



ПРИМЕР ОТ ПРАКТИКАТА

Десетгодишната парола зад Domain Admin

Банкиране · Red team: фишинг и предполагаем пробив

Потвърдени защиты и план за укрепване на Active Directory

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



ПРИМЕР ОТ ПРАКТИКАТА

Десетгодишната парола зад Domain Admin

Сектор	Банкиране
Ангажимент	Red team: фишинг и предполагаем пробив
Резултат	Потвърдени защиты и план за укрепване на Active Directory

0 / 2	1	десетки
успешни фишинг кампании	открит път до Domain Admin	акаунти, уязвими на AS-REP roasting

ПРЕДИЗВИКАТЕЛСТВОТО

Финансова институция искаше да провери устойчивостта си срещу фишинг и срещу нападател, получил достъп до стандартен домейнов акаунт на виртуален работен плот.

КАК СЕ РАЗВИ

1. Проведохме две фишинг кампании: първата беше блокирана от пощенския шлюз, а съобщенията от втората бяха доставени, но служителите не се подведоха.
2. Продължихме със сценарий за предполагаем пробив: достъп до стандартен домейнов акаунт на виртуален работен плот.
3. Събрахме информация за домейна единствено с вградени системни средства.
4. Открихме служебен акаунт с права Domain Admin, регистриран Kerberos SPN и парола, която не беше променяна от повече от десет години.
5. Използвахме Kerberoasting за офлайн разбиване на паролата. Открихме и десетки акаунти, уязвими на AS-REP roasting, както и стар администраторски акаунт с парола без срок на валидност.
6. Сегментацията между виртуалните работни плотове и локалната инфраструктура на директорията значително ограничи придвижването към други системи.

ОСНОВНИ КОНСТАТАЦИИ

High	Служебен акаунт Domain Admin, уязвим на Kerberoasting, с непроменяна от години парола
High	Десетки акаунти, уязвими на AS-REP roasting
Medium	Стар вграден администраторски акаунт с парола без срок на валидност
Positive	Ефективни защиты срещу фишинг, подготвени служители и работеща сегментация

ВЪЗДЕЙСТВИЕ

Обикновен потребителски акаунт можеше да доведе до пълно компрометиране на домейна. Същевременно защитите на електронната поща, подготовката на служителите и мрежовата сегментация ограничиха възможностите за атака.

РЕЗУЛТАТ

Предадохме ясен план за управление на привилегированите акаунти и укрепване на Kerberos. Независимо потвърдихме и ефективността на защитите срещу фишинг, подготовката на служителите и мрежовата сегментация.

ТЕХНИКИ

Фишинг · Предполагам пробив · Използване на вградени средства · Kerberoasting · AS-REP roasting

УСЛУГИ

Red Teaming · Active Directory и вътрешна мрежа · Социално инженерство и фишинг

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