



UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

9. Základy reverznej analýzy kódu v OS Windows

Architektúra Windows

- **Segregácia procesov a ochrana pamäte:**
 - Základ stability moderných OS (Windows NT rodina).
- **User Mode (Ring 3) - Obmedzený režim:**
 - Bežné aplikácie (Word, Chrome) a 95% malvéru.
 - Izolovaný virtuálny adresný priestor (VAS). Pre 32-bitové (x86) procesy štandardne 2GB (až do 4GB s LAA), pre moderné 64-bitové (x64) procesy (Win10/11) až 128 TB pre User Mode.
 - Žiadny priamy prístup k fyzickému hardvéru alebo pamäti iných procesov (bez API volaní).
 - Pád aplikácie nespôsobí pád systému.
- **Kernel Mode (Ring 0) - Privilegovaný režim:**
 - Vykonáva sa tu kód jadra (`ntoskrnl.exe`), ovládače zariadení (`.sys`) a HAL (Hardware Abstraction Layer).
 - Zdieľaný adresný priestor pre všetky komponenty jadra.
 - Priamy prístup k CPU inštrukciám a fyzickej pamäti.
 - Chyba v kóde = BSOD (Blue Screen of Death) - kritické zlyhanie systému.



Prechod medzi režimami

- **Mechanizmus prechodu (User -> Kernel):**
 - Aplikácie nemôžu priamo vykonávať privilegované operácie (čítanie súboru, alokácia pamäte). Musia požiadať OS.
- **Hierarchia volaní (Flow):**
 - Aplikácia volá **Win32 API** (napr. `CreateFile` v `kernel32.dll` - zdokumentované, User Mode).
 - Volanie prechádza do **Native API** (`NtCreateFile` v `ntdll.dll` - nezdokumentované, User Mode wrapper).
 - `ntdll.dll` naplní register EAX číslom služby (System Service Number - SSN).
 - Vykoná sa inštrukcia `syscall` (x64) alebo `sysenter` (x86), ktorá prepne CPU do Kernel Mode.
 - Jadro (`ntoskrnl.exe`) prevezme riadenie cez **SSDT (System Service Descriptor Table)** a vykoná operáciu.
- **Význam pre RE:** Malvér sa často snaží obísť Win32 API a volať priamo `syscall` (tzv. Direct Syscalls), aby obišiel User-land hooking bezpečnostných produktov.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Portable Executable (PE) Formát

- **Definícia PE:** Štandardizovaný formát pre spustiteľné súbory (**.exe**, **.dll**, **.sys**, **.efi**) na Windows.
- **Funkcia:** Slúži ako "kuchárska kniha" pre Windows Loader – inštruuje OS, ako presne načítať súbor z disku do pamäte (mapovanie).
- **Základná štruktúra:**
 - **DOS Header:** Dedičstvo pre spätnú kompatibilitu.
 - **DOS Stub:** Malý program, ktorý vypíše "This program cannot be run in DOS mode".
 - **NT Headers:** Hlavná hlavička obsahujúca **FileHeader** a **OptionalHeader**.
 - **Section Headers:** Tabuľka popisujúca jednotlivé segmenty dát (názov, veľkosť na disku vs. v pamäti, oprávnenia).
 - **Sections:** Samotné dáta (kód, obrázky, texty).



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Analýza PE Hlavičky

- **DOS Header:**
 - **e_magic:** Signatúra **"MZ"** (0x4D 0x5A) - pocta Markovi Zbikowskemu. Musí byť na začiatku súboru.
 - **e_lfanew:** Offset (adresa), kde začína NT hlavička. Kritické pre parsovanie súboru.
- **NT Headers (File Header & Optional Header):**
 - **TimeStamp:** Čas kompilácie v sekundách od roku 1970.
 - *Pozor:* Útočníci často používajú "Timestomping" (falšovanie času na minulé roky), aby súbor vyzeral legitímne. Delphi/Borland kompilátory historicky nastavovali TimeDateStamp na 1992-06-19T22:22:17 (Unix timestamp 0x2A425E19), čo zodpovedá dátumu z roku 1992.
 - **AddressOfEntryPoint (EP):** Relatívna virtuálna adresa (RVA) prvej inštrukcie. Pozor na rozdiel voči OEP (Original Entry Point), čo je analytický termín pre pôvodný začiatok kódu po jeho dynamickom rozbalení v pamäti.
 - **ImageBase:** Preferovaná adresa načítania do pamäte (štandardne 0x400000 pre 32-bit .exe, 0x140000000 pre 64-bit .exe a 0x10000000 pre staršie DLL). Dnes často ignorovaná kvôli ASLR.
 - **DllCharacteristics:** Príznaky bezpečnosti (ASLR, DEP/NX, Code Integrity).



