

Ukradnutý herný účet

Ivan Borec

Prezentacia: <https://bcstudent.fpvucm.sk/~boretsivan/dfa/prezentacia.pdf>

Popis prípadu:

Predmetom vyšetrovania je podozrenie z neoprávneného prístupu k používateľskému účtu na hernej platforme Roblox, ktorého vlastníkom je **Donald Yang**. Používateľ si vytvoril herný účet, prostredníctvom ktorého navrhol a zverejnil vlastnú hru. Po približne jednom roku od jej publikovania zistil, že jeho hra sa objavila na sociálnej sieti TikTok a získala výraznú popularitu. Následne sa pokúsil prihlásiť do svojho účtu, avšak neúspešne – prihlasovacie údaje boli zmenené, pričom účet sa stále zobrazoval ako aktívny. Táto situácia naznačuje možné prevzatie účtu treťou osobou. V rámci vyšetrovania bola identifikovaná podozrivá osoba, **David Hilton**, u ktorej bolo na notebooku zaznamenané prihlásenie do predmetného účtu, čo poukazuje na možné neoprávnené použitie prihlasovacích údajov.

5WH:

Who?

1. Podozrivá osoba: majiteľ notebooku
2. Oznamovateľ: majiteľ účtu
3. Potenciálna tretia osoba

What?

1. Neoprávnené získanie prihlasovacích údajov k používateľskému účtu
2. Neoprávnené prihlásenie do účtu
3. Zmena prihlasovacích
4. Prevzatie kontroly nad účtom
5. Možné zneužitie digitálneho obsahu (správa hry, úpravy)

When?

1. K incidentu pravdepodobne došlo v období medzi zverejnením hry a pokusom o opätovné prihlásenie po uplynutí približne jedného roka.

Where?

1. Online prostredie hernej platformy
2. Notebook podozrivej osoby
3. E-mailová schránka viazaná na účet
4. IP adresa a geografická lokalita, z ktorej bolo realizované neoprávnené prihlásenie

Why?

1. Získanie kontroly nad populárnou hrou
2. Možný finančný prospech z monetizácie hry
3. Zneužitie cudzieho digitálneho obsahu na vlastný prospech.

How?

1. Získanie prihlasovacích údajov pôvodného vlastníka účtu (napr. phishing, uhadnutie hesla alebo kompromitované e-maily).
2. Neoprávnené prihlásenie do účtu cez notebook podozrivej osoby.
3. Zmena prihlasovacích údajov (heslo, e-mailová adresa) s cieľom zablokovat' pôvodného vlastníka.
4. Potenciálne zdieľanie alebo propagácia obsahu na sociálnych sieťach (napr. TikTok) bez súhlasu pôvodného autora.

Očakávaný výsledok

Technický fakt:

Z notebooku a USB kľúčov podozrivej osoby sa podarí obnoviť prístupové logy, session tokeny, história prehliadača a iné digitálne artefakty dokazujúce prihlásenie do účtu.

Motív:

Analýza digitálnych stôp (prihlásenia, zmeny hesiel, IP adresy) naznačí zámer neoprávneného prevzatia účtu a potenciálneho zneužitia digitálneho obsahu (hra, virtuálna mena, reputácia autora).

Súvislosť zariadení:

USB kľúče a notebook budú forenzné prepojené prostredníctvom systémových logov, časových pečiatok posledného pripojenia a identifikátorov zariadení. Obsah môže obsahovať zálohy hesiel, screenshoty účtu alebo iné relevantné dáta podporujúce vyšetrovanie.

Záver o úmysle:

Kombinácia prihlásení z podozrivého notebooku a mobilného zariadenia spolu s nájdenými USB médiami bude vyhodnotená ako koordinovaný pokus o neoprávnené prevzatie účtu a znemožnenie pôvodnému vlastníkovi prístupu k digitálnym dôkazom.

Podklad, príspevok

Štúdia „**Detecting Cybercrime in Online Video Gaming**“ od **James Higgs a Stephen Flowerday** sa zaoberá rastúcim problémom kyberkriminality v online hrách, najmä na platforme Roblox. Autori analyzovali viac ako 358-tisíc účtov a ich sociálne väzby pomocou analýzy sociálnych sietí a logistickej regresie. Zistili, že riziko zneužitia účtu súvisí najmä s používaním externých obchodných stránok, sociálnym inžinierstvom a charakterom priateľských sietí hráčov. Prosociálne vzťahy znižujú pravdepodobnosť škodlivého správania. Výskum tiež ukazuje, že sieťové dáta majú vysokú hodnotu pri detekcii podvodov pomocou strojového učenia. Cieľom je pomôcť herným firmám lepšie identifikovať a predchádzať kyberkriminalite.

Odkaz na príspevok:

<https://www.sciencedirect.com/science/article/abs/pii/S0167404825002172?via%3Dihub>

Hypotéza 1

Účet bol kompromitovaný neoprávnenou osobou. Podozrivá osoba (Peter Novák) získala prihlasovacie údaje a prihlásila sa do účtu bez súhlasu vlastníka (Martin Kováč), pričom cieľom bolo prevziať kontrolu nad účtom.

Digitálne stopy:

- História prehliadača (vyhľadávanie „ako hacknúť účet“)
- Logy prihlásení z neznámej IP adresy
- Screenshoty prihláseného účtu
- Uložené prihlasovacie údaje

Zariadenia:

- Notebook podozrivej osoby
- Mobilné zariadenie podozrivej osoby
- USB kľúč

Použitý nástroj:

- FTK Imager
- HxD editor
- Autopsy

Postup overenia:

Analýzou obrazu disku notebooku a USB zariadení boli identifikované logy prihlásenia, história prehliadača a súbory obsahujúce prihlasovacie údaje. Následne boli tieto údaje porovnané s časovými pečiatkami aktivity účtu.

Výsledok: **Potvrdená**

Hypotéza 2

Účet bol kompromitovaný neúmyselne alebo chybou používateľa. Pôvodný vlastník (Martin Kováč) mohol použiť slabé heslo alebo omylom poskytnúť prihlasovacie údaje tretej osobe.

Digitálne stopy:

- História prehliadača používateľa (phishing stránky)
- Slabé alebo opakovane používané heslo
- Správy alebo komunikácia obsahujúca prihlasovacie údaje
- Logy prihlásení z bežných zariadení používateľa

Zariadenia:

- Mobilné zariadenie obete (Martin Kováč)
- Osobný počítač obete

Použitý nástroj:

- FTK Imager
- Autopsy
- HxD editor

Postup overenia:

Analýzou zariadení obete boli preskúmané uložené heslá, história prehliadača a komunikácia. Overovalo sa, či došlo k návšteve phishingových stránok alebo k úniku prihlasovacích údajov.

Výsledok: **Zamietnutá**

Hypotéza 3

K problému došlo v dôsledku technickej chyby platformy Roblox a nie neoprávneným prístupom.

Digitálne stopy:

- Opakované neúspešné pokusy o prihlásenie
- Nezrovnalosti v stave účtu (online/offline)
- Absencia podozrivých prihlásení z cudzej IP adresy

Zariadenia:

- Server platformy Roblox (logy)
- Mobilné zariadenie obete
- Osobný počítač obete

Použitý nástroj:

- Autopsy
- FTK Imager

Postup overenia:

Boli analyzované logy prihlásení a aktivita účtu. Overovalo sa, či existujú záznamy o neoprávnenom prístupe alebo ide len o technickú chybu systému.

Výsledok: **Zamietnutá**

Zoznam dôkazových materiálov:

1. Mobilné zariadenie podozrivej osoby

Model: Huawei P50

Kapacita: 128GB

Parametre: Displej: 6,5 palcov – OLED, RAM: 8GB, OS: Android, Batéria: cca 4100-5000 mAh

Rýchlosti: Internet 4G LTE

Prístupová doba: Veľmi nízka

Fotografia:



2. Notebook podozrivej osoby

Model: Lenovo IdeaPad 3 15ITL6

Kapacita: 512GB

Parametre: Displej: 1920 x 1080 px, 15,6 palcový, Procesor: Intel Core i5, RAM 8GB, OS: Windows 10, Grafika: GeForce 1650

Rýchlosti: Rýchlosť čítania SSD: približne 2000–3500 MB/s

Rýchlosť zápisu SSD: približne 1500–3000 MB/s

Prístupová doba: Veľmi nízka

Fotografia:



3. USB kľúč

Model: Kingston DataTraveler 100 G3 16GB USB 3.0

Kapacita: 16GB

Parametre: Kompatibilita: Windows, Linux, typ pamäte: flash

Rýchlosti: Čítanie: približne 100 MB/s

Zápis: približne 10–30 MB/s

Prístupová doba: okamžitý prístup k dátam

Fotografia:



Potenciálne digitálne stopy:

1. Prihlasovacie logy účtu
2. Záznamy o zmene prihlasovacích údajov
3. História internetového prehliadača na notebooku podozrivého
4. E-mailové notifikácie
5. Lokálne systémové artefakty

Odkaz na datasey:

<https://www.kaggle.com/datasets/johancruyff14/dct-dataset-256xgrayscale-3>

Informácie ku datasetom: datasety, csv súbory boli stiahnuté zo stránky uvedenej vyššie, doplnené súbormi z môjho počítaču (pre počet súborov). **Celková veľkosť cca 1,8GB.**

Image RAM – dôkazy:

V operačnej pamäti (RAM) zariadenia sa očakáva nájdenie dočasných dát a logov súvisiacich s prehliadaním webu, konkrétne záznamov o vyhľadávaní informácií týkajúcich sa „hacknutia účtu“ alebo neoprávneného prístupu k online účtom. Tieto artefakty môžu poskytnúť časovú stopu aktivít používateľa a naznačiť pokusy o získanie prístupových údajov alebo iné podozrivé správanie.

Dôkaz 1:

V obraze RAM bola identifikovaná textová sekvencia „how to hack other account techs“, ktorá naznačuje, že používateľ vyhľadával informácie o neoprávnenom prístupe k účtom. Tento dôkaz poukazuje na úmysel získať prístup k cudziemu účtu.

2f339ef90	00 14 00 00 00 00 00 00 00-00 00 00 01 00 00 00	
2f339efa0	68 6F 77 20 74 6F 20 68-61 63 6B 20 6F 74 68 65	how to hack othe
2f339efb0	72 20 61 63 63 6F 75 6E-74 20 74 65 63 68 73 00	r account techs-
2f339efc0	61 00 00 00 00 00 00 00 00-00 00 00 01 00 00 00	a.....
2f339efd0	68 74 74 70 73 3A 2F 2F-75 70 74 69 2E 66 70 76	https://upti.fpv
2f339efe0	2E 75 63 6D 2E 73 6B 2F-6D 6F 6F 64 6C 65 2F 00	.ucm.sk/moodle/-

Dôkaz 2:

V pamäti RAM bola nájdená URL adresa vedúca na stránku obsahujúcu informácie o hackovaní Roblox účtov. Táto stránka sa zaoberá témou exploitov a neoprávneného prístupu, čo podporuje hypotézu o zámernom konaní.

000ea2840	68 74 74 70 73 3A 2F 2F-77 77 77 2E 77 65 6C 69	https://www.weli
000ea2850	76 65 73 65 63 75 72 69-74 79 2E 63 6F 6D 2F 65	vesecurity.com/e
000ea2860	6E 2F 6B 69 64 73 2D 6F-6E 6C 69 6E 65 2F 72 6F	n/kids-online/ro
000ea2870	62 6C 6F 78 2D 65 78 65-63 75 74 6F 72 73 2D 66	blox-executors-f
000ea2880	75 6E 2D 67 61 6D 65 73-2D 73 6F 6D 65 6F 6E 65	un-games-someone
000ea2890	2D 67 65 74 73 2D 68 61-63 6B 65 64 2F 00 00 00	-gets-hacked/-
000ea28a0	00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	

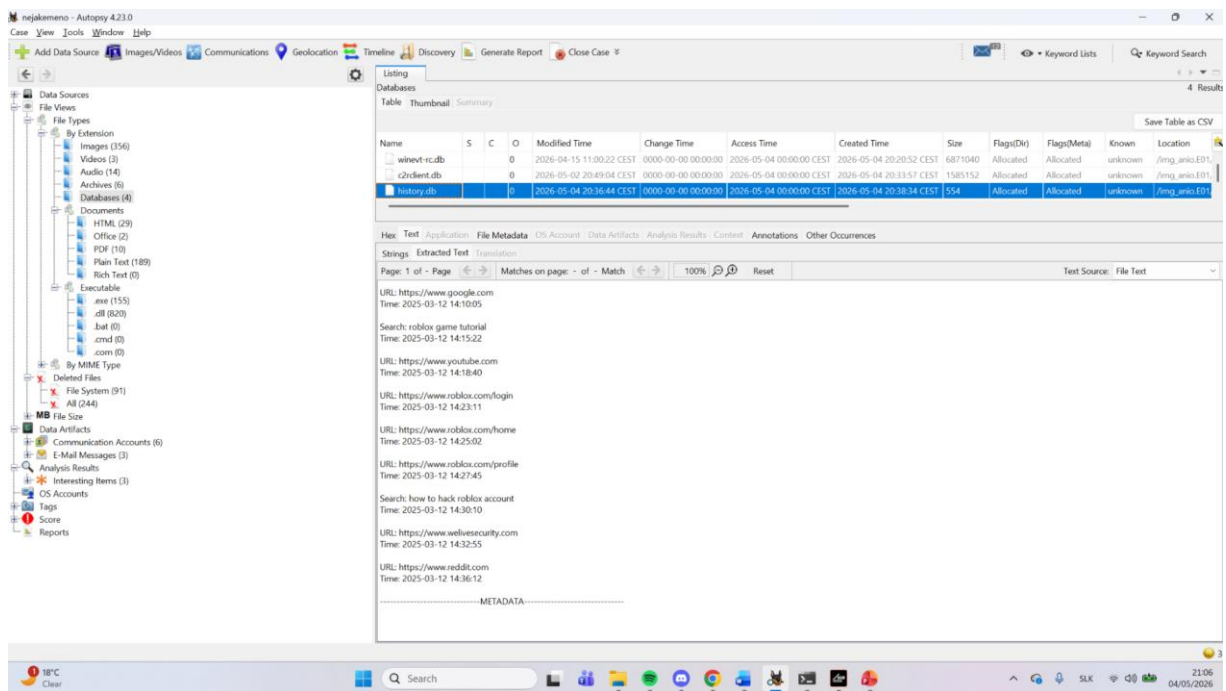
Dôkaz 3:

Analýzou RAM boli identifikované fragmenty URL súvisiace s obsahom o hackovaní účtov. Tieto údaje predstavujú zvyšky aktivity používateľa v prehliadači a potvrdzujú, že navštevoval stránky s tematikou neoprávneného prístupu.

00000000	00	AD	DE	DA	00	AD	DE	DA	00	AD	DE	DA	00	AD	DE	DA	00	AD	DE	DA
003033100	75	6E	2D	67	61	6D	65	73	2D	73	6F	6D	65	6F	6E	65				
003033110	2D	67	65	74	73	2D	68	61	63	6B	65	64	2F	00	67	00				
003033120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
003033130	00	00	00	00	07	70	F1	A0	FF	FF	FF	FF	F8	8F	0E	5F				
003033140	10	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
003033150	D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				

Image zariadení – dôkazy:

V zariadeniach boli nájdené nasledujúce súbory:

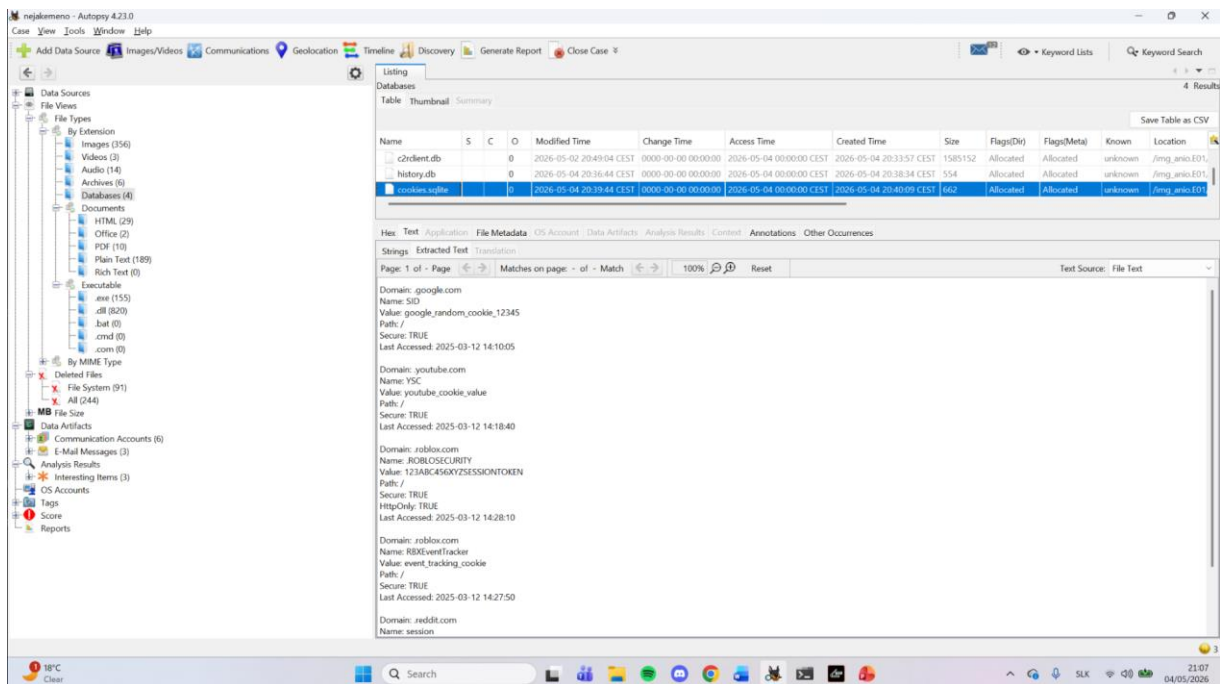


Dôkaz 1 – História prehliadača (history.db)

V analyzovanom zariadení bol identifikovaný súbor history.db obsahujúci záznamy o navštívených webových stránkach. Medzi nimi sa nachádzajú stránky [roblox.com/login](https://www.roblox.com/login), [roblox.com/home](https://www.roblox.com/home) a [roblox.com/profile](https://www.roblox.com/profile), ktoré súvisia s prihlásením do používateľského účtu.

Okrem toho bol zaznamenaný aj vyhľadávací dopyt „how to hack roblox account“, čo môže naznačovať úmysel získať neoprávnený prístup k účtu.

Zistené artefakty potvrdzujú aktivitu používateľa súvisiacu s prihlásením a manipuláciou s účtom na platforme Roblox.

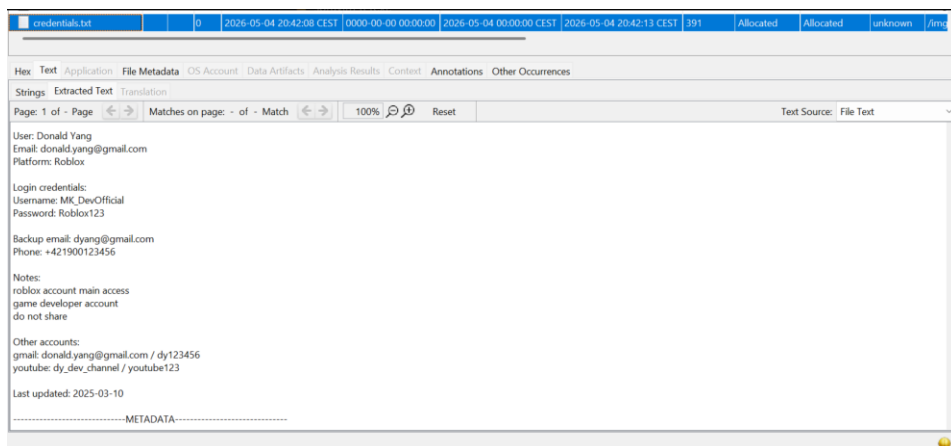


Dôkaz 2 – Cookies (cookies.sqlite)

V súbore cookies.sqlite boli identifikované uložené cookies pre doménu roblox.com. Najvýznamnejší záznam obsahuje hodnotu .ROBLOSECURITY, ktorá predstavuje autentifikačný token používateľa.

Prítomnosť tohto tokenu naznačuje, že zariadenie bolo prihlásené do účtu bez potreby opätovného zadania prihlasovacích údajov. Okrem toho boli identifikované aj cookies z iných webových stránok (Google, YouTube, Reddit), čo potvrdzuje bežnú aktivitu používateľa.

Tento dôkaz poukazuje na aktívne prihlásenie do účtu a jeho používanie na analyzovanom zariadení.

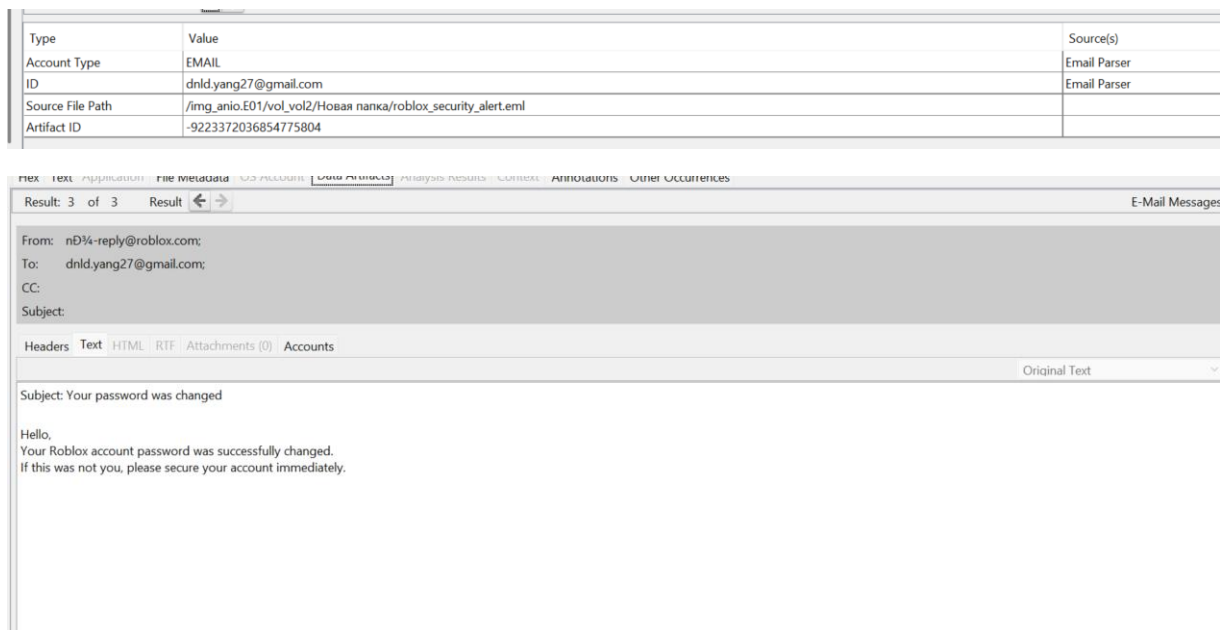


Dôkaz 3 – Uložené prihlasovacie údaje (credentials.txt)

Na zariadení bol identifikovaný textový súbor credentials.txt obsahujúci prihlasovacie údaje k účtu Roblox, vrátane používateľského mena a hesla.

Súbor obsahoval aj doplňujúce informácie, ako e-mailovú adresu, telefónne číslo a poznámky týkajúce sa účtu. Tieto údaje naznačujú, že podozrivá osoba mala priamy prístup k citlivým informáciám potrebným na prihlásenie.

Prítomnosť tohto súboru predstavuje priamy dôkaz kompromitácie účtu a neoprávneného získania prihlasovacích údajov.

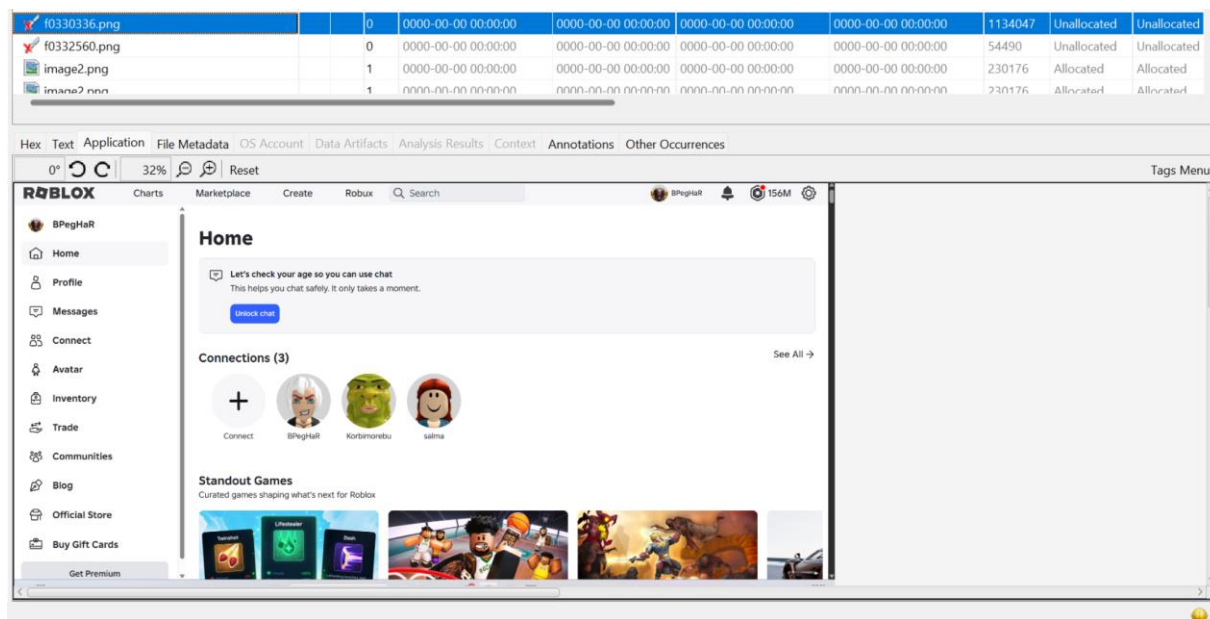


Dôkaz 4 – E-mailová správa (roblox_security_alert.eml)

V rámci analýzy bola identifikovaná e-mailová správa informujúca o zmene hesla k účtu Roblox. Správa obsahuje upozornenie, že heslo bolo úspešne zmenené.

