

DIGITÁLNÁ FORENZNÁ ANALÝZA

Prípad: Ukradnutý herný účet

Ivan Borec



ZHRNUTIE PRÍPADU

Používateľ Donald Yang zistil neoprávnený prístup k svojmu účtu na platforme Roblox

Jeho hra sa objavila na sociálnej sieti TikTok a získala popularitu bez jeho súhlasu

Podozrenie na prevzatie účtu treťou osobou

Hlavný podozrivý: David Hilton (majiteľ notebooku)

Cieľ vyšetrovania:

1. zistiť spôsob získania prihlasovacích údajov,
2. potvrdiť neoprávnený prístup k účtu,
3. zaistiť digitálne dôkazy (logy, e-maily, RAM artefakty)

5WH

Who? (Kto?)

Donald Yang – vlastník Roblox účtu

Obeť neoprávneného prístupu

David Hilton – majiteľ notebooku

Hlavný podozrivý s možným prístupom k účtu

What? (Čo?)

Neoprávnené získanie prihlasovacích údajov
a prevzatie kontroly nad Roblox účtom

Zmena prihlasovacích údajov a zneužitie
digitálneho obsahu (hra, profil)

When? (Kedy?)

Roky 2024 – 2025

kritické obdobie: pred zistením straty prístupu
k účtu a zmenou prihlasovacích údajov

Where? (Kde?)

- notebook podozrivého (David Hilton)
- mobilné zariadenie podozrivého
- online prostredie platformy Roblox
- e-mailová schránka viazaná na účet

Why? (Prečo?)

Predpokladaný motív:

- získanie kontroly nad populárnou hrou
- finančný prospech
- zneužitie cudzieho digitálneho obsahu

How? (Ako?)

Predpokladaný spôsob útoku:

- získanie prihlasovacích údajov (phishing/slabé heslo)
- prihlásenie do účtu z cudzieho zariadenia
- zmena prihlasovacích údajov
- následné využívanie účtu bez súhlasu vlastníka

HYPOTÉZY VYŠETROVANI A

H1 – Neoprávnený prístup (insider)

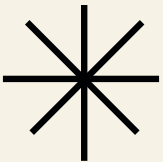
David Hilton získal prihlasovacie údaje a prihlásil sa do účtu Donalda Yanga, pričom prevzal kontrolu nad účtom

H2 – Externý útok

Neznáma osoba získala prístup k účtu prostredníctvom phishingu alebo slabého hesla a následne zmenila prihlasovacie údaje

H3 – Chyba používateľa

Donald Yang mohol neúmyselne zdieľať prihlasovacie údaje alebo použiť slabé heslo, čo viedlo k kompromitácii účtu



DIGITÁLNE ZARIADENIA

Mobilné zariadenie podozrivej osoby

Huawei P50 (128 GB)

- Android, 8 GB RAM
- Používané na prístup k účtu

Očakávané digitálne stopy:

- História prehliadača (vyhľadávanie „hack účtu“)
- Prihlasovacie logy
- Uložené prihlasovacie údaje
- Cookies / session tokeny
- E-mailové notifikácie o zmene hesla



DIGITÁLNE ZARIADENIA

Notebook podozrivej osoby

Lenovo IdeaPad 3 (512 GB SSD)

- Windows 10, 8 GB RAM
- Hlavné zariadenie na prístup k účtu

Očakávané digitálne stopy:

- História prehliadača (Roblox, hack návody)
- Súbory s prihlasovacími údajmi (credentials.txt)
- Cookies (.ROBLOSECURITY token)
- Prihlasovacie logy a časové pečiatky
- E-mail o zmene hesla



DIGITÁLNE ZARIADENIA



USB kľúč
Kingston DataTraveler 16 GB

- Prenosné úložisko
- Používané na prenos dát

Očakávané digitálne stopy:

- Zálohy prihlasovacích údajov
- Screenshoty účtu
- Exportované dáta / logy
- Prepojenie na notebook (časové pečiatky)

ANALÝZA RAM - KLÚČOVÉ ARTEFAKTY



Analýza RAM – klúčové artefakty

- V RAM neboli nájsené priame prihlasovacie údaje
 - Neboli identifikované aktívne session tokeny
-

Nájsený artefakt:

- Vyhľadávanie: „how to hack roblox account“
-

Interpretácia:

- Aktivita prebehla pred spáchaním incidentu
 - Naznačuje úmysel získať neoprávnený prístup
 - Podporuje hypotézu plánovaného útoku
-

DÔKAZY Z IMAGE ZARIADENÍ

Dôkazy z image zariadení

- history.db – história prehliadača

→ prístupy na Roblox + vyhľadávanie „hack účtu“

- cookies.sqlite – autentifikačné údaje

→ .ROBLOSECURITY token (aktívne prihlásenie)

- credentials.txt – uložené prihlasovacie údaje

→ meno, heslo, e-mail

- E-mail (security alert)

→ potvrdenie zmeny hesla

- Vymazaný profilový obrázok

→ pokus o odstránenie dôkazov

Záver:

- Priame dôkazy neoprávneného prístupu k účtu



POUŽITÉ NÁSTROJE

- FTK
Imager

- HxD
(Hex
Editor)

- Autopsy

- RAM-
Capturer

VÝSLEDKY HYPOTÉZ



Výsledky hypotéz

Hypotéza 1:

- Neoprávnený prístup podozrivou osobou

→ Potvrdená

Hypotéza 2:

- Únik údajov chybou používateľa

→ Zamietnutá

Hypotéza 3:

- Technická chyba platformy

→ Zamietnutá

ZÁVER

- Bola potvrdená kompromitácia účtu
- Neoprávnený prístup z notebooku podozrivej osoby
- Nájdene dôkazy:
 - história prehliadača
 - cookies a session token
 - uložené prihlasovacie údaje
 - e-mail o zmene hesla
- Aktivita bola vykonaná úmyselne
- Pokus o zahľadenie stôp (vymazané dáta)

Konečný záver:

- Účet bol zneužitý podozrivou osobou

ĎAKUJEM ZA POZORNOSŤ

Priestor pre otázky