Sekcie (Sections) a detekcia anomálií

- **Štandardné sekcie a ich účel:**
 - **.text / .code:** Obsahuje spustiteľné inštrukcie CPU. (Oprávnenia: Read, Execute).
 - **.data:** Globálne a statické premenné (inicializované). (Oprávnenia: Read, Write).
 - **.rdata:** Importy, konštanty, reťazce. (Oprávnenia: Read).
 - **.rsrc:** Zdroje (ikony, dialógy, verzie, vnorené binárne súbory).
 - **.reloc:** Relokačná tabuľka (nevyhnutná pre funkčnosť ASLR).
- **Indikátory malvéru v sekciách:**
 - **Vysoká entropia:** Ak má sekcia entropiu blízku 8.0 (náhodné dáta), indikuje to kompresiu alebo šifrovanie. Bežný kód má entropiu okolo 6.0-6.5.
 - **VirtualSize >> RawSize:** Veľkosť v pamäti je oveľa väčšia ako veľkosť na disku. Znamená to, že program si alokuje prázdne miesto, kam sa za behu rozbalí.
 - **Neštandardné názvy:** **.UPX0**, **.protect**, alebo náhodné zhlučky znakov.
 - **Oprávnenia RWX:** Sekcia, ktorá je zapisovateľná (Write) aj spustiteľná (Execute) súčasne, je obrovský "red flag". V legitímnom softvéri sa takmer nevyskytuje.



Windows API, knižnice (DLL) a importy

- **Import Address Table (IAT):** Zoznam funkcií z externých DLL, ktoré program potrebuje pre svoj beh.
- **Kľúčové DLL pre analýzu malvéru:**
 - **Kernel32.dll:** Základné operácie (súbory, pamäť, procesy, vlákna).
 - **User32.dll:** Grafické rozhranie, vstupy (klávesnica/myš), hookovanie vstupov (**SetWindowsHookEx** - keyloggery).
 - **Advapi32.dll:** Práca s Registrami, Službami a Bezpečnostnými tokenmi.
 - **Ws2_32.dll / Wininet.dll:** Nízkoúrovňová (sockety) a vysokoúrovňová (HTTP/FTP) sieťová komunikácia.
 - **Crypt32.dll:** Kryptografické API (často používané ransomvérom).
- **Techniky maskovania importov:**
 - **Import by Ordinal:** Importovanie funkcie číslom, nie názvom (sťažuje čítanie).
 - **Dynamické načítanie:** Použitie **LoadLibrary** a **GetProcAddress**. IAT je prázdna, funkcie sa hľadajú až za behu.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Mechanizmy perzistencie

- **Definícia:** Schopnosť malvéru spustiť sa automaticky po reštarte systému alebo prihlásení používateľa.
- **Registre (Registry Run Keys):**
 - **HKCU\...\Run** (Len pre aktuálneho používateľa - nevyžaduje admin práva).
 - **HKLM\...\Run** (Pre celý systém - vyžaduje admin práva).
 - **Winlogon Helper / Userinit:** Pripojenie k procesu **explorer.exe** alebo **winlogon.exe**.
 - **IFEO (Image File Execution Options):** Pôvodne pre ladenie. Útočník nastaví kľúč "Debugger" pre **osk.exe** (klávesnica na obrazovke) na cestu k malvéru. Spustenie OSK spustí malvér.
- **Služby (Windows Services):**
 - Spustenie pred prihlásením používateľa (System level).
 - Často maskované názvami podobnými legitímnym službám (napr. "Windows Update Helper").
- **Naplánované úlohy (Scheduled Tasks):**
 - Flexibilné spúšťanie (časovač, nečinnosť, štart systému).
 - Možnosť spúšťať úlohy pod systémovým účtom.