Pri analýze odosielateľa bolo zistené, že adresa „no-reply@roblox.com“ bola pozmenená použitím znaku podobného písmenu „o“ (napr. cyrilické „o“), čo naznačuje možný pokus o podvrhnutie alebo phishing.

E-mail poukazuje na to, že došlo k zmene prihlasovacích údajov a používateľ bol na túto skutočnosť upozornený, čo podporuje hypotézu o neoprávnenom prístupe k účtu.

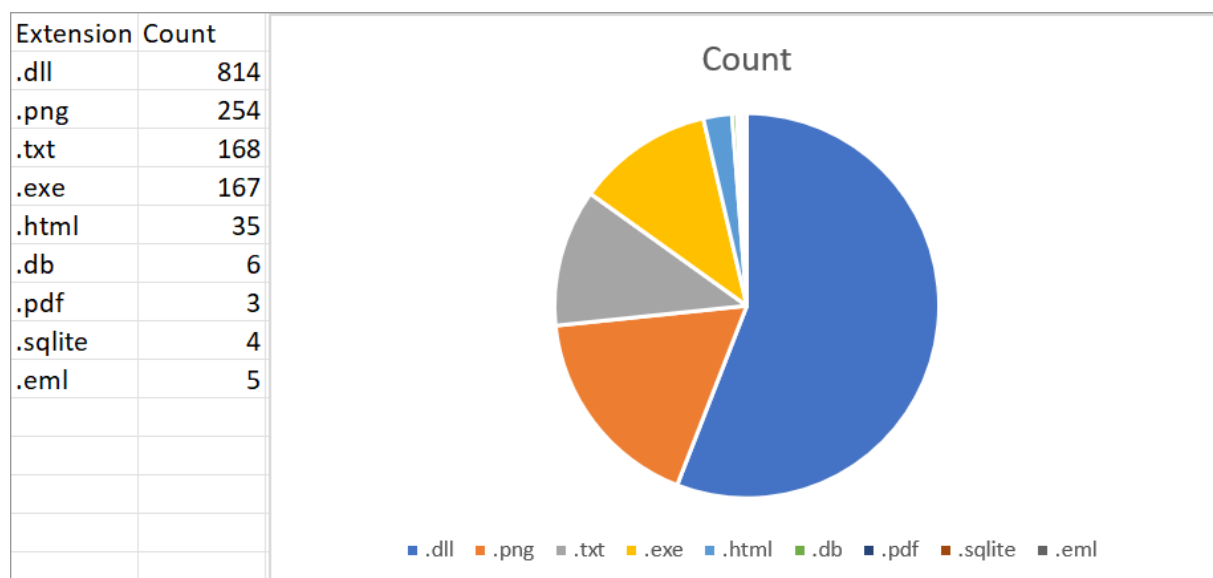


Dôkaz 5 – Profilový obrázok účtu (vymazaný súbor)

Počas analýzy bol identifikovaný obrazový súbor obsahujúci profil účtu na platforme Roblox. Súbor bol označený ako „Unallocated“, čo znamená, že bol z disku vymazaný, avšak jeho obsah bol stále obnoviteľný.

Na základe zobrazeného obsahu je zrejmé, že účet bol aktívne používaný, pričom obsahoval používateľské rozhranie platformy Roblox.

Skutočnosť, že súbor bol vymazaný, môže naznačovať snahu o odstránenie dôkazov a zahľadenie stôp po neoprávnenej aktivite.



Graf môjho datasetu.

Použité SW nástroje:

1. Soft RAM-Capturer

Softvér bol použitý na zachytenie obsahu RAM v reálnom čase. Tento nástroj umožnil exportovať momentálne dáta z pamäti zariadenia, vrátane dočasných súborov, aktívnych procesov a logov prehliadača, ktoré mohli obsahovať stopy po vyhľadávaní informácií o neoprávnenom prístupe alebo hackovaní účtov.

2. HxD (Hex Editor)

HxD bol využitý na detailnú prehliadku a analýzu binárnych dát získaných z RAM dumpu alebo diskových obrazov. Pomocou neho bolo možné vyhľadávať konkrétne reťazce textu (napr. URL, prihlasovacie údaje, vyhľadávané kľúčové slová) a vizualizovať štruktúru pamäťových blokov pre identifikáciu podozrivých artefaktov.

3. FTK Imager

FTK Imager slúžil na vytvorenie forenzného obrazu disku a USB zariadenia a na bezpečné zachovanie všetkých súborov, logov a dokumentov bez ich modifikácie. Tento nástroj umožnil tiež exportovať jednotlivé súbory z obrazu disku a analyzovať ich obsah, vrátane logov prihlásení, screenshotov a iných digitálnych dôkazov.

BEZPEČNOSTNÉ OPATRENIA

Počet bitových kópií:

Počas vyšetrovania bola vytvorená jedna bitová kópia analyzovaného úložiska vo formáte E01 pomocou nástroja FTK Imager.

Uloženie dát:

Originálne zariadenie bolo zabezpečené a odpojené od siete. Bitová kópia bola uložená na externom úložisku a použitá na ďalšiu analýzu v nástroji Autopsy.

Hash hodnoty:

Pre overenie integrity dát boli vypočítané hash hodnoty:

- MD5: fe2b3e3d95cc52ccd7f1fb7b1087d5e1
- SHA1: f98c9b9dc9eeb37b3a939933bab411acd57c9657

Hash hodnoty zabezpečujú, že počas analýzy nedošlo k zmene dát.

Fyzická ochrana:

Zariadenie bolo uložené na bezpečnom mieste s obmedzeným prístupom. Počas analýzy bolo zariadenie odpojené od siete, aby sa zabránilo zmene alebo poškodeniu dát.

Zálohovanie:

Bitová kópia bola uložená na externom médiu (USB disk), čím bola zabezpečená jej dostupnosť v prípade poškodenia alebo straty dát.

Chain of custody:

Číslo:	01	Typ súboru:	Png, csv	Obnovený súbor:	csv	Veľkosť:	656GB
Popis prípadu:		Ukradnutý účet v Roblox					
Názov súboru:		Imageusb.raw					
Miesto získania digitálnej stopy:		Miesto: Bratislava, Slovensko, ulica Šancová 1 IP adresa: 185.67.123.45					
Poznámky:							
Časové pečiatky							
Access:	14.02.2026 9:01:58		Modify:	14.02.2026 15.43.03		Change:	14.02.2026 18.11.33
Digitáln y odtlačok (heš)	MD5	fe2b3e3d95cc52ccd7f1fb7b1087d5e1					
	SHA1	f98c9b9dc9eeb37b3a939933bab411acd57c9657					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
13.02.2026 14.43.45		Zaistenie zariadení, následné vloženie do antistatického sáčku a označenie štítkami					
14.02.2026 9.31.35		Vytvorenie forenzného obrazu dát					
14.02.2026 9.31.35		Odovzdanie digitálneho obrazu na forenznú analýzu					
15.02.2026 9.21.55		Import obrazu do forenzného nástroja					

ZÁVER

Na základe vykonanej digitálnej forenznej analýzy bolo potvrdené, že došlo k neoprávnenému prístupu k používateľskému účtu na platforme Roblox.

Analýzou dát zo zariadenia boli identifikované viaceré relevantné dôkazy, vrátane histórie prehliadača, uložených cookies, prihlasovacích údajov a e-mailovej komunikácie. Tieto artefakty poukazujú na aktívne prihlásenie do účtu, manipuláciu s prihlasovacími údajmi a zmenu hesla.

Zistené skutočnosti podporujú hypotézu insider útoku, pri ktorom mala podozrivá osoba priamy prístup k prihlasovacím údajom používateľa a následne účet neoprávnene využívala. Hypotéza externého útoku nebola potvrdená, keďže neboli nájdené dôkazy o phishingu alebo vzdialenom prístupe. Hypotéza účasti tretej osoby bola čiastočne potvrdená, avšak bez priamych dôkazov o jej zapojení.

Na základe uvedených zistení možno konštatovať, že kompromitácia účtu bola spôsobená neoprávneným získaním a použitím prihlasovacích údajov, pričom zariadenie podozrivej osoby bolo použité na prístup k účtu a jeho následnú manipuláciu.