Другой сценарий — игрокам рассылаются сообщения с ссылками на фишинговые ресурсы, якобы позволяющие конвертировать игровую валюту в рубли. Для этого жертв просят авторизоваться в Telegram, после чего контроль над аккаунтом жертвы переходит в руки мошенников, которые могут использовать его в своих целях.

Мошенничество с использованием аудио и видеодипфейков

Специалистам по информационной безопасности давно знаком сценарий социальной инженерии, получивший название FakeBoss. Через фальшивые профили сотруднику пишет злоумышленник, представляясь руководителем компании, в которой работает жертва, и под различными предлогами пытается узнать информацию или убедить сотрудника провести финансовую операцию. Теперь, благодаря технологиям искусственного интеллекта, у киберпреступников появилась возможность модернизировать эту схему. В частности, мошенники вместо текстовых сообщений стали совершать звонки. Для имитации голоса руководителя во время звонка киберпреступники используют аудиодипфейки — голос, сгенерированный искусственным интеллектом. Например, в марте стало известно, что злоумышленники подделали голос гендиректора московского фитнес-клуба и убедили сотрудницу передать крупную сумму денег курьеру.

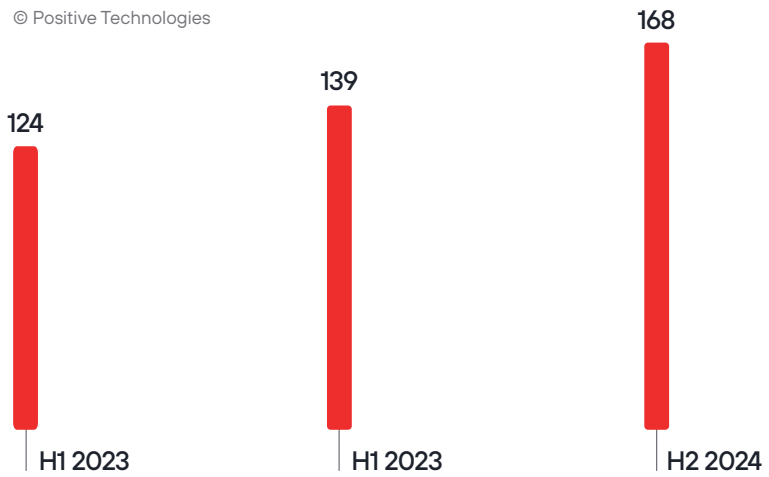
Подобные атаки могут совершаться не только на сотрудников организаций, но и на частных лиц. Так, в январе кибермошенники украли деньги у жительницы Москвы, подделав голос родственника жертвы в сообщении из мессенджера Telegram. В Казахстане пожилая женщина тоже чуть было не лишилась крупной суммы денег. Ей по видеосвязи позвонил человек в форме, представившись сотрудником правоохранительных органов. Образ полицейского был создан с помощью нейросети. Мошенник пытался убедить женщину перевести деньги на счет злоумышленников, однако инцидент удалось предотвратить благодаря бдительности сотрудников банка. В Узбекистане мошенники создали видеодипфейк с участием гендиректора горно-металлургического комбината и от его имени предлагали гражданам вступить в группу в Telegram, посвященную инвестиционной программе, с помощью которой якобы можно за короткий срок получить крупную прибыль.

Это были всего лишь несколько примеров атак с применением искусственного интеллекта. Последствия могут быть гораздо серьезнее, чем в описанных примерах. К примеру, эксперты считают, что в 2024 году дипфейки в сочетании с социальной инженерией могут помешать проведению выборов во всем мире. В некоторых странах СНГ из-за участившихся киберпреступлений, например в России и Узбекистане, уже рассматриваются законопроекты, предусматривающие уголовную ответственность за создание и использование дипфейков.

