KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

5. Dynamická analýza strojového kódu

Úvod do dynamickej analýzy

- **Statická analýza (Code Analysis):**
  - *Nástroje:* Disassemblery a dekompilátory (IDA Pro, Ghidra, Binary Ninja, Radare2).
  - *Limitácie:* Moderný malvér používa obfuskáciu (napr. OLLVM), "packing" (UPX, custom packery) a dynamické načítanie API (dlopen/dlsym), čo robí statický kód nečitateľným.
  - *Využitie:* Identifikácia kryptografických konštánt, štruktúry funkcií a základných reťazcov.
- **Dynamická analýza (Behavioral Analysis):**
  - *Definícia:* Pozorovanie interakcie programu s operačným systémom a sieťou v reálnom čase.
  - *Princíp "Black Box":* Spustiť vzorku v kontrolovanom prostredí a zaznamenávať všetky vstupy a výstupy (I/O).
  - *Kľúčová výhoda:* Odhalenie skutočného zámeru (payloadu) až