Алексей Титов
Руководитель группы поддержки продаж «Восток»

PT Dephaze

Безопасный внутренний автопентест инфраструктуры

Два кейса из современной реальности

Реальная атака

- Получен полный массив баз данных
- Скомпрометированы все критически значимые корпоративные системы, включая Exchange, SharePoint, CRM-, ERP-, DLP-решения, КАСУД, продукты «1С» и другие
- Получен контроль над персональными компьютерами сотрудников, в том числе высшего руководства
- Скопированы данные с серверов, включая аудиозаписи телефонных разговоров и сообщения
- Извлечены данные из систем наблюдения и контроля за персоналом
- Получен доступ к 122 гипервизорам, 43 инсталляциям виртуализации zVirt, примерно к сотне iLO-интерфейсов для управления серверами, 4 кластерам Proxmox
- Уничтожено около 7000 серверов — физических и виртуальных

Отчет о «пилоте» PT Dephaze у одного из заказчиков

- Потеря контроля над ИТ-системами
- Полная компрометация конфиденциальных сведений (баз данных, файловых хранилищ, почты)
- Возможность шифрования всех серверов и рабочих станций (например, с помощью ransomware)
- Нарушение работы критически важных сервисов (DHCP, DNS, центра сертификации, систем «1С» и других)
- Потенциальное нарушение бизнес-процессов
- Массовое заражение узлов сети
- Падение производительности и (или) потеря данных на множестве серверов и рабочих станций
- Высокие затраты на восстановление (откат из бэкапов, реимиджинг, аудит)

Регулярная проверка защищенности

Российские компании работают в условиях постоянного изменения не только ИТ-инфраструктуры, но и ландшафта киберугроз

53%

компаний

подвергались атакам за последний год, несмотря на наличие в среднем более 20 средств защиты в инфраструктуре

в 79%

компаний

изменения в ИТ-среде происходят чаще, чем раз в квартал, но только 21% компаний регулярно заказывают услуги по тестированию на проникновение

в 100%

компаний

при проведении внутреннего пентеста можно установить полный контроль над инфраструктурой

Недостаточно использовать средства защиты: необходимо также регулярно проверять их эффективность и оценивать защищенность систем

Результаты опроса Positive Technologies в ноябре 2024 года
Итоги пентестов 2023

Оценка защищенности. Сравнение методов

Критерий	Сканер уязвимостей	Ручной пентест
Способ оценки	Автоматизированными средствами	Вручную, зависит от знаний и навыков тестировщика
Исполнитель	Штатные специалисты	Независимый внешний консультант
Частота	Постоянно	Периодически
Показатели	Известные гипотетически эксплуатируемые уязвимости	Реально эксплуатируемые уязвимости
Релевантность результатов	Низкая: не учитывает специфику сети и процессов	Высокая: показывает реальный ущерб для бизнеса
Охват уязвимостей	Только уязвимости ПО	Уязвимости ПО и человеческий фактор

01

Автопентест от Positive Technologies

Оценка защищенности. Сравнение методов

Критерий	Сканер уязвимостей	Ручной пентест
Способ оценки	Автоматизированными средствами	
Исполнитель	Штатные специалисты	
Частота	Постоянно	
Показатели		Реально эксплуатируемые уязвимости
Релевантность результатов		Высокая: показывает реальный ущерб для бизнеса
Охват уязвимостей		Уязвимости ПО и человеческий фактор

Концепция PT Dephaze

Не просто симулирует атаку, а проводит реальное тестирование на проникновение, как это мог бы делать настоящий злоумышленник

Самостоятельно принимает решение о продвижении внутри инфраструктуры и собирает полную цепочку атаки

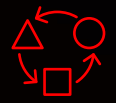
Проводит контролируемое и безопасное тестирование, которое не может нарушить критически важные процессы в компании

Масштабирует практики ручного пентеста, позволяя в комплексе находить больше потенциальных векторов атак

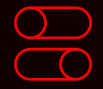
Пентест запускается в несколько кликов: достаточно подключить PT Dephaze к сети и начать проверку

Безопасность и контроль при проведении пентеста

«Под капотом» PT Dephaze нет опасных эксплойтов, способных вывести из строя ПО или актив



Все атакующие действия проходят тестирование перед попаданием в продукт



В продукте есть возможность настроить ограничения тестирования и параметры его контроля

Опыт проведения «пилотов» PT Dephaze

45 минут

потребовалось пользователю, чтобы запустить первый пентест после получения дистрибутива

≈3 дня

время работы пентеста на 512 узлах с Active Directory

Результат

зависит от сегмента, наличия пользовательской активности, сетевых сервисов и служб, количества доменов

Результаты пилотных проектов

1. 20 «пилотов» с полным согласованием атак и отсутствием негативного влияния на инфраструктуру
2. Эксплуатация мисконфигураций с получением учетных записей пользователей и администраторов (доменных и локальных)
3. Получение привилегированного доступа к Windows- и Linux-узлам
4. Перехват критически важных данных в сетевом трафике

02

Как работает PT Dephaze

Компоненты системы

Сервер

Для управления симуляциями — минимум один

Атакующие узлы

Для выполнения атакующих действий

Мобильный модуль*

Для установки на ноутбуке. Поддерживается до 500 узлов, есть возможность переноса

Количество узлов — основной параметр для оценки стоимости

* При закупке соответствующих лицензий

PT Dephaze поможет повысить общий уровень защищенности

Сервер управления отправляет на атакующий узел данные, необходимые для выполнения команд и инструкций

Агент на атакующем узле обрабатывает полученные данные и выполняет команды на их основе

Агент на атакующем узле передает на сервер статус выполнения команд и инструкций. Переход к этапу 1

PT Dephaze поможет повысить общий уровень защищенности

1

Подключаем PT Dephaze к сети компании для старта работы

Не требуется долгое внедрение, продукт быстро вводится в эксплуатацию

2

Запускаем тестирование после согласования критически важных действий

Обеспечиваем безопасную и контролируемую проверку

3

Наблюдаем за процессом построения цепочки атаки

В любой момент атака может быть остановлена по желанию оператора

4

Получаем отчет о проверке

Находим уязвимые узлы и выбираем пути оптимизации защиты

03

Как использовать PT Dephaze

Для чего применять PT Dephaze

Обнаружение и эксплуатация недостатков безопасности

Оптимизация и масштабирование ручного пентеста

Проверка эффективности СЗИ и SOC

Выявление векторов атак, которыми могут воспользоваться хакеры

Что оценивает PT Dephaze

Сервер

Помогает компаниям внедрять практики наступательной безопасности, заранее оценивать защищенность инфраструктуры и выявлять уязвимые места до того, как ими воспользуются киберпреступники

Поможет

- Оптимизировать и масштабировать ручной пентест
- Минимизировать вероятность успешных кибератак

Эффективность работы системы защиты

Позволяет оценить качество обнаружения и противодействия нелегитимной активности в тестируемых сегментах сети, работу средств защиты (классов SIEM, NTA, EDR, EPP) и оперативно внести изменения в механизмы обеспечения ИБ

Поможет

- Обнаружить пробелы в системе защиты
- Выбрать приоритет для инвестиций в ИБ

Когда запускать PT Dephaze

Для поиска тех недостатков в защите инфраструктуры, с помощью которых злоумышленник сможет провести атаку	Для проверки реагирования SOC
Для проверки устранения замечаний из отчетов о пентестах	Для тестирования эффективности средств защиты информации
При изменении инфраструктуры (добавление или исключение активов)	Для подготовки к ручному пентесту
При обновлении атакующих техник в продукте	Для приоритизации исправления недостатков защиты

04

Планы развития PT Dephaze

Планы по развитию

Q2 2025

Экспертиза

- SSH и первичная разведка (Linux)
- PostgreSQL
- GitLab
- Расширение атакующих действий на Windows, Active Directory

Продукт

- Экстренное завершение пентеста
- Уровень опасности атак и приоритизация

Q3 2025

Экспертиза

- SCCM
- Confluence
- Расширение списка атакующих действий на Windows, Active Directory (например, атаки на центр сертификации)
- Атаки на Linux, разведка и повышение привилегий
- MSSQL
- FTP, ARP spoofing
- Расширение перечня сетевых атак и атак для получения первичного доступа (например, MITM6, PetitPotam)

Продукт

- Экстренное завершение пентеста
- Уровень опасности атак и приоритизация

Q4 2025

Экспертиза

- Поддержка атак на FreeIPA
- Поддержка атак на системы управления безопасностью организаций (KSC)
- Поддержка атак на Zabbix
- Поддержка атак на «Битрикс-24»
- Поддержка атак на продукты «1С»
- Поддержка СУБД (MongoDB, ClickHouse)

Продукт

- Расширение области тестирования при возможном горизонтальном перемещении
- Поиск конфиденциальных данных
- Уведомления (статус пентеста, согласования, результаты)

Попробовать PT Dephaze

Задать вопрос по теме выступления

habrahabr.ru/company/pt

pt@ptsecurity.com

ptsecurity.com

Спасибо