DLL a Search Order Hijacking (Sideloading)

- **Princíp:** Zneužitie deterministického poradia, v akom Windows loader hľadá DLL knižnice, ak nie je zadaná plná cesta.
- **Moderné (bezpečné) poradie je:**
 - Adresár aplikácie.
 - Systémový adresár (System32).
 - 16-bit systémový adresár.
 - Windows adresár.
 - Aktuálny pracovný adresár (CWD) - posunutý sem vďaka SafeDllSearchMode = Enabled (predvolené od Windows XP SP2)
 - PATH.
- **Vektor útoku:** Útočník umiestni legitímnu, digitálne podpísanú aplikáciu (napr. staršiu verziu VLC playera alebo Microsoft Teams) a škodlivú DLL s názvom, ktorý aplikácia vyžaduje (napr. `version.dll` alebo `mpsvc.dll`), do rovnakého priečinka.
- **Výsledok:** Legitímna aplikácia načíta malvér (škodlivú DLL), pretože ho nájde ako prvý (v bode 1). Malvér beží v kontexte dôveryhodného procesu.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Injekcia Kódu: Klasická a Reflective

- **Motivácia:** Maskovanie (beh pod `svchost.exe`), prístup k dátam cudzieho procesu (krádež hesiel z prehliadača), obídenie personálneho firewallu.
- **Klasická DLL Injekcia:**
 - Vyžaduje škodlivú DLL fyzicky na disku.
 - **API volania:**
 - `OpenProcess` (získanie handle cieľového procesu).
 - `VirtualAllocEx` (alokácia pamäte v cieľi).
 - `WriteProcessMemory` (zápis cesty k DLL do cieľa).
 - `CreateRemoteThread` (spustenie `LoadLibrary` s cestou k DLL).
 - **Nevýhoda:** Ľahko detegovateľné, súbor na disku.
- **Reflective DLL Injection:**
 - Načíta DLL priamo z pamäte (bez súboru na disku - Fileless).
 - DLL musí byť špeciálne upravená – obsahuje **Reflective Loader**.
 - **Proces:** Loader sám nájde svoju adresu v pamäti, vyrieši importy, aplikuje relokácie a zavolá `DllMain`.
 - Využívané nástrojmi ako Cobalt Strike alebo Metasploit (Meterpreter).



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Process Hollowing a Doppelganging

- **Process Hollowing (RunPE):**
 - Vytvorenie legitímneho procesu (napr. `svchost.exe`) v stave `SUSPENDED`.
 - Odmapovanie ("odstránenie") pôvodného legitímneho kódu (`NtUnmapViewOfSection`).
 - Alokácia pamäte a zápis škodlivého kódu na rovnakú adresu.
 - Úprava registrov vlákna (`SetThreadContext`), aby ukazovali na nový Entry Point.
 - Spustenie vlákna (`ResumeThread`).
- **Process Doppelganging:**
 - Využíva **NTFS Transakcie (TxF)**, čo je dnes už zastaraná, ale stále prítomná funkcia.
 - Kód sa zapíše do transakcie (súbor je "akože" vytvorený).
 - Z tohto transakčného súboru sa vytvorí pamäťová sekcia.
 - Transakcia sa vráti späť (Rollback).
 - **Výsledok:** Proces beží z kódu, ktorý na disku reálne nikdy neexistoval. Obchádza skenovanie súborov pri spustení.
- Moderná alternatíva z rodiny týchto útokov je Process Herpaderping, ktorá obchádza niektoré bezpečnostné mechanizmy modifikáciou súboru na disku po jeho namapovaní do pamäte, ale pred samotným spustením vlákna.



Obchádzanie Detekcie: Direct Syscalls

- **Problém (z pohľadu útočníka):** EDR/AV produkty inštalujú “hooks” na funkcie v `ntdll.dll` (v User Mode).
 - Hook je inštrukcia `JMP`, ktorá presmeruje tok programu do DLL bezpečnostného produktu.
- **Riešenie: Priame systémové volania (Direct Syscalls).**
 - Malvér si “prinesie vlastnú implementáciu” `syscall` inštrukcie v assembleri.
 - Namiesto volania `NtAllocateVirtualMemory` v `ntdll.dll`, malvér vykoná `MOV EAX, <SSN>; SYSCALL`.
 - Týmto úplne obchádza `ntdll.dll` a akékoľvek kontroly v nej.
- **Výzva:** Čísla syscallov (SSN) nie sú stabilné. Menia sa medzi verziami Windows (napr. XP, 7, 10 1903, 10 20H2, 11).



