PRÍBEH 2

SKUTOČNÝ RANSOMWARE ÚTOK NA SLOVENSKÚ VÝROBNÚ FIRMU

—

KROK ZA KROKOM.

KOVOTRON

PRESNÁ KOVOVÝROBA · SLOVENSKO

Noc

Šifrovanie spustené naprieč celou sieťou naraz.

06:40

Prvé zamknuté obrazovky. Objavený „ransom note“ na desktopoch operátorov.

07:00

Produkčná infraštruktúra nepoužiteľná. Linky stoja, ERP nepristupný.

08:00

IT administrátori v práci

TIMELINE · PRVÝCH OSEM HODÍN PO ŠIFROVANÍ

VYŠETROVANIE UKÁZALO

ZAČALO TO DOMA, V PREHLIADAČI.

01 Zamestnanec si doma stiahol crackovaný softvér.
Bežný, „neškodný“ krok na súkromnom PC.

02 So softvérom bol ”pribalený” infostealer.
Vytiahol heslá, cookies, session tokeny.

03 Obeť bola IT administrátor.
V prehliadači mal uložené aj firemné prístupy — vrátane privilegovaných.

04 Do 24 hodín boli heslá na predaj.
Initial Access Broker ich umiestnil na trh prístupov pre najvyššiu ponuku.

ŽIADNE HACKOVANIE — ÚTOK SA “KÚPIL.”

Initial Access Broker zbiera a predáva firemné prístupy.

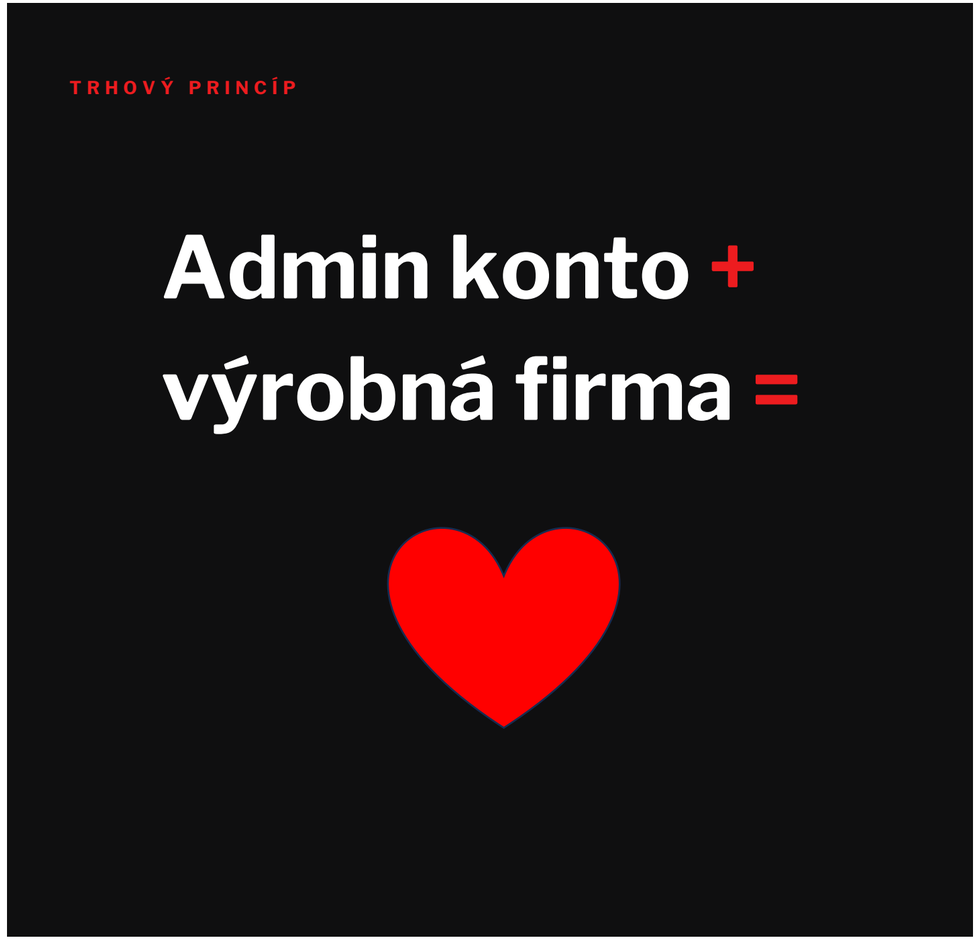
Nezaujíma ho, čo je za nimi. Predá ich tomu, kto zaplatí.

Ransomware skupina si kúpila prístup do KOVOTRON-u.

Admin konto + výrobná firma = ideálny cieľ.

Od kúpy po šifrovanie ubehli zhruba tri týždne.

Ticho. Pozorovanie. Mapovanie. Príprava.



C2 SERVER VNÚTRI SIETE

TRI TÝŽDNE TICHÉHO PRIESKUMU SIETE.

Mapovanie cieľov vysokej hodnoty.
Zálohy, doménový radič, EDR konzola, mapa privilégií.

C2 server nasadený priamo vo vnútri siete.
Hostiteľ: zabudnutý interný server, ktorý nikto roky nepatchol.

Komunikácia ostala interná.
Perimeter nikdy nevidel exfiltrované alerty — a tak nepípol.

PRINCÍP

Ak C2 býva v rovnakej sieti ako obeť, perimeter je slepý.

Vnútorný monitoring, segmentácia a hľadanie anomálií v lateral movement-e sú jediná cesta, ako toto zachytiť.

LIVING OFF THE LAND

ÚTOČNÍK NEPOUŽIL VLASTNÉ NÁSTROJE. POUŽIL VAŠE.

PowerShell, legitímne skripty, plánovač úloh.

Pre monitoring to vyzeralo ako bežná IT aktualizácia.

EDR killer cez zraniteľný ovládač.

EDR nebol obídený — bol vypnutý. Cielene, na kľúčových serveroch.

DEFINÍCIA

Living off the land = útok vyzerá ako práca vášho vlastného administrátora.

NAJPRV KRÁDEŽ, POTOM ŠIFROVANIE

DOUBLE EXTORTION — ŠIFROVANIE AJ KRÁDEŽ.

TICHÁ EXFILTRÁCIA

Desiatky GB von, postupne, bez špičky v sieťovom traffic-u.

EXFILTRÁCIA CEZ ONEDRIVE

KOVOTRON používal OneDrive. Útočník tiež.

Dôveryhodné služby sú najlepšia kamufláž.

LIKVIDÁCIA ZÁCHRANY

PROFESIONÁL NAJPRV ZNIČÍ ZÁLOHY. (FIRMA S DOBROU ZÁLOHOU ZLE PLATÍ.)

Shadow copies zrušené jedným príkazom.

Žiadny restore point, žiadne „vrátiť o hodinu späť“.

Cloudové zálohy? Admin konto stačilo.

Tá istá identita, ktorá zálohy spravuje, ich aj likviduje.

Vymazaná nie jednotlivá záloha — celá zálohovacia inštancia.

Vrátane konfigurácie a retenčných pravidiel.

ZÁVER

KOVOTRON nemal cestu späť. Len o tom ešte nevedel.

Záloha, ktorú vie zničiť bežné admin konto, nie je záloha. Je to iba kópia v rovnakej dôveryhodnej zóne.

DOPADY NA KOVOTRON

ŠIFROVANIE TRVALO PÁR HODÍN. DOPADY TRVAJÚ DODNES.

01 · VÝROBA

9 dní stojaca výroba

Zmluvné pokuty voči odberateľom. Dohnať skĺz objednávok trvalo mesiace.

02 · DÁTA

Trvalá strata časti dát

Časť firemných údajov je nenávratne preč.

03 · SÚKROMIE

Únik citlivých údajov

Dokumentácia, personálne dáta, zmluvy. Notifikačné povinnosti voči úradom a dotknutým osobám.

04 · NÁKLADY

Stovky človekodní obnovy

Forenzná analýza, reinštalácie, prepisovanie procesov, externé tímy.

05 · ROZHODNUTIE

Otázka výkupného

Eticky, právne aj finančne ťažké. Žiadna z odpovedí nie je dobrá.

06 · REPUTÁCIA

Reputačný dopad

Klienti, partneri, dodávatelia

ŠTYRIA EXPERTI

ČO BY SPRAVILA ODOLNÁ FIRMA INÁČ?

Štyri pohľady na ten istý prípad — od prevencie po legislatívu.

01
PREVENCIA

02
DETEKCIA

03
REAKCIA

04
LEGISLATÍVA

01

PREVENCIA

02

ZO ŠTYROCH POHĽADOV

DETEKCIA

03

REAKCIA

04

ZO ŠTYROCH POHĽADOV

LEGISLATÍVA

RÝCHLE ODPORÚČANIA

ŠTYRI ODPORÚČANIA ”SO SEBOU.”

01 **Strážte EDR a zálohy ako prioritu č. 1.**
Ich vypnutie alebo mazanie = okamžitý alarm.

02 **Oddeľte privilegované účty a zaveďte MFA.**
Žiadne účty z Internetu bez MFA. Žiadne zdieľané admin kontá.

03 **Majte immutable / offline zálohu — a testujte obnovu.**
Záloha, ktorú zničí jedno admin konto, nie je záloha.

04 **Ransomware IR plán a dohodnutý tím.**
V noci o tretej je už neskoro hľadať telefónne číslo.

Dva veľmi odlišné útoky. Rovnaký záver.

01

Ani jeden z nich nebol o geniálnom hackingu. Boli o zle nastavených nástrojoch a procesoch.

02

Rozhodli postupy a (ne)príprava — všetko spravené dávno pred incidentom.

03

Odolnosť nie je produkt. Je to spôsob, akým je firma postavená.