Анализ теневых площадок

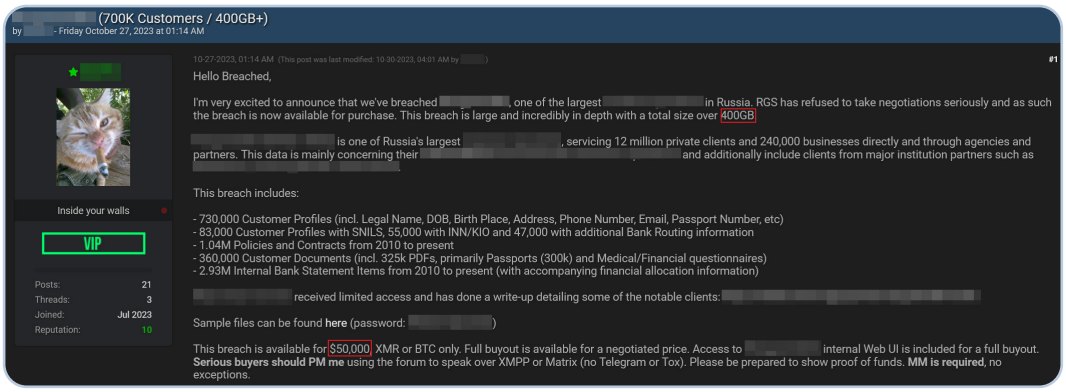
На теневых площадках злоумышленники ведут торговлю и обмен украденными данными, фальшивыми документами, доступами в сети скомпрометированных организаций, инструментами и услугами для проведения атак. Мы проанализировали 431 уникальное объявление на различных теневых форумах и Telegram-каналах, в которых упоминались страны СНГ на протяжении 2023-го и первой половины 2024 года. Объем публикаций растет: в первом полугодии 2024 года было опубликовано на 35% больше объявлений, чем за аналогичный период в 2023 году.

Рисунок 47. Распределение объявлений по полугодиям



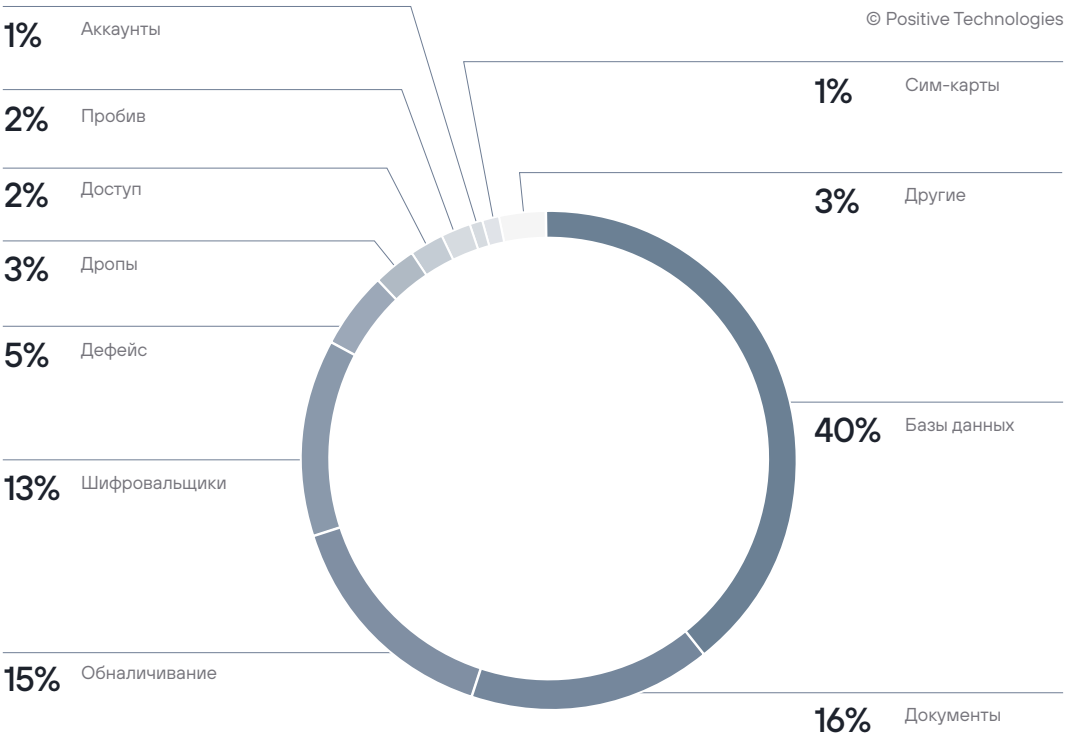
Большая часть сообщений связана с базами данных (40%), при этом только в 20% из них базы данных продаются, а в 79% раздаются бесплатно. Часть таких объявлений относится к публикациям хактивистов, которые «сливают» данные в дарквеб, руководствуясь политическими мотивами, без преследования финансовой выгоды. Другая часть — это базы данных, которые были похищены финансово мотивированными злоумышленниками, однако компании-жертвы отказались платить выкуп, и теперь их данные выложены в дарквебе бесплатно.

