

DIGITÁLNA FORENZNÁ ANALÝZA

Prípad: Interný únik dát (Aether
Defense)

Bahdan Rychak

Zhrnutie prípadu

Spoločnosť **Aether Defense** zistila únik proprietárneho zdrojového kódu

Konkurenčná firma publikovala produkt s podobnou navigačnou logikou

Hlavný podozrivý: **Alexej S.** (bývalý vedúci vývojár)

Cieľ vyšetrovania:

- ▶ zistiť spôsob úniku,
- ▶ identifikovať páchatela,
- ▶ zaistiť digitálne dôkazy

Obráz incidentu (Metodika 5WH)

Who? (Kto?)

Alexej S. - bývalý vedúci
vývojár spoločnosti

Aether Defense

Hlavný podozrivý s plným
prístupom k internému
zdrojovému kódu

What? (Čo?)

Neoprávnené kopírovanie
a odcudzenie
proprietárneho
zdrojového kódu
navigačného systému
spoločnosti **Aether
Defense**

When? (Kedy?)

1. - 30. marec 2026

kritické obdobie: posledné
dni pred odovzdaním
služobného notebooku

Where? (Kde?)

- firemný notebook
podozrivého
- USB zariadenie
nájsené u podozrivého
- osobný smartfón
(komunikácia)

Why? (Prečo?)

Predpokladaný motív:

- osobná frustrácia po
prepustení
- finančný motív
- snaha predat' interné
dáta konkurencii

How? (Ako?)

Predpokladaný spôsob
exfiltrácie:

- otvorenie projektových
súborov
- kompresia do ZIP archívu
- kopírovanie na USB
- komunikácia cez smartfón
- pokus o predaj konkurencii

Časová os incidentu

Marec 2026



18.03.

Príprava postupu

- Vytvorenie notes.txt
- Plán kopírovania zdrojového kódu



18.–25.03.

Práca so zdrojovým kódom

- Úpravy projektu NavigationCore
- Práca s citlivými súbormi



25.03.

Vytvorenie ZIP archívu

- Kompresia projektu
- Názov archívu: NavigationCore.zip



25.03.

Kopírovanie na USB

- Prenos archívu na USB kľúč
- Použité médium: Smartbuy 8GB



25.–27.03.

Komunikácia o predaji dát

- Komunikácia cez Telegram
- Dohoda na predaji kódu



30.03.

Odovzdanie notebooku

- Alexej S. odovzdáva pracovný notebook
- Koniec pracovného pomeru

Hypotézy vyšetrovania

► H1 - Insider útok

Alexej S. skopíroval zdrojový kód na USB a pokúsil sa ho predat'

► H2 - Externý útok

Hackeri získali prístup cez phishing / VPN

► H3 - Súčasný zamestnanec

Niektor zamestnancov poskytol kód po prepustení

Digitálne zariadenia



NOTEBOOK

Dell Latitude 7450



Primárna pracovná stanica
podozrivého



Uložené projektové súbory,
dokumenty, lokálne dáta



Prístup do firemnej siete
a Git repozitára



USB KĽÚČ

Smartbuy USB 8 GB



Vymeniteľné médium
exfiltrácie



Obsah: komprimovaný
archív so zdrojovým kódom



Notes.txt – plán a inštrukcie
na export dát



SMARTFÓN

Xiaomi Mi 9T



Komunikácia s externými
osobami



Dôkazy o predaji kódu
a motíve



Správy, chaty, súbory,
metadáta



RAM DUMP

Volatilná pamäť



Dočasné dáta v pamäti
počas aktivity



Zvyšky otvorených aplikácií,
vyhľadávačov, e-mailov



Dáta, ktoré sa nenachádzajú
na disku

Analýza RAM - klúčové artefakty

► RAM-01: Konkurenčný web + e-mail

URL konkurenčnej firmy

fragment e-mailu s ponukou interného kódu

► RAM-02: Otvorený projekt

NavigationCore

CalculateBearing

AetherDefense.Navigation

► RAM-03: Podozrivé vyhľadávania

“how to compress large project folders”

“how to copy files from work computer without being detected”

Dôkazy z image zariadení

- ▶ **Zdrojový kód na osobnom PC**
GeoPoint.cs, INavigationCore.cs
- ▶ **Timeline activity**
Aktívna práca so súbormi počas incidentu
- ▶ **ZIP archív na USB**
Projekt prenesený na externé médium
- ▶ **Notes.txt**
export navigation core
USB only
compress - zip

Smartfón - komunikácia a motív

► John Smith

potvrdený predaj kódu

potvrdený ZIP archív

potvrdené USB

odmena: **1000 EUR**

► Kamarat

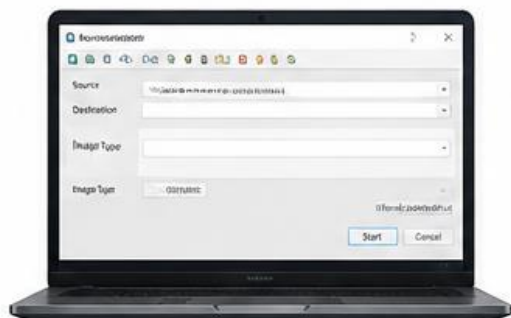
frustrácia po prepustení

motív: pomsta + peniaze

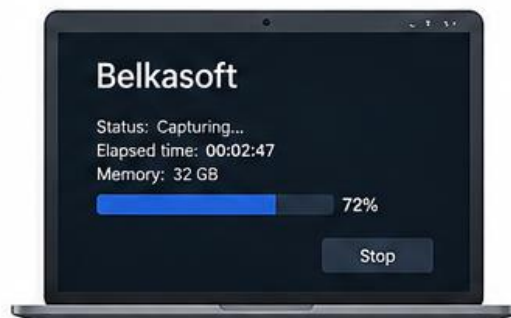
Použíte nástroje



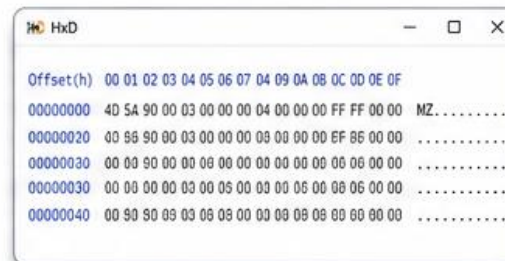
FTK Imager



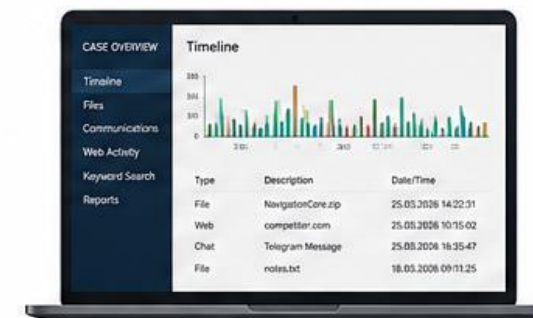
Belkasoft Live RAM Capturer



HxD Hex Editor



Magnet AXIOM



Bitové kópie zariadení

Vytvorenie forenzných obrazov (dd, E01)



Overenie integrity

Výpočet a overenie hash hodnôt (MD5, SHA-256)



Write blocker podpora

Zabezpečenie dôkazov pred zmenou počas kopírovania



Zachytenie RAM pamäte

Vytvorenie dumpu volatilnej pamäte (RAM)



Volatilné dáta

Získanie dočasných dát, ktoré sa po vypnutí stratia



Dôkazy v pamäti

Procesy, sieťové pripojenia, otvorené súbory, príkazy



Hex analýza

Prezeranie a úprava binárnych dát na nízkej úrovni



Hľadanie signatúr

Vyhľadávanie textov, hex výrazov, súborových hlavičiek



Manuálna analýza artefaktov

Overenie a rekonštrukcia dát, file carving



Centralizovaná analýza

Analýza diskových obrazov, RAM dumpov, mobilných dát



Timeline & korelácia

Časová os udalostí a prepojenie artefaktov



Reporty a export

Vytváranie forenzných správ pre vyšetrovanie

Výsledky hypotéz

► H1 - POTVRDENÁ

Insider útok

USB + ZIP + komunikácia + RAM

► H2 - ZAMIETNUTÁ

Externý útok

bez phishingu, bez VPN stôp

► H3 - ZAMIETNUTÁ

Súčasný zamestnanec

bez relevantných dôkazov

Záver

- ▶ Alexej S. neoprávnene skopíroval interný zdrojový kód
- ▶ použil USB ako médium exfiltrácie
- ▶ pripravil ZIP archív
- ▶ plánoval vyhnúť sa detekcii
- ▶ pokúsil sa dáta predať konkurencii

Ďakujem za
pozornosť

Priestor pre
otázky