СПОСОБЫ ПРОНИКНОВЕНИЯ В СЕТЬ КОМПАНИИ

Денис Батранков, Positive Technologies

Positive Technologies: максимальное число векторов проникновения в ЛВС в 2021 – 19
В среднем на проникновение во внутреннюю сеть компании уходит два дня.

Источник: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf

Проникнуть в инфраструктуру большинства компаний может даже низкоквалифицированный хакер

Среднее время проникновения в сеть (результаты пентестов)

2 дня

Минимальное время

30 минут

Среднее время до обнаружения (результаты расследований)

200 дней

2000–2022

Максимальное время

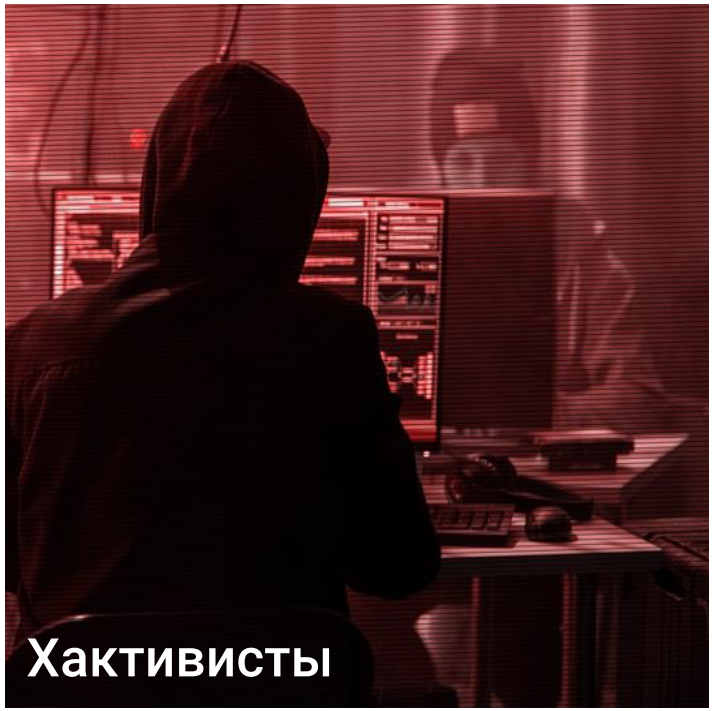
11 лет

Источник: ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf

Каналы проникновения в организацию

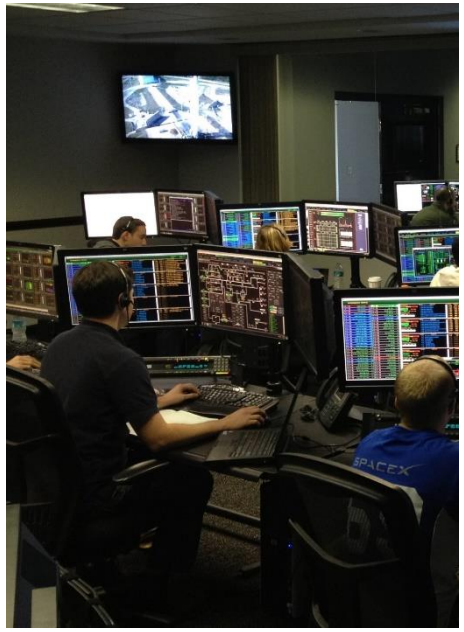
Электронная почта	Веб-сервер	Уязвимости	Соседний офис	Облачный файлообменник
Облачные ресурсы	USB флешки	Wi-Fi сеть	Взломанный софт	Мобильные устройства и удаленные рабочие места
Встроенные в сети вебкамеры и IoT	Контейнеризация и вредоносные контейнеры	Подрядчики	Watering Hole	Атаки на DNS

Портрет злоумышленников

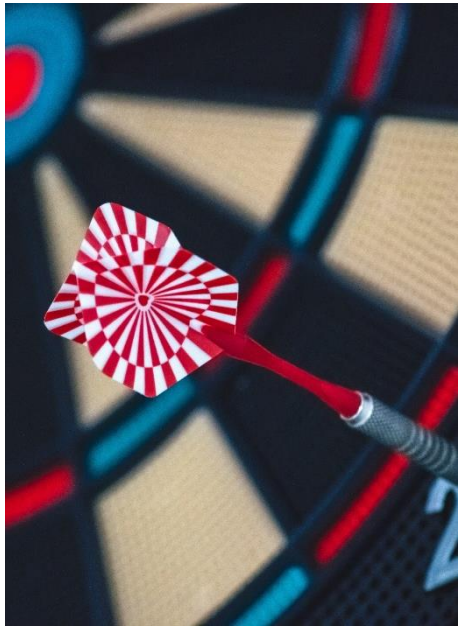


... или просто захватить сеть.
Любую.

Чем опасны таргетированные атаки?

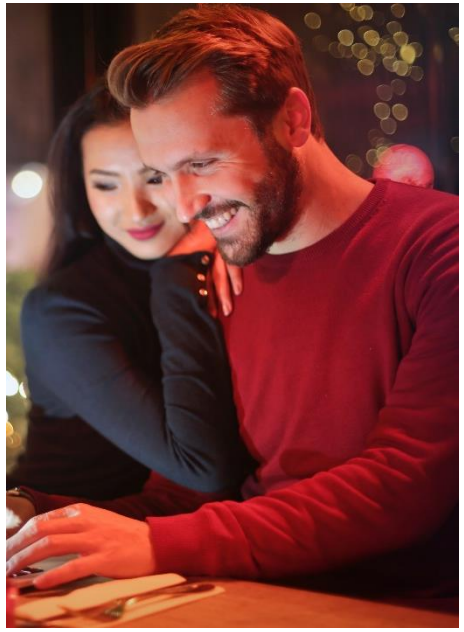


Таргетированные атаки обычно хорошо спланированы и включают **несколько этапов**

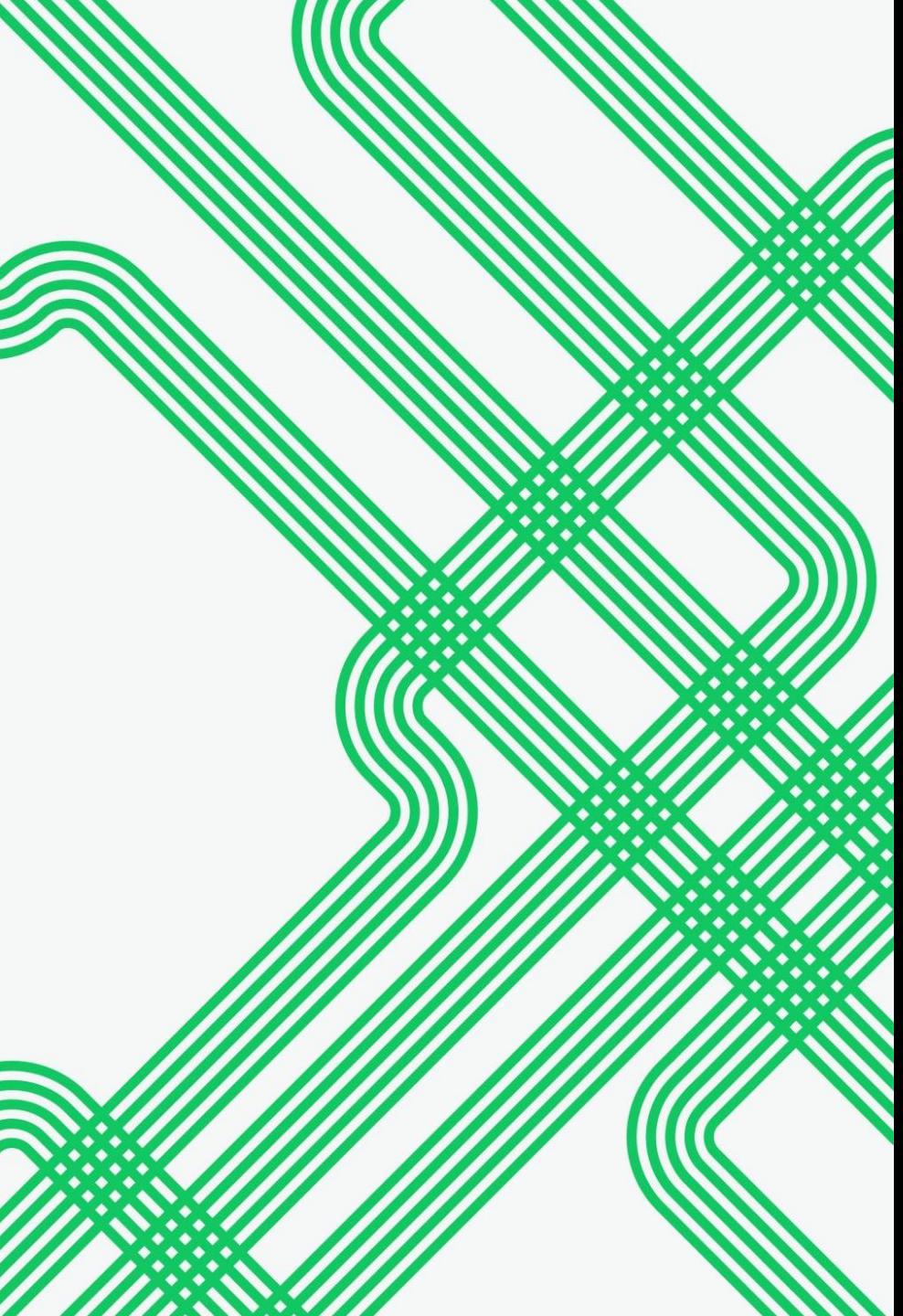


- Разведка
- Внедрение
- Уничтожение следов присутствия

Злоумышленники закрепляются в инфраструктуре жертвы и остаются незамеченными в течение **месяцев или даже лет**



На протяжении **всего этого времени** они имеют доступ ко всей **корпоративной информации**



ПОДБОР УЧЕТНЫХ ДАННЫХ

Чаще всего злоумышленники просто подбирают пароль!

Подбор учетных данных остается основным способом проникновения во внутреннюю сеть: для проектов пентеста второй половины 2020 — первой половины 2021 года использовать эти уязвимости удалось в 71% проектов.

Успешные атаки внутри сети также не обходятся без подбора учетных записей: этот метод использовался в 93% успешных атак.

ДОСТУПНЫЕ СНАРУЖИ СЕРВИСЫ

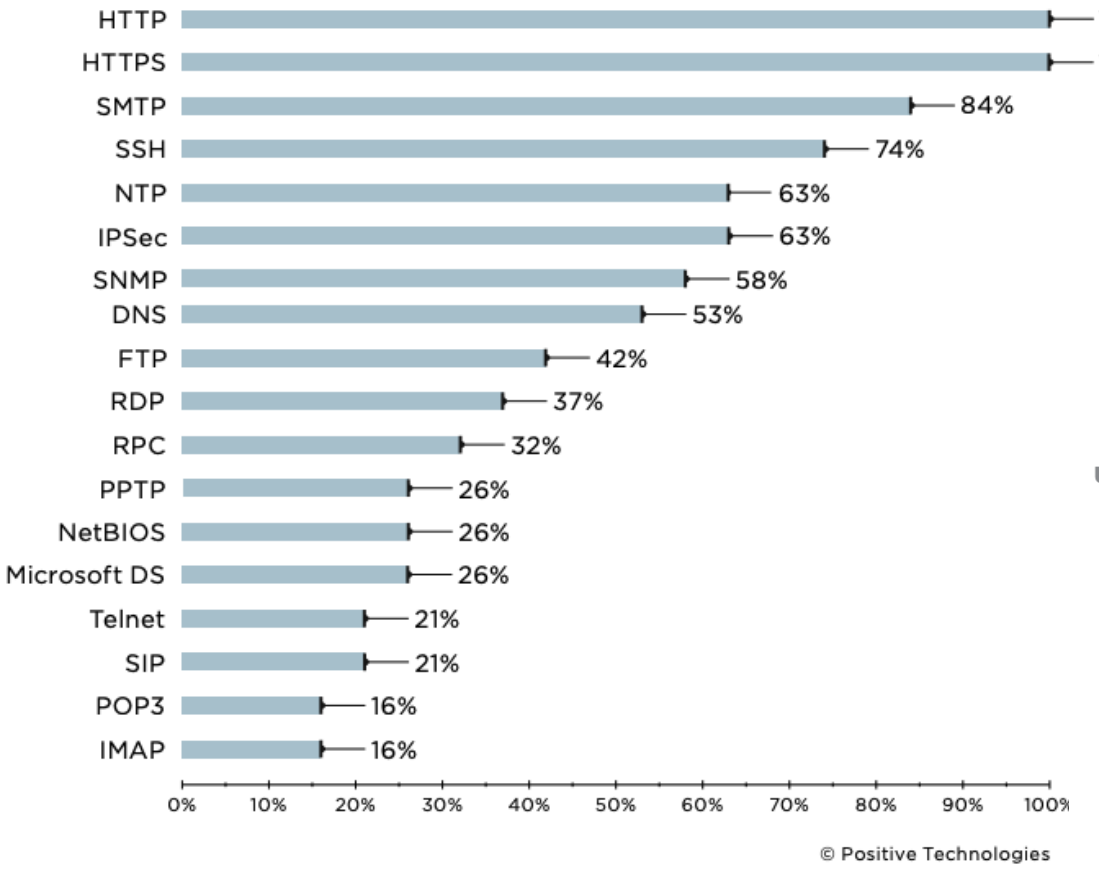


Рисунок 5. Службы, доступные на сетевом периметре (доля организаций)

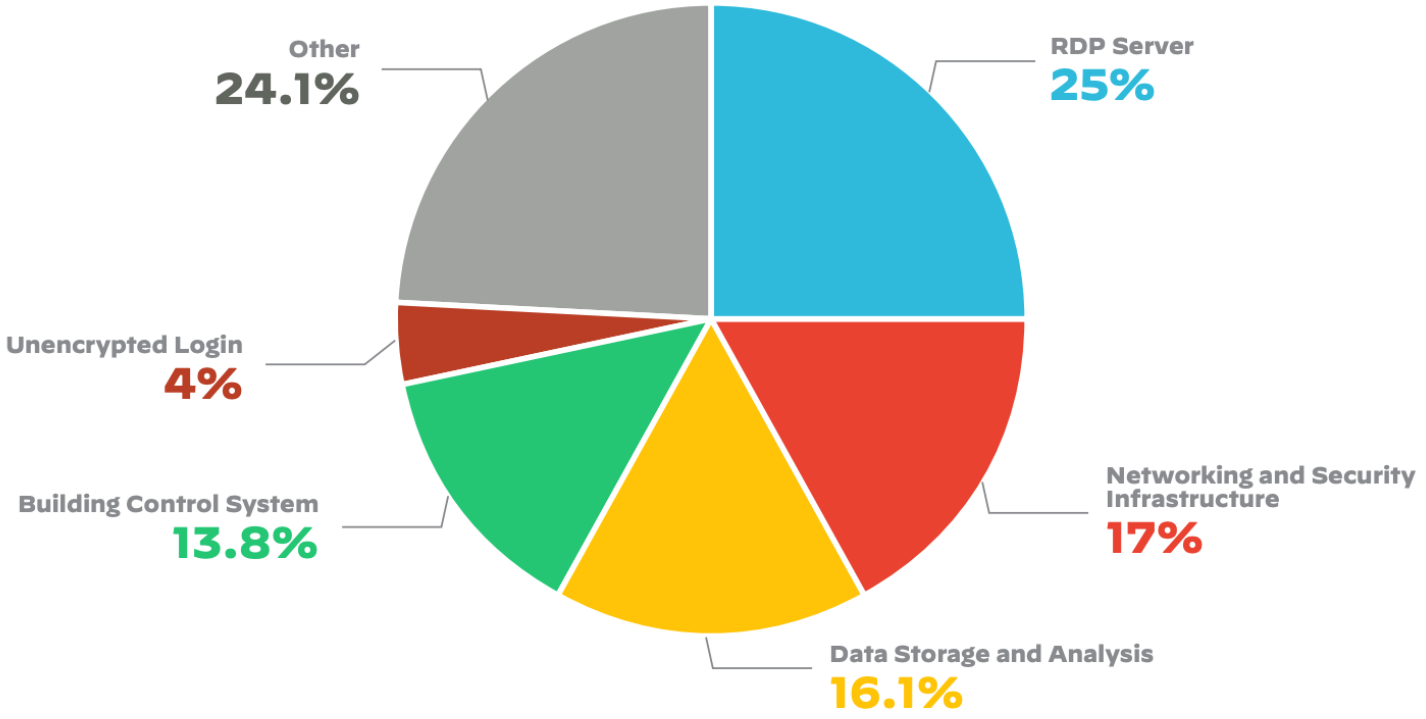
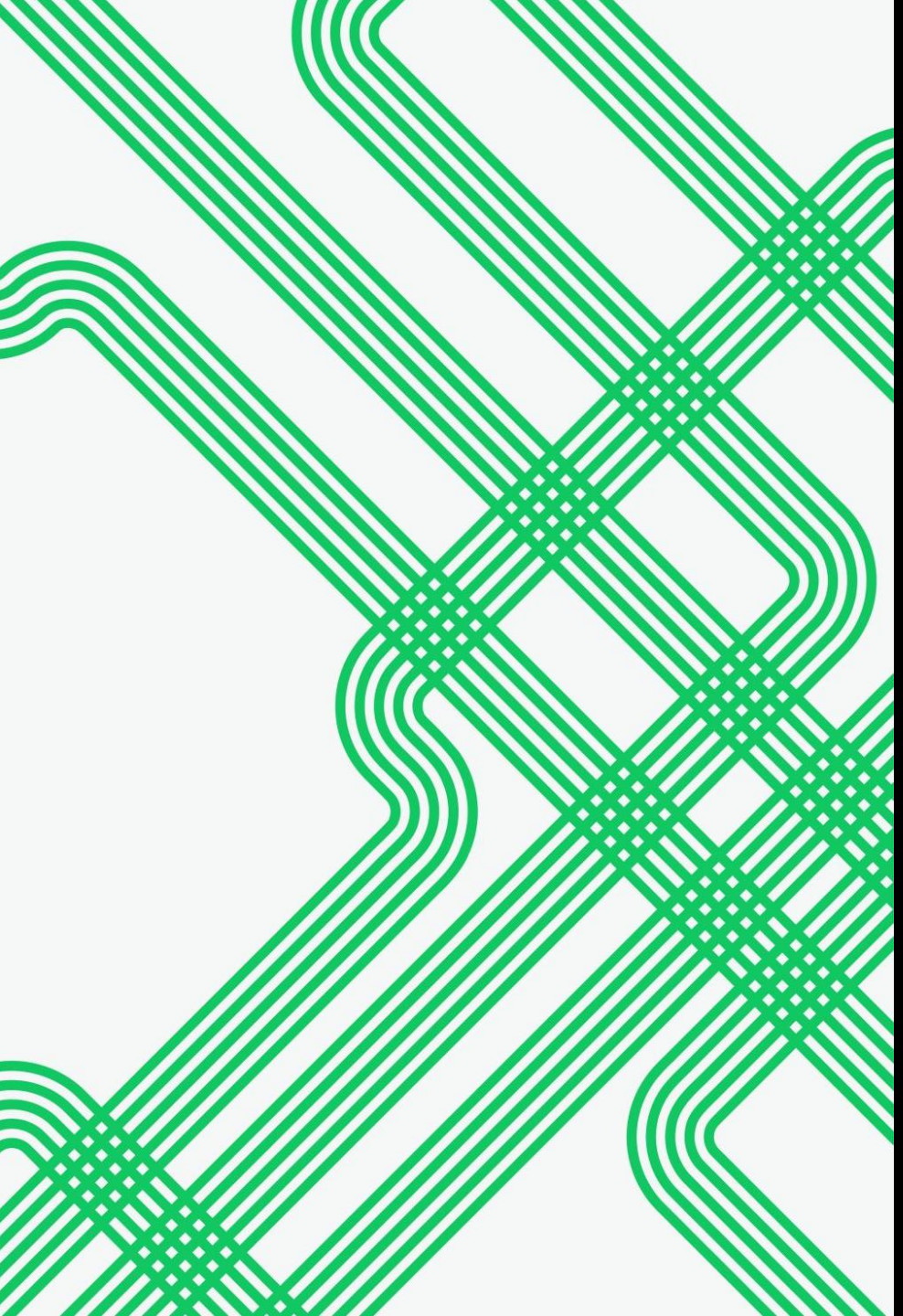


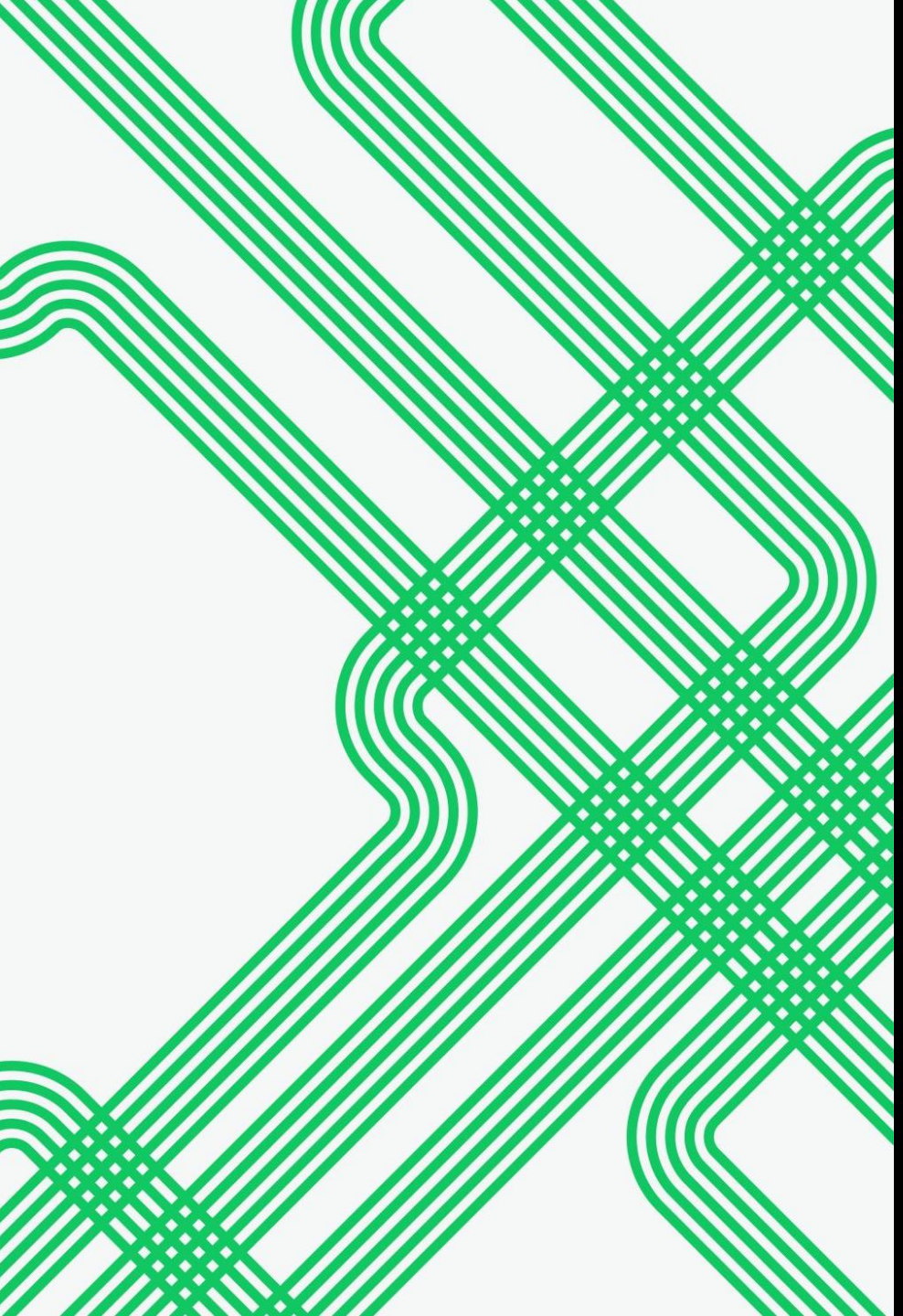
Figure 3: Distribution of risks across the global attack surface



ВЕБ ПРИЛОЖЕНИЯ

Практически в каждой компании существует способ проникнуть в локальную сеть именно через веб-приложения.

В 2020 году: во время удаленной работы многие организации массово выводили веб-сервисы на внешний периметр, что позволяло найти дополнительные возможности для проникновения во внутреннюю структуру



УЯЗВИМОСТИ

Компании работают на устаревшем оборудовании и программном обеспечении, в котором есть уязвимости, через которые проникает хакер!

В 60% проектов пентеста именно эксплуатация известных уязвимостей в ПО была использована для проникновения во внутреннюю сеть.

В среднем каждый день обнаруживается более 50 уязвимостей. В 2021 году найдено 20000 уязвимостей.

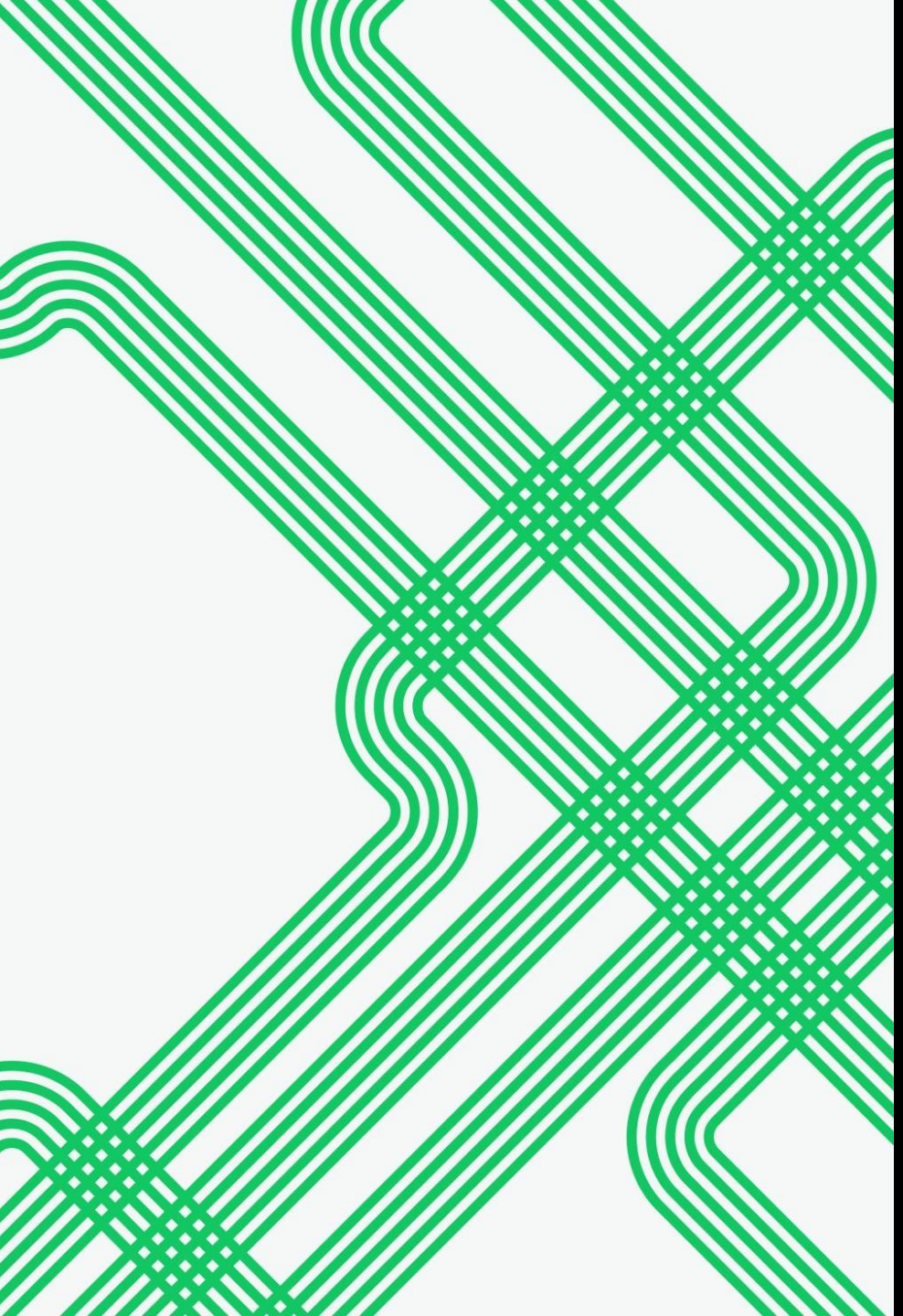
Уязвимости ProxyLogon, Accellion FTA, Zerologon, Log4Shell были сразу использованы!

Обновляйтесь, люди!

ПРИМЕРЫ

Как проникли пентестеры Positive Technologies в сети в 2021 году

- «Удаленное выполнение произвольного кода» (CVE2020-0688) в доступном из интернета сервере Microsoft Exchange;
- «Чтение произвольных файлов» (CVE-2020-3452) и «Разглашение информации» (CVE-2020-3259) в веб-интерфейсе управления устройствами Cisco ASA;
- «Удаленное выполнение произвольного кода» (CVE-2020- 1147) в Microsoft SharePoint;
- «Удаленное выполнение команд ОС» (CVE-2019-19781) в программном обеспечении Citrix NetScaler;
- «Удаленное выполнение произвольного кода» (CVE-2015- 8562) в CMS Joomla.



ФИШИНГ

Результаты проектов по осведомленности сотрудников, проводимые специалистами Positive Technologies, показывают низкий уровень готовности персонала к фишинговым атакам.

В 2017 году по ссылке в фишинговом письме перешли 26% сотрудников, 16% запустили вложенный файл, а учетные данные были введены в поддельные формы аутентификации в 11% случаев.

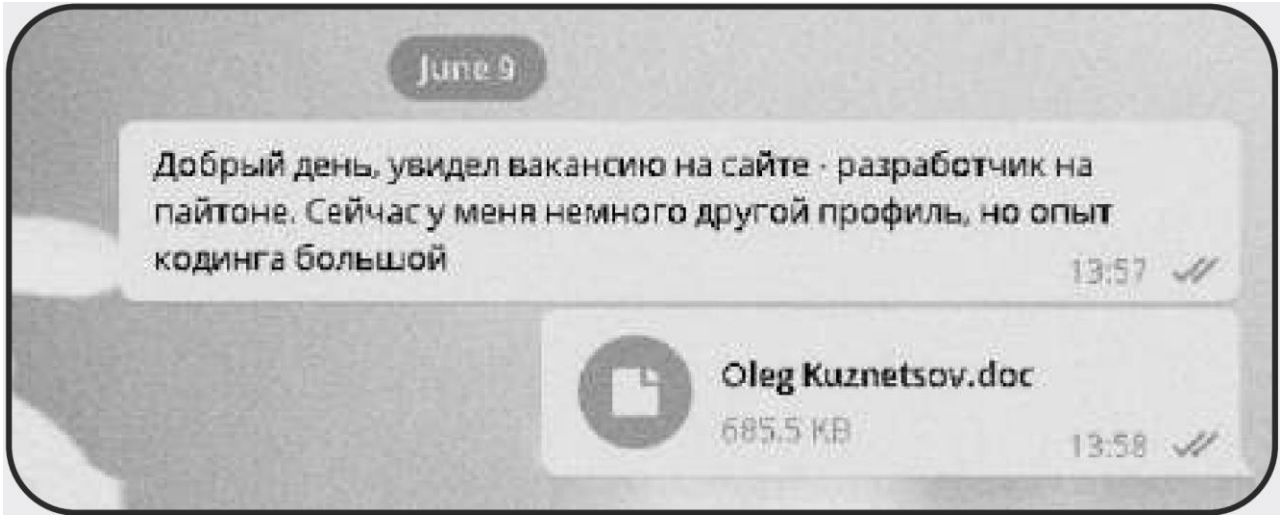
К текущему моменту улучшений не видно: по ссылкам в фишинговых письмах переходят 38% сотрудников, учетные данные вводят 31%, а вредоносное вложение может быть запущено в 39% случаев.

АТАКА НА ПОЗИТИВ

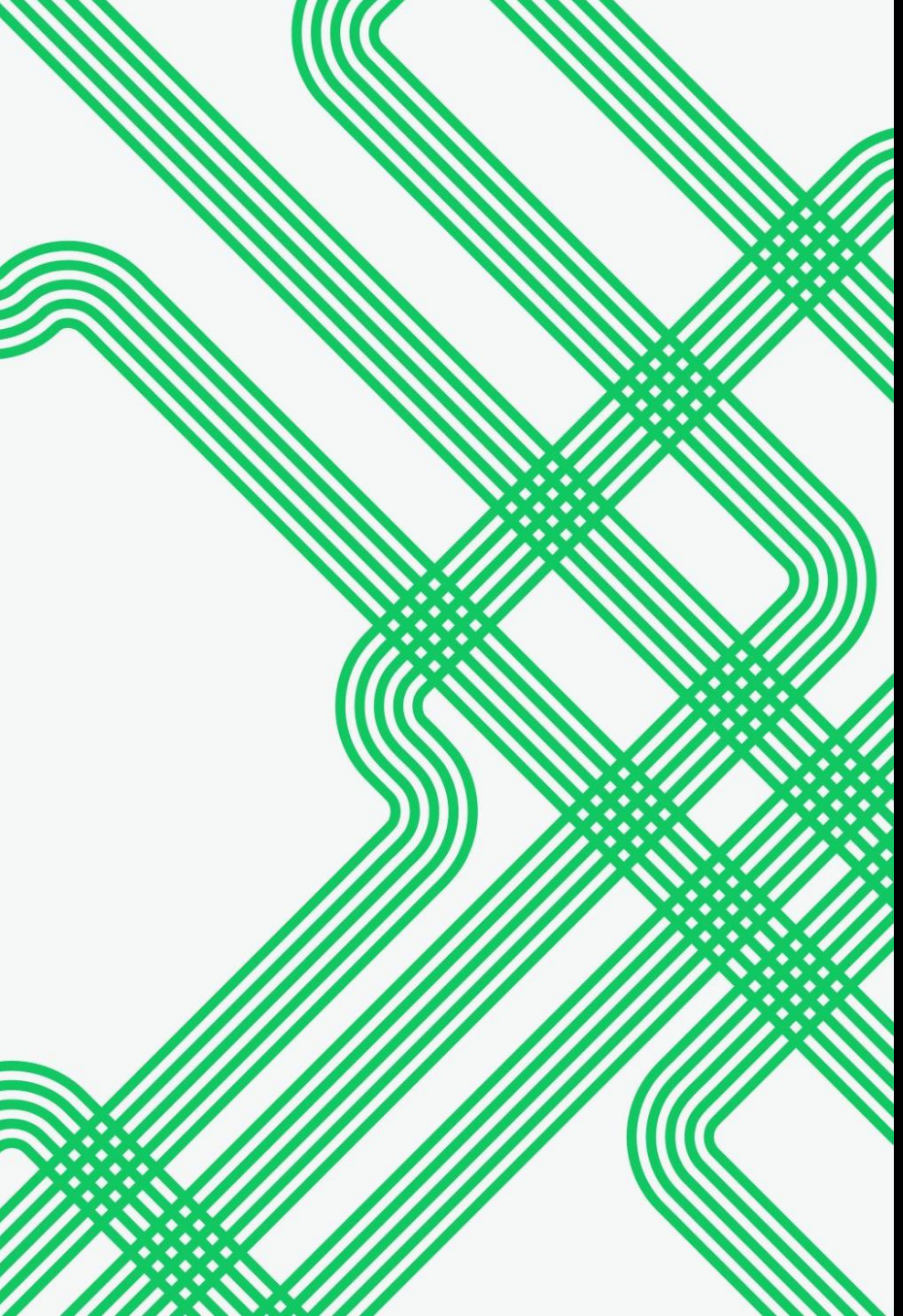
1. Для фишинговых атак нападающие чаще всего выбирали наших HR-специалистов, сотрудников, которые регулярно дают комментарии и интервью СМИ, и тех, кто указывал свое место работы на страницах в соцсетях. Любопытно, что атакующие писали им не только на рабочие электронные адреса в надежде, что кто-то по невнимательности оставит свои учетные данные на фишинговом сайте или откроет вредоносное вложение, но и в мессенджеры

2. Летом 2021 года на удочку классического фишинга пытались поймать команду пиарщиков Positive Technologies, но файл с вредоносным вложением в телеграмме был проанализирован в PT Expert Security Center и найден вредоносный код, который предоставлял доступ к управлению зараженными компьютерами.

Пример фишинговой атаки на HR-специалиста



Источник: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf



КРАЖА УЧЕТНЫХ ДАННЫХ

Учетные данные водят в поддельные формы аутентификации

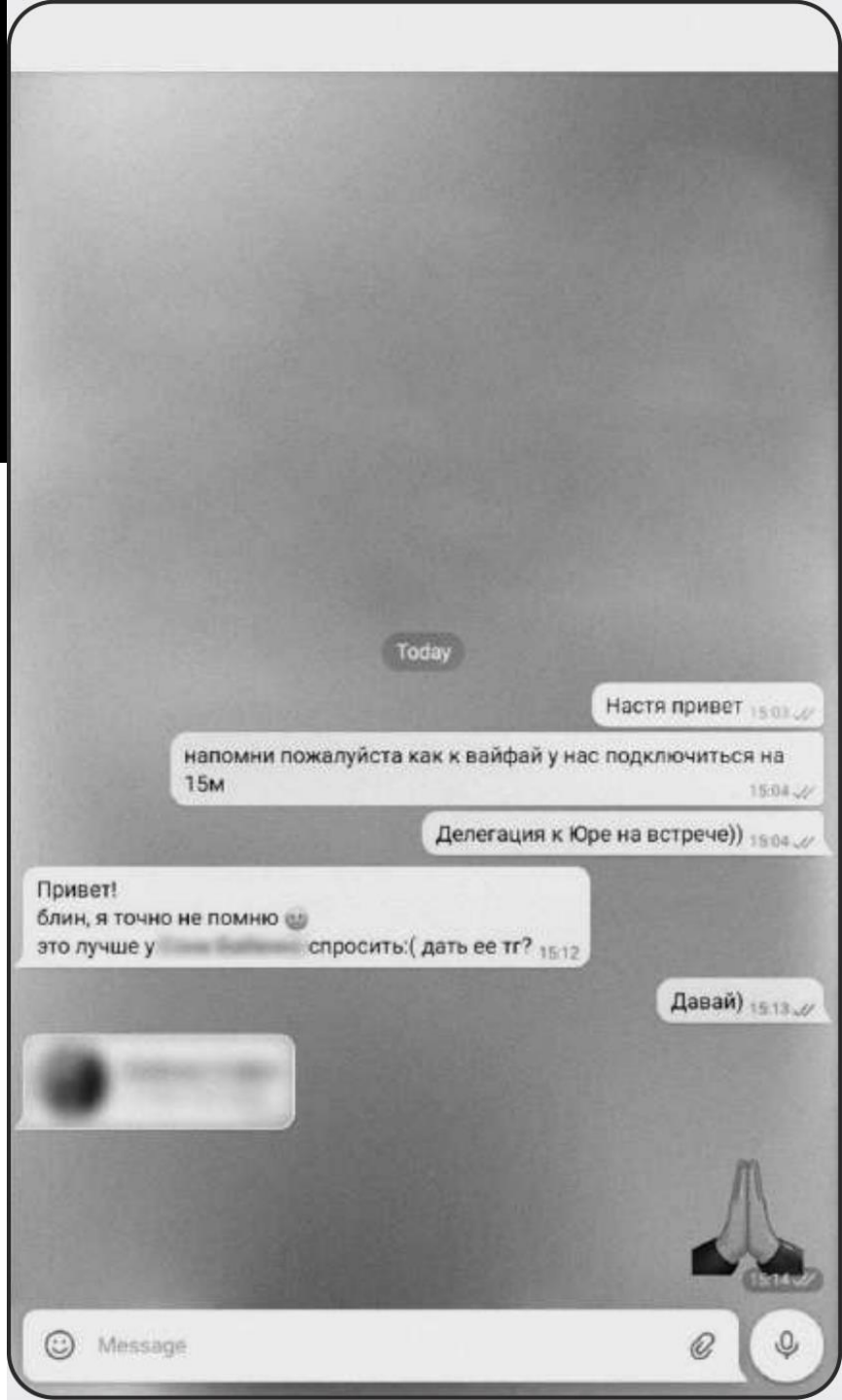
Учетные данные используют одинаковые на всех сервисах, даже администраторы сети. Кража доступа к одному серверу приводит к доступу ко всем остальным – логин и пароль одинаковый

Остаются пароли по-умолчанию на сетевых устройствах

АТАКА НА ПОЗИТИВ

1. Создали поддельный аккаунт в Telegram
на реального сотрудника компании. Узнали пароль через соц. инженерию

2. Находясь в корпоративной Wi-Fi-подсети, изолированной от внутренней IT-инфраструктуры, получили возможность атаковать все подключенные к ней устройства, в том числе ноутбуки сотрудников.

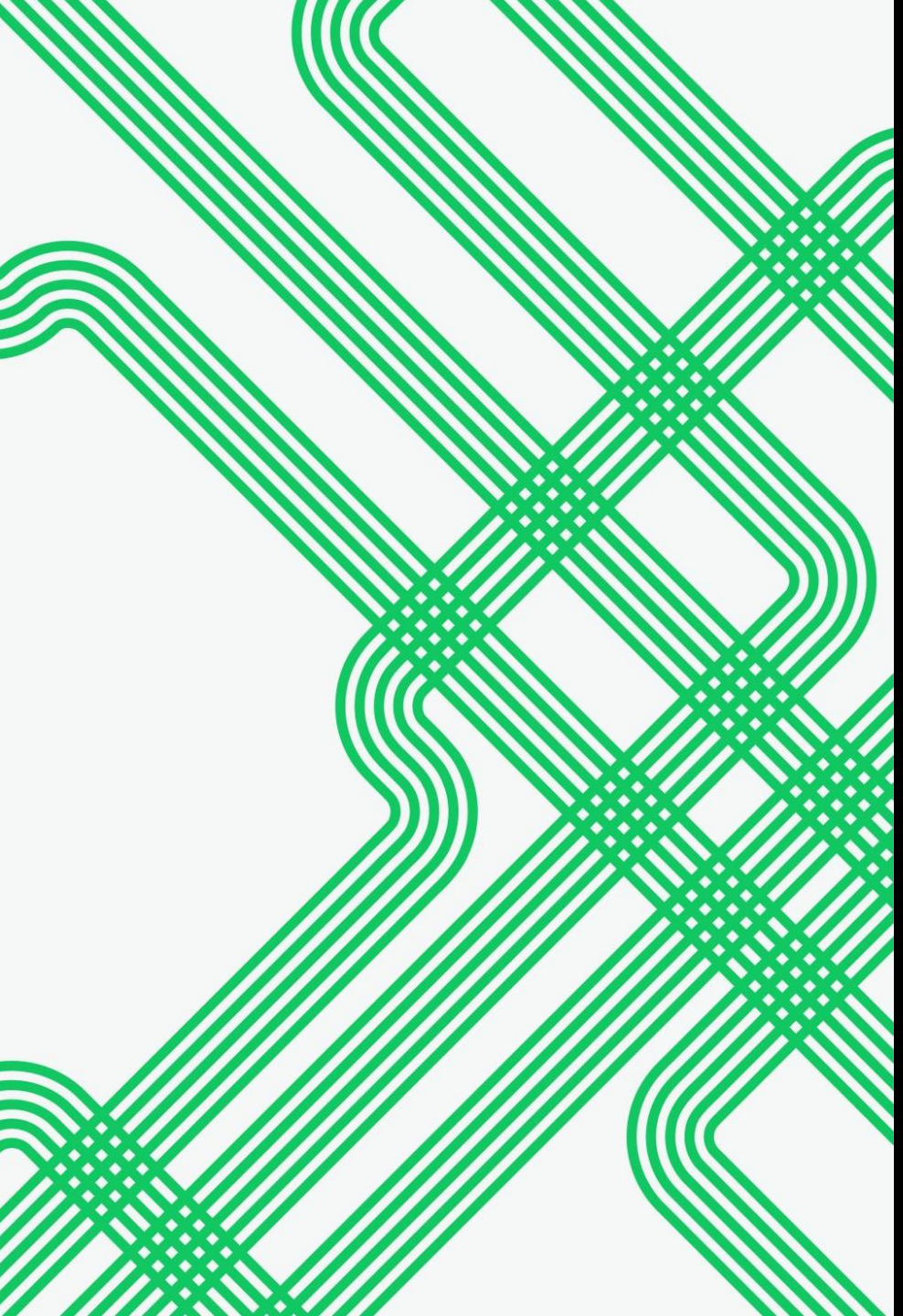


Источник: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf

АТАКА WATERING HOLE

Злоумышленники размещают вредоносное программное обеспечение на сайтах, которые посещает потенциальная жертва, и ожидают, когда жертва придет и сама скачает вредоносный код на свой компьютер.

Watering hole (водопой) взято из мира дикой природы: хищники нередко ждут свою добычу у рек и озер, куда животные приходят за водой.



ПОВЫШЕНИЕ ПРИВИЛЕГИЙ

В 100% компаний внутренний злоумышленник может получить полный контроль над инфраструктурой.

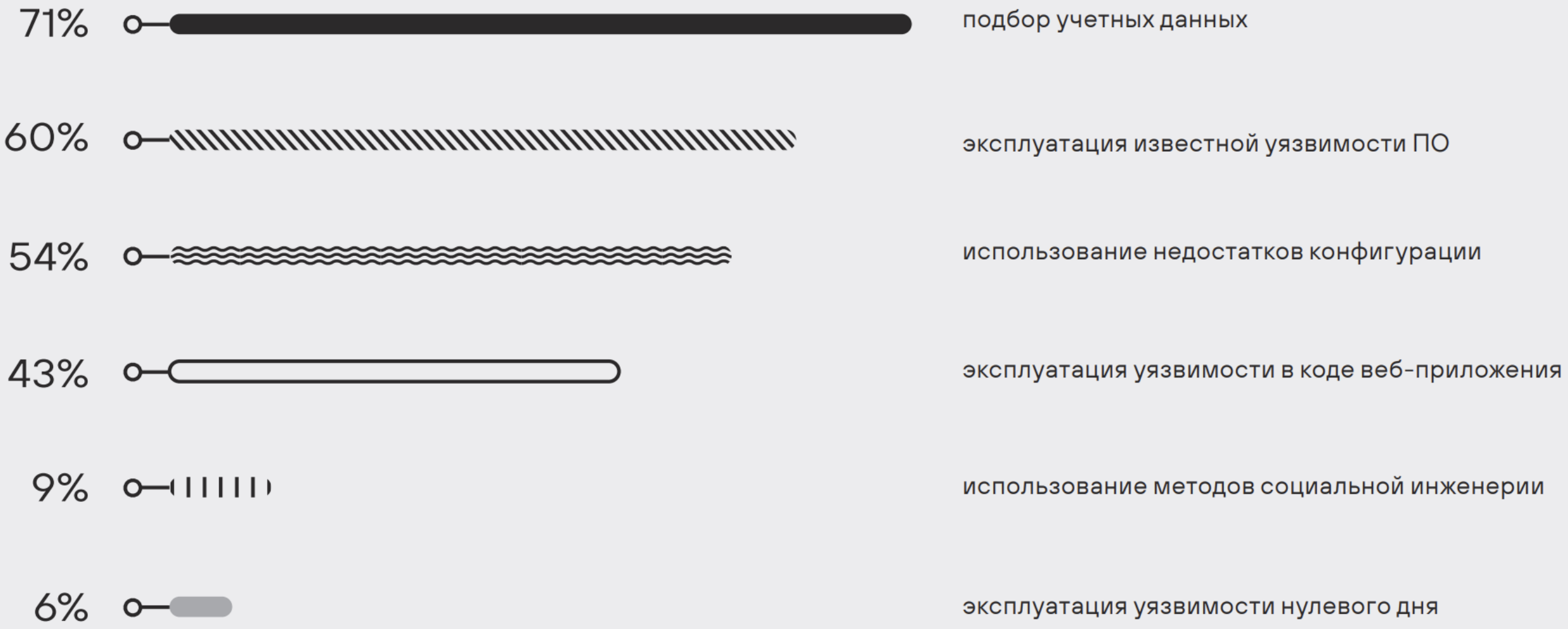
В 81% компаний существует простой способ получить привилегии администратора домена, который под силу даже низкоквалифицированному хакеру.

ПРИМЕРЫ

Как повышали привилегии пентестеры Positive Technologies в сети в 2021 году

- Атака Zerologon использовала уязвимость в протоколе Netlogon (CVE-2020-1472);
- уязвимость PrintNightmare в диспетчере очереди печати Windows (CVE-2021-34527).

Методы проникновения в локальную сеть (доля компаний)



Источник: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf

ВНУТРЕННИЕ ПЕРЕМЕЩЕНИЯ

Перемещаться от устройства к устройству злоумышленнику необходимо, чтобы достичь нужной ему цели

Действия атакующих внутри сети

Перехват учетных данных одного из сетевых узлов

Продвижение в инфраструктуре:
эксплуатация уязвимостей, применение хакерского инструментария, сокрытие своей активности от средств защиты

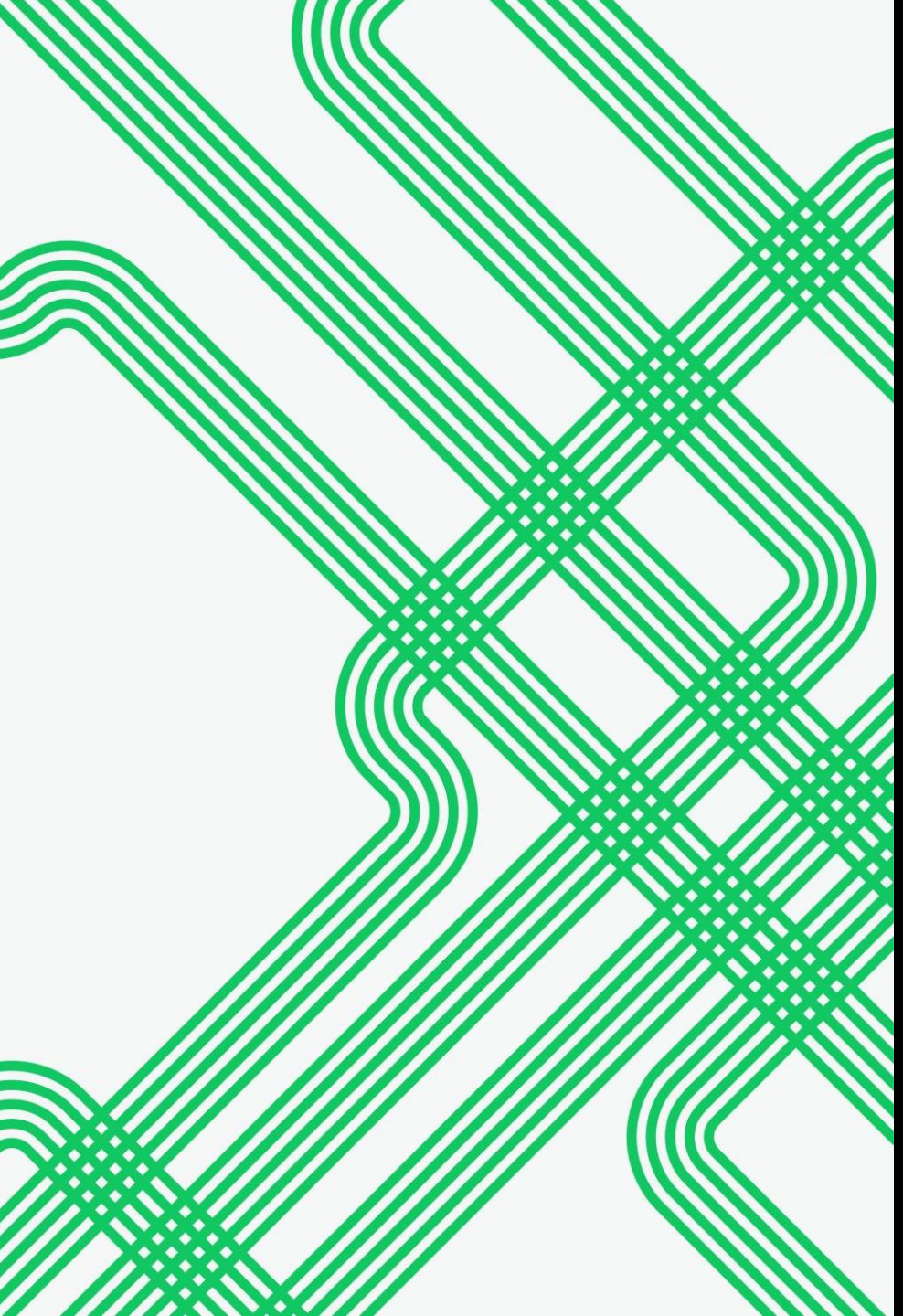
Охота за учетными данными администратора

Полная компрометация инфраструктуры:
получение доступа к контроллеру домена с максимальными привилегиями

Закрепление в инфраструктуре:
постоянный доступ к целевому хосту

Постоянный доступ к интересующей информации

В 2021 году **наши пентестеры** во всех исследуемых системах **получили полный контроль** над внутренней инфраструктурой.



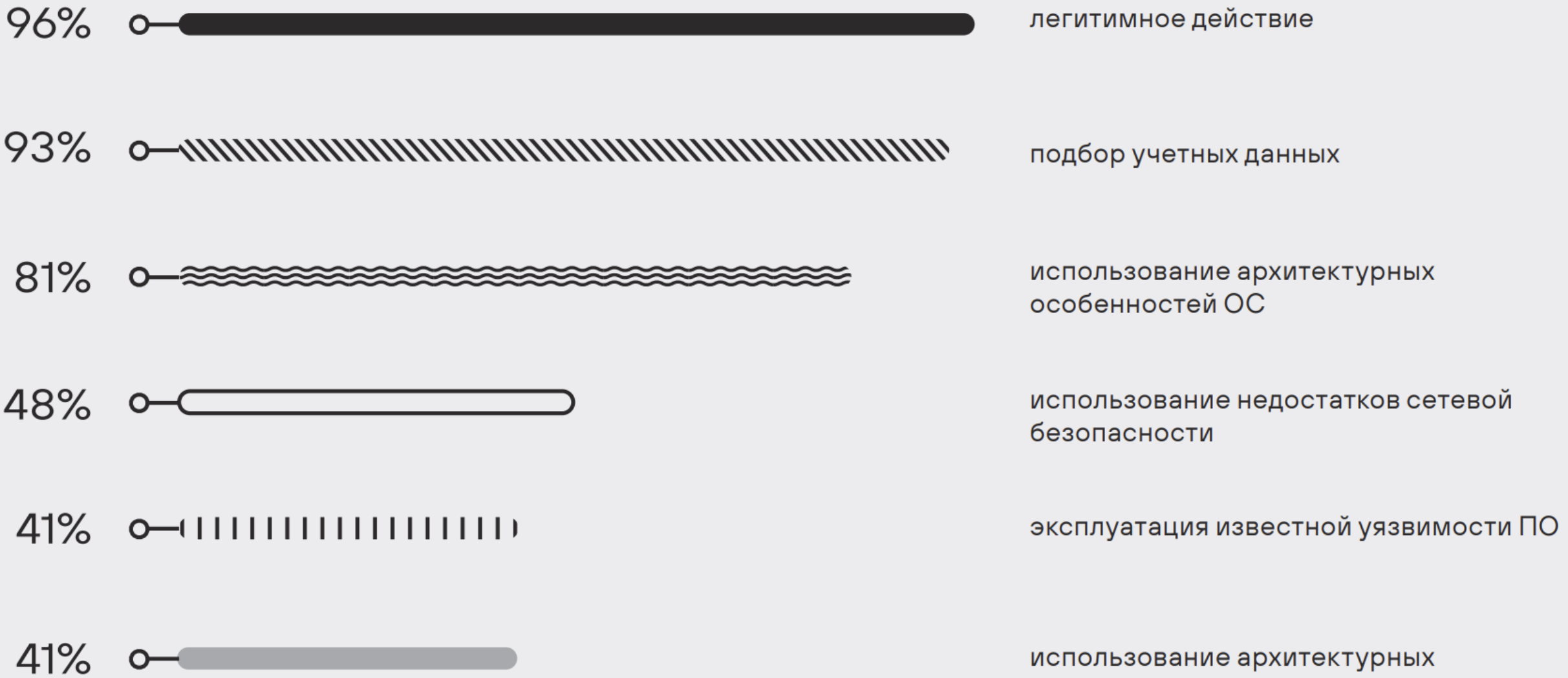
НЕТ СЕГМЕНТАЦИИ

В большинстве компаний отсутствует сегментация сети по бизнес-процессам, что позволяет развивать несколько векторов атак вплоть до реализации нескольких недопустимых событий одновременно.

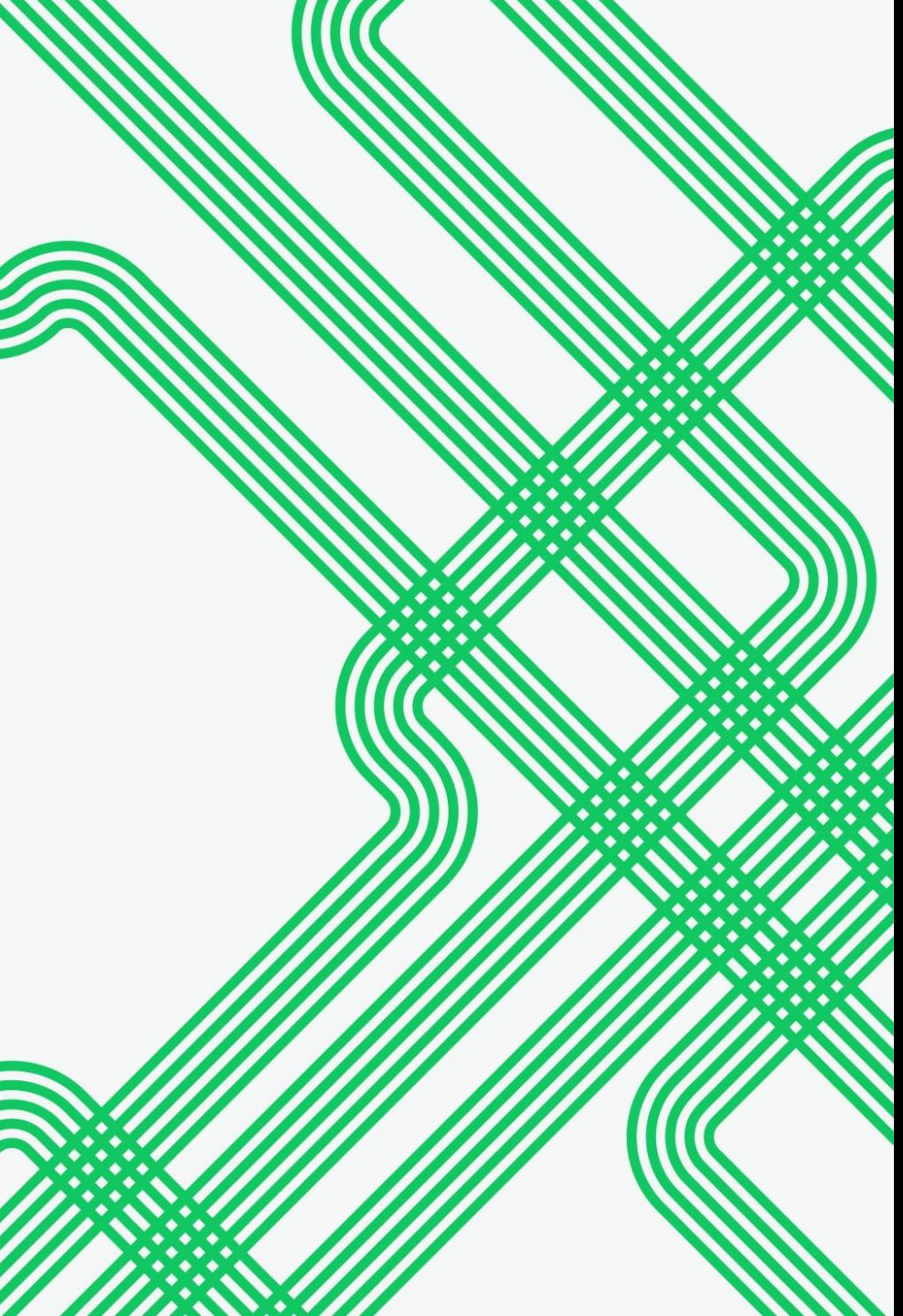
Доверительные отношения между доменами либо одни и те же учетные данные администраторов, дают контроль и над другими корпоративными доменами и позволяет проводить атаки дальше.

Максимальное число подконтрольных доменов внутри одной компании, полученное в рамках работ по анализу защищенности со стороны внутреннего злоумышленника, — десять.

Успешные атаки внутри сети (доля компаний)



Источник: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf



КЛЮЧЕВЫЕ СИСТЕМЫ НЕ ЗАЩИЩЕНЫ

Получить доступ в изолированные сегменты сети, к ключевым компьютерам и серверам нарушителю зачастую помогают средства администрирования, виртуализации, защиты или мониторинга.

Хранят информацию об инфраструктуре (устройствах, IP-адресах, активных сервисах, используемом ПО);
позволяют удаленно контролировать устройства (есть возможность удаленно выполнить код на агентах);
имеют распределенную архитектуру (веб-интерфейс, базы данных, сервер, агенты);
имеют предустановленные учетные записи и используют определенные порты для подключения;
при отсутствии своевременных обновлений могут содержать уязвимости.

КЛЮЧЕВЫЕ СИСТЕМЫ БАНКОВ

В банковской сфере в число ключевых систем входят рабочие станции сотрудников, обеспечивающих администрирование платежных систем и банкоматов

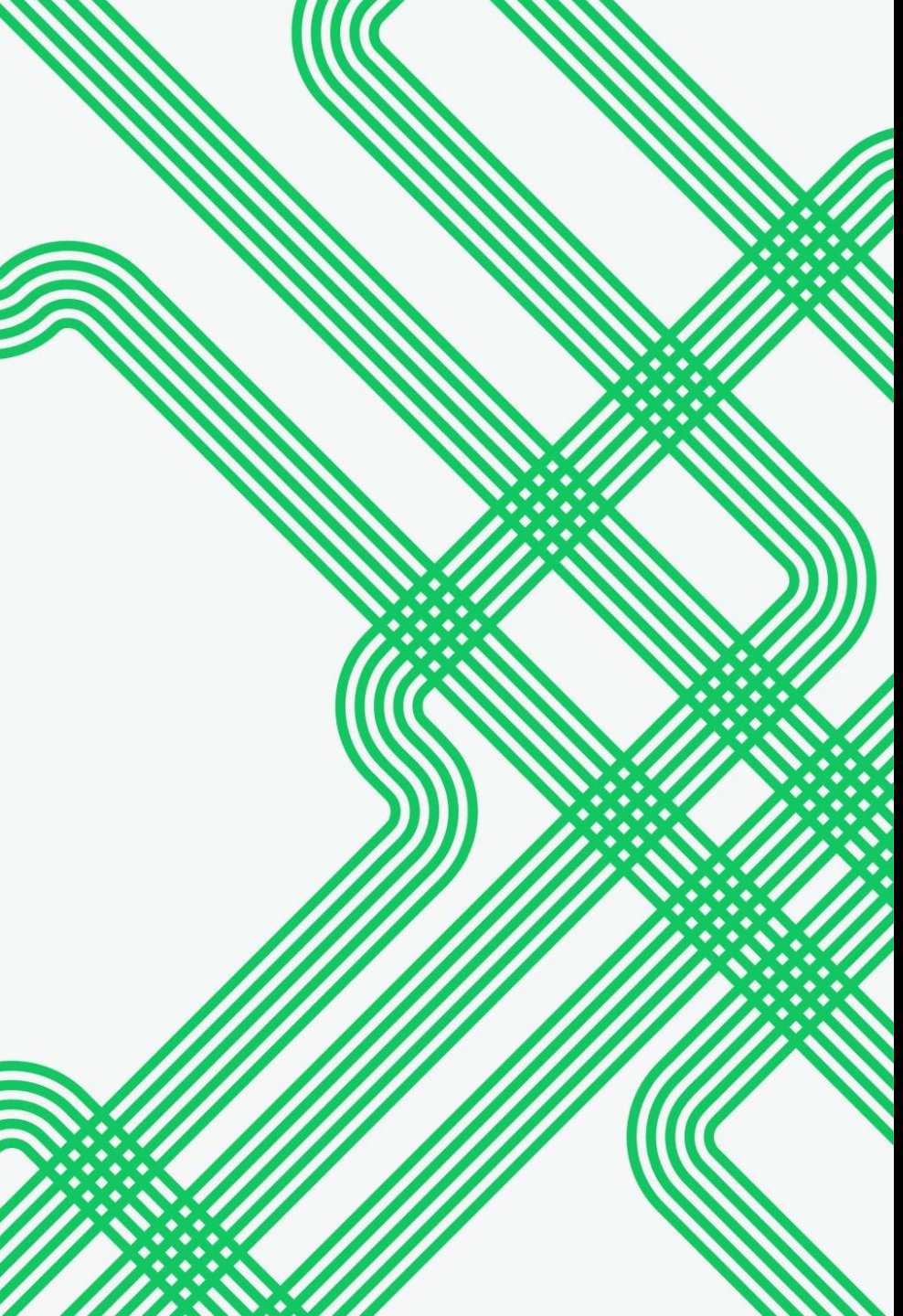
АТАКУЮТ КРИТИЧНЫЕ РЕСУРСЫ

Сегмент бухгалтерии

Сегмент топ-менеджеров

Сегмент АСУТП

НЕДОПУСТИМЫЕ СОБЫТИЯ



БЕСПЕЧНОСТЬ

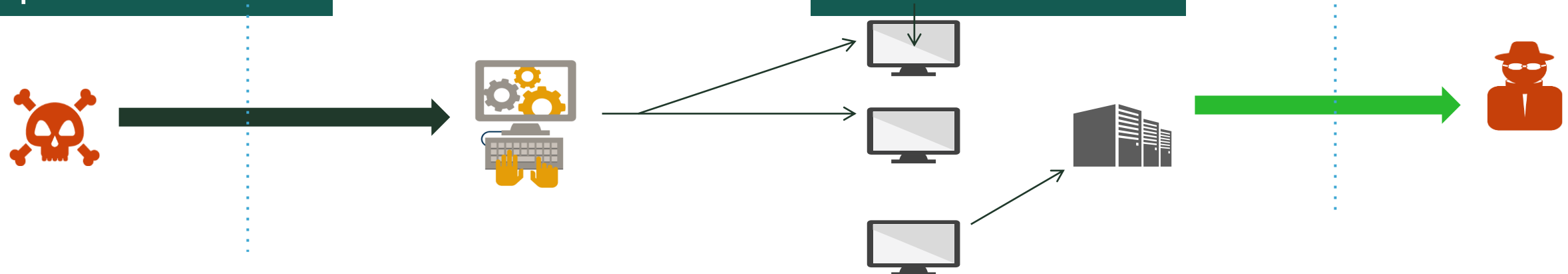
У 9 из 10 инженеров на компьютере в открытом виде хранится документ с перечнем используемых систем, кратким описанием, IP-адресами и учетными данными для входа

КАК ВОВРЕМЯ ОБНАРУЖИТЬ И ОСТАНОВИТЬ АТАКУ

- Разделение бизнес-процессов
- Харденинг ключевых и целевых систем
- Мониторинг
- Удлинение цепочек атаки

KILL CHAIN ИЛИ ПОШАГОВЫЙ ВЗЛОМ

Взлом Периметра	Доставка вредоносного ПО	Продвижение по сети	Кража данных
• Шифрованный трафик • Туннели • Вредоносные URLs • Передача файлов	• Скачивание в фоне (дроперы) • Установка C&C канала	• Поиск ценной информации (ЦОД) • Исполнение вредоносного ПО	• Скрытая выгрузка файлов/данных



КИБЕРБЕЗОПАСНОСТЬ - ЭТО ИНВЕСТИЦИИ В R&D

https://www.ptsecurity.com/ru-ru/research/

- Мы самый большой исследовательский центр в Восточной Европе. Более 150 экспертов мирового уровня по защите SCADA- и ERP-систем, веб-приложений, банковских и телекоммуникационных технологий ежегодно проводят исследования, тестирования на проникновение, анализ угроз и уязвимостей.
- Мы занимаемся
  - обнаружением новых угроз
  - threat hunting
  - поиском zero-day уязвимостей
  - reverse-engineering вредоносного ПО
  - анализом кода
  - анализом поведения хакерских группировок и их тактик, техник и процедур
  - поиском уязвимостей аппаратных решений
- Результаты работы используются для обновления баз угроз Positive Technologies, совершенствования существующих алгоритмов и разработки новых продуктов и решений

positive security day

ЧАТ В ТЕЛЕГРАММ

@PTNADCHAT

t.me/PTNADChat

Проверьте, что в вашей сети нет хакеров!

Денис Батранков,
эксперт по информационной безопасности, CISSP

bdv@ptsecurity.com

ptsecurity.com