Рисунок 48. Объявление о продаже базы данных российской компании за 50 тысяч долларов США



На втором и третьем месте стоят объявления, связанные с фальшивыми либо украденными документами (16%) и обналичиванием денег (15%). Часть публикаций не связана с покупкой или продажей, а представляет собой новости о заражении шифровальщиками (13%) либо о дефейсах сайтов (5%). Небольшое количество объявлений связано с поиском дропов и дроповодов (3%), продажей доступов в скомпрометированные компании (2%) и услугами по пробиву информации о человеке (2%). Несколько объявлений были связаны с продажей либо покупкой аккаунтов в различных сервисах (1%) и продажей «серых» сим-карт — зарегистрированных на посторонних людей сим-карт, с помощью которых злоумышленники совершают мошеннические операции.

Рисунок 49. Распределение объявлений по темам



Каждое пятое объявление (21%), связанное с базами данных, относится к сфере ритейла, в основном это раздачи и продажи баз данных интернет-магазинов. На втором месте — IT-компании. Как показали результаты нашего исследования, связанного с утечками конфиденциальных данных, одним из факторов, влияющих на высокую долю утечек информации из IT-компаний, является множественное заражение вредоносным ПО открытых репозиториев, которые активно используются разработчиками.

Рисунок 50. Категории жертв, базы данных которых продаются или раздаются бесплатно на теневых площадках

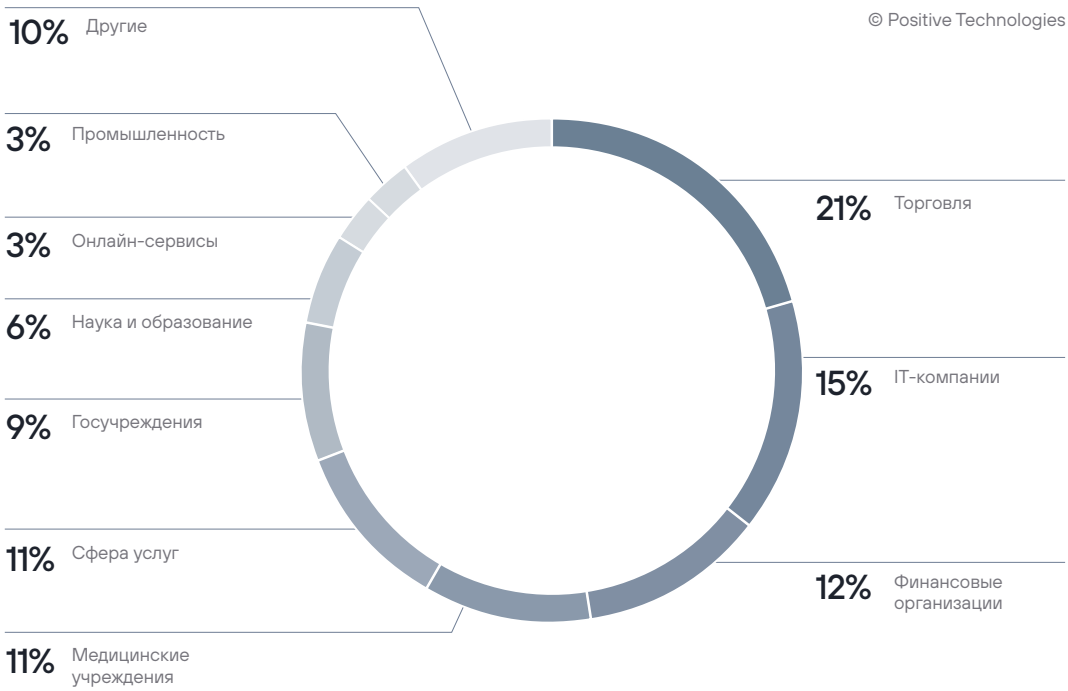
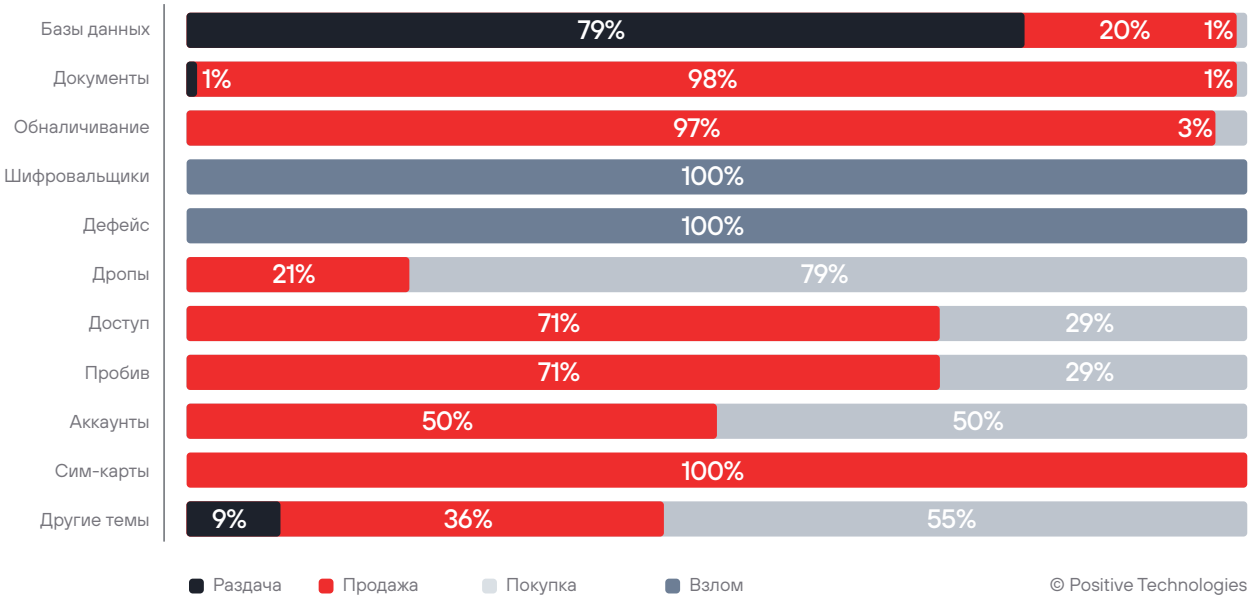


Рисунок 51. Распределение объявлений по типам



Цены на базы данных, которые находятся в продаже, сильно варьируются, начиная от 100 долларов и заканчивая 50 тысячами долларов США. Медианная цена на базы данных российских компаний в дарквебе составляет 900 долларов США. Важно отметить, что в 80% объявлений, связанных

с продажей, цена не указана и является договорной, поэтому объективно оценить стоимость каждого вида информации или услуг, выставленных на продажу, не представляется возможным.

Рисунок 52. Цены на некоторые виды информации, которая продается на теневых площадках



Некоторые объявления касаются двух и более стран СНГ. Например, в одном объявлении могут продаваться доступы к нескольким организациям из разных государств. Большая часть объявлений касалась России (85%), Беларуси (29%) и Казахстана (28%). Напомним, что именно на эти три государства совершается наибольшее число атак.

В половине (46%) объявлений, связанных с Россией, продаются или раздаются бесплатно базы данных. Для Беларуси и Казахстана наиболее актуальны объявления, связанные с обналичиванием денег и фальшивыми документами.

Рисунок 53. Распределение объявлений по странам

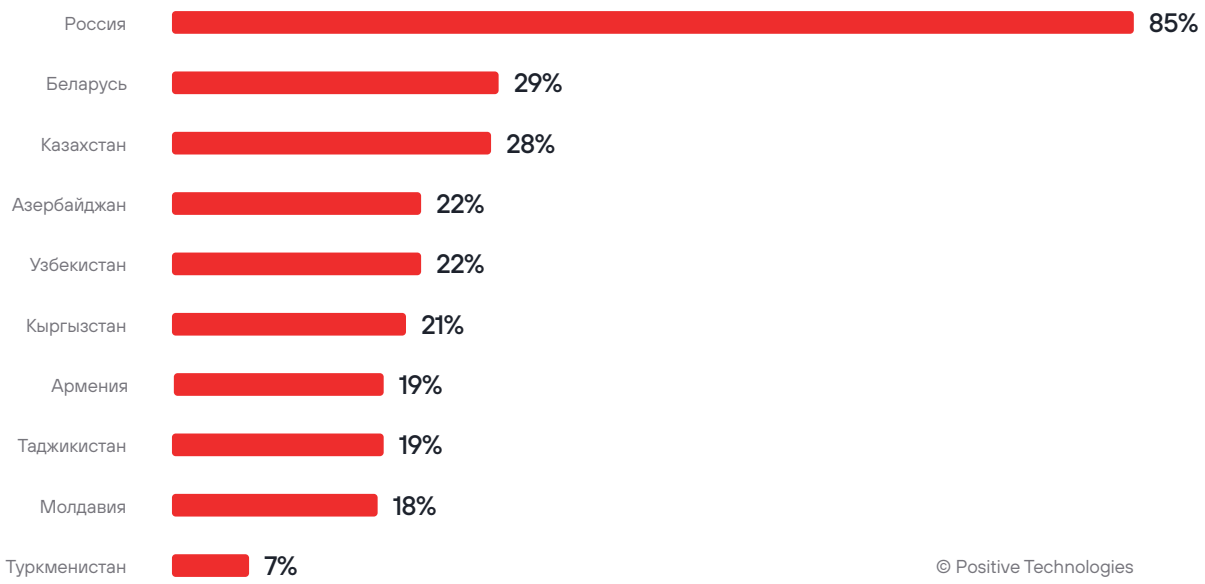
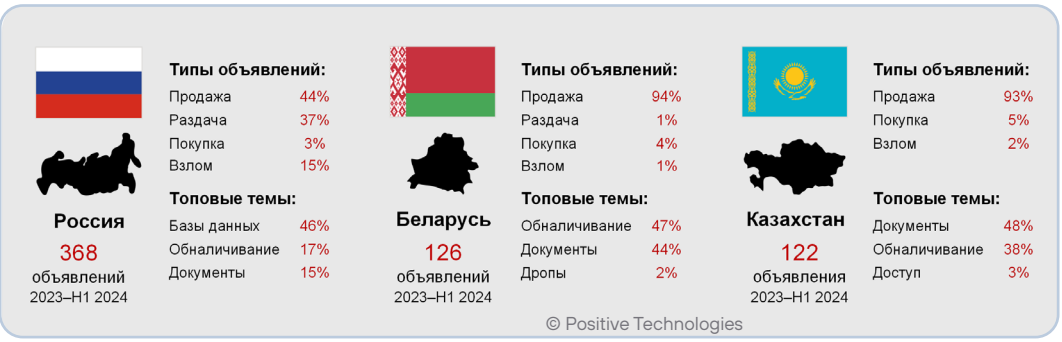


Рисунок 54. Статистика по объявлениям в дарквебе, связанным с Россией, Беларусью и Казахстаном



Выводы и рекомендации

Последние несколько лет на международном и региональном уровнях в странах СНГ происходят преобразования геополитического плана. Несмотря на это, цифровая трансформация региона набирает обороты. Это неминуемо привлекает внимание киберпреступников. Количество атак на страны СНГ увеличивается с каждым кварталом, поэтому государствам и организациям необходимо усиливать свою защиту.

Рекомендации для государств

Развитие нормативно-правовой базы на государственном, региональном и международном уровнях

На сегодняшний день все страны СНГ приняли и реализуют собственные государственные стратегии и концептуальные документы, направленные на развитие цифрового общества, перевод госуправления и финансово-экономического сектора в электронный формат. Однако нормативно-правовая база, направленная на защиту от кибератак, в некоторых странах СНГ все еще остается неполной. Следует предпринимать шаги, направленные на решение этой проблемы. Так, в апреле 2023 года Межпарламентская Ассамблея государств — участников СНГ приняла модельный закон «О противодействии киберпреступности», который является основой совершенствования государственных законодательств стран — участников СНГ в области противодействия киберпреступности. Важно обеспечить имплементацию этого закона в государственные законодательства государств СНГ. Это позволит скоординировать деятельность госорганов и повысит раскрываемость киберпреступлений.

Сотрудничество государства и бизнеса

Для достижения успеха при реализации проектов в области кибербезопасности необходимо выстроить прочные партнерские отношения между госорганами и коммерческими организациями.

Пример такого партнерства — создание центров по реагированию на киберинциденты (CERT/CSIRT/CIRT). Благодаря им, госучреждения и бизнес имеют возможность объединить усилия для урегулирования инцидентов, связанных с кибербезопасностью. В большинстве стран СНГ уже созданы подобные центры. Однако их необходимо развивать, а также создавать новые, в том числе отраслевые центры. Это эффективное решение для координации действий, направленных на сбор и обработку информации, касающейся кибербезопасности, а также на принятие мер реагирования на киберинциденты.

Международное сотрудничество

Государствам СНГ необходимо активно включаться в международное сотрудничество по линии кибербезопасности. Это позволит эффективно внедрять передовые практики, сокращать «цифровой разрыв» внутри региона и улучшать позиции отстающих государств. Необходим обмен опытом реагирования на киберпреступления. Для этого хорошо подходит формат региональных киберучений. Они должны быть регулярными и открытыми для государственных центров по реагированию на инциденты, регуляторных органов, операторов связи и других заинтересованных организаций из различных стран СНГ.

Защита критической информационной инфраструктуры

В условиях сложной геополитической обстановки государства должны особенно бдительно защищать критическую информационную инфраструктуру, атаки на которую могут привести к недопустимым событиям на уровне отраслей и страны. В первую очередь важно обезопасить инфраструктуру государственных учреждений, телекоммуникаций и промышленности. При этом необходимо учитывать скорость цифровой трансформации в стране и уровень зрелости ИБ.

Безопасность критической информационной инфраструктуры требует сотрудничества специалистов в области ИБ, государственных органов и частных компаний. Следует обеспечить защиту сетей электросвязи, центров обработки данных, точек доступа к интернету, диверсифицировать поставщиков ключевой технологической инфраструктуры и по возможности поощрять развитие государственных предприятий, осуществляющих деятельность, связанную с обеспечением кибербезопасности.