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Hell's Gate a Halo's Gate (koncept)

- **Hell's Gate:**
 - Technika na dynamické čítanie SSN priamo z pamäte `ntdll.dll` za behu.
 - Nájde exportovanú funkciu, prečíta bajty `B8 <SSN> 00 00` (čo je opkód pre `MOV EAX, SSN`).
 - **Limitácia:** Zlyháva, ak je funkcia hookovaná EDR (pretože začiatok funkcie je prepísaný inštrukciou `JMP` a pôvodné bajty tam nie sú).
- **Halo's Gate (Tartarus Gate):**
 - Vylepšenie Hell's Gate. Ak je cieľová funkcia hookovaná, skontroluje susedné funkcie (hore a dole v pamäti).
 - Využíva fakt, že SSN sú v jadre priradené sekvenčne.
 - Ak `NtFunctionX` má SSN 50, sused bude mať 49 alebo 51.
 - Odvodí správne číslo od nemodifikovanej susednej funkcie.
- **Výsledok:** Schopnosť volať funkcie jadra bez detekcie EDR aj v silne monitorovanom prostredí.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Statická analýza

- **Ghidra (NSA):** Open-source SRE Framework vyvinutý americkou NSA.
- **Hlavné funkcionality:**
 - **Dekompilátor:** Kľúčová vlastnosť. Transformuje assembler na C-like pseudokód. Výrazne urýchľuje pochopenie logiky.
 - **Program Tree:** Organizácia sekcií a segmentov.
 - **Symbol Tree:** Prehľad importov, exportov, funkcií a labelov.
 - **Function Graph:** Vizuálna reprezentácia toku programu (Control Flow Graph - CFG). Pomáha identifikovať slučky a podmienky.
 - **Skriptovanie:** Podpora Python a Java pre automatizáciu (napr. automatické premenovanie funkcií, dešifrovanie reťazcov).
- **Porovnanie:** Bezplatná alternatíva k drahému IDA Pro, hoci IDA má stále lepší dekompilátor pre C++.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Dynamická analýza

- **x64dbg:** Moderný, open-source debugger pre Windows (nástupca OllyDbg).
- **Použitie:** Analýza správania malvéru v reálnom čase, obchádzanie packerov.
- **Metodológia rozbaľovania (Manual Unpacking):**
 - Malvér sa načíta zabalený.
 - Nastavíme breakpoint na **VirtualAlloc** (pretože malvér musí alokovať pamäť pre rozbalený kód).
 - Sledujeme alokovanú oblasť v "Memory Map".
 - Nastavíme Hardware Breakpoint na vykonanie (Execute) v tejto novej pamäti. Keď packer dokončí dešifrovanie a odovzdá riadenie pôvodnému programu (skok na OEP), debugger sa tam zastaví.
 - Použijeme plugin **Scylla** na dumpnutie procesu z pamäte na disk a opravu IAT.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Pamäťová forenzka

- **Volatility:** Štandard pre analýzu RAM dumpov (snímkov operačnej pamäte).
- **Kľúčové pluginy pre Windows:**
 - **pslist** vs. **psscan**: **pslist** číta zoznam procesov tak, ako ho vidí OS. **psscan** skenuje pamäť a hľadá štruktúry **EPROCESS**. Rozdiel indikuje **DKOM** (Direct Kernel Object Manipulation) rootkit.
 - **malfind**: Skenuje pamäť procesov a hľadá VAD (Virtual Address Descriptor) uzly, ktoré sú RWX (Read-Write-Execute) a obsahujú MZ hlavičku. Indikuje injektovaný kód.
 - **netscan**: Zobrazuje aktívne a ukončené sieťové pripojenia, otvorené porty a priradené procesy.
 - **cmdline**: Zobrazuje argumenty príkazového riadku (často prezradia zámery PowerShell skriptov).
- Dôležité upozornenie: pri Volatility 3 došlo k zmene syntaxe. Napríklad, vo Volatility 3 sa príkaz volá **windows.pslist.PsList**, **windows.malfind.Malfind** alebo **windows.netscan.NetScan**.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Záver

- **Zhrnutie:** Úspešná analýza nie je o jednom nástroji, ale o kombinácii prístupov.
 - Statická (Ghidra/IDA) pre pochopenie "veľkého obrazu".
 - Dynamická (x64dbg) pre detailné správanie a dešifrovanie.
 - Forezná (Volatility) pre analýzu artefaktov v pamäti.
- **Trendy do budúcnosti:**
 - **Obchádzanie EDR:** Masívne nasadenie Direct Syscalls a Call Stack Spoofing.
 - **Fileless techniky:** Útoky, ktoré využijú disk len minimálne (PowerShell, .NET assemblies v pamäti).
 - **Cross-platform malvér:** Rast malvéru v jazykoch ako Go a Rust (GoLang malvér je extrémne ťažké analyzovať kvôli veľkosti a štruktúre binárky).
 - **AI v ofenzíve aj defenzíve:** Generovanie polymorfného kódu pomocou AI.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY





UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť.