



ПРИМЕР ОТ ПРАКТИКАТА

Добре защитен периметър — и атака в ход

Производство · Външен мрежови тест за проникване и OSINT

2 критични проблема и данни за активна атака

Анонимизиран съгласно NDA. Клиентът и идентифициращите детайли са премахнати. PXLSecurity LTD. · София, България · pxlsec.com



ПРИМЕР ОТ ПРАКТИКАТА

Добре защитен периметър — и атака в ход

Сектор	Производство
Ангажимент	Външен мрежови тест за проникване и OSINT
Резултат	2 критични проблема и данни за активна атака

2	в реално време	стегнат
критични проблема	засечена активна атака с изтекли идентификационни данни	иначе добре защитен с защитни стени

ПРЕДИЗВИКАТЕЛСТВОТО

Производител искаше да оцени сигурността на малкия си интернет периметър, защитен с внимателно настроени защитни стени, и рисковете за потребителските си акаунти.

КАК СЕ РАЗВИ

1. Картографирахме ограничен интернет периметър с добре настроени защитни стени.
2. Открихме публично достъпен шлюз за отдалечен достъп, който удостоверяваше потребители към AD, но работеше върху сървърна операционна система без поддръжка.
3. Потвърдихме, че NTLM отговорът на шлюза разкрива имената на вътрешния домейн и хостове.
4. Засяхохме активна външна кампания за credential stuffing — опити за вход с изтекли идентификационни данни — срещу няколко акаунта за облачна поща.
5. Открихме пароли в изтекли набори от данни, но потвърдихме, че те вече са били сменени. Предадохме идентификаторите за проследяване от доставчика, за да бъдат съпоставени със записите в журналите.
6. Открихме услуга за обмен на файлове с партньори, която допускаше остарели слаби криптографски алгоритми и не изискваше взаимно TLS удостоверяване.

ОСНОВНИ КОНСТАТАЦИИ

Critical	Шлюз за отдалечен достъп, достъпен от интернет, върху ОС без поддръжка
Critical	Засечена активна кампания за credential stuffing
Medium	Разкриване на имена на вътрешен домейн и хостове чрез NTLM
Medium	Слаби криптографски алгоритми и липса на взаимно TLS удостоверяване при обмена с партньори

ВЪЗДЕЙСТВИЕ

Един неактуализиран шлюз или повторно използвана парола можеше да даде на нападател начален достъп. По време на нашия тест вече течеше реална атака срещу компанията.

РЕЗУЛТАТ

Предадохме приоритизиран план: извеждане от употреба на шлюза без поддръжка, ограничаване на риска от credential stuffing, въвеждане на DMARC, взаимно TLS удостоверяване и съвременни криптографски алгоритми. Предоставихме и конкретни данни за разследване на атаката, която вече течеше.

ТЕХНИКИ

Картографиране на периметъра · OSINT · Засичане на credential stuffing · Сигурност на електронната поща (DMARC) · Остарял TLS

УСЛУГИ

Тестване за проникване · Оценка на уязвимостите

Работете с PXLSec

Независимо офанзивно тестване на сигурността от 2014 г. — тестване за проникване, red teaming и сигурна разработка, изпълнявани от старши инженери, с доказателство за всяка констатация и повторен тест, който потвърждава поправката.

Заявете предложение: pxlsec.com/bg/contact · hello@pxlsec.com

PXLSecurity LTD. · бул. „Васил Левски“ 12, 1142 София, България · VAT BG203239331