Развитие специалистов в области кибербезопасности

Развитие человеческого капитала и подготовка нового конкурентоспособного поколения IT-специалистов в области кибербезопасности будет способствовать дальнейшему успеху цифровой трансформации. Однако страны СНГ не обошла общемировая проблема — нехватка квалифицированных специалистов в области кибербезопасности. Аналитики прогнозируют, что к 2025 году дефицит специалистов в области ИБ достигнет 3,5 миллионов открытых вакансий.

Необходимо инвестировать средства в подготовку кадров и образование в области кибербезопасности. Многие государства СНГ уже предпринимают меры по взращиванию собственных

высококвалифицированных специалистов. К примеру, в марте 2023 года в Азербайджане начал работу Центр кибербезопасности, созданный совместно с израильским технологическим вузом, целью которого стала подготовка специалистов и инструкторов в области кибербезопасности. Странам с более низким уровнем развития образования в сфере кибербезопасности стоит перенимать положительный опыт у своих соседей.

Рекомендации для бизнеса

Сегодня большинство компаний в странах СНГ укрепляют IT-инфраструктуру выборочно. К примеру, результаты нашего исследования показали, что 80% российских организаций не занимаются полноценным укреплением IT-инфраструктуры. Для исправления сложившейся ситуации и повышения устойчивости бизнеса к кибератакам необходимо придерживаться методологии результативной кибербезопасности. На пути к ней каждая компания проходит три основных этапа.

Этап 1. Формирование перечня недопустимых событий

Для обеспечения киберзащиты компаниям необходимо провести анализ основных рисков и сформировать список недопустимых событий, которые могут нанести существенный ущерб компании, сценарии их реализации и перечень целевых систем. Этот позволит сконцентрировать усилия на защите наиболее ценных ресурсов. Следует разработать стратегию предотвращения недопустимых событий, включая необходимые меры безопасности и мониторинг сетевой активности с использованием современных средств защиты.

Этап 2. Кибертрансформация и построение результативной безопасности

Для обеспечения киберустойчивости компании необходимо подготовить IT-инфраструктуру, создать центр мониторинга и противодействия киберугрозам, а также обучить сотрудников практическим аспектам кибербезопасности.

Для мониторинга и своевременного реагирования на угрозы рекомендуется использовать SIEM-системы, которые в реальном времени собирают и анализируют информацию о событиях безопасности из различных источников. Если использовать SIEM совместно с NTA-решениями, предназначенными для анализа сетевого трафика, а также с решениями класса EDR для выявления сложных целенаправленных атак, можно повысить эффективность защиты, обнаруживать атаки на ранних стадиях и обеспечивать быструю реакцию на угрозы, снижая риски для организации. Для выявления атак в промышленной инфраструктуре SIEM могут дополняться специализированными продуктами для анализа трафика систем АСУ ТП.

Для получения практического подтверждения текущего уровня киберустойчивости необходимо регулярно проводить оценку защищенности инфраструктуры. Существует несколько способов оценки защищенности. Выбор того или иного способа будет зависеть от цели, этапа жизненного цикла объекта и уровня зрелости информационной безопасности в организации.

Этап 3. Подтверждение высокого уровня киберустойчивости

Следует поддерживать перечень недопустимых событий в актуальном состоянии и регулярно проводить практическую проверку работоспособности мер и средств защиты. Рекомендуется принимать участие в программах bug bounty, которые позволяют привлечь внешних исследователей безопасности для поиска новых уязвимостей. Это поможет обнаружить и устранить уязвимости до того, как они будут использованы злоумышленниками.

ptsecurity.com
pr@ptsecurity.com

Positive Technologies — лидер в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 4000 организаций по всему миру.

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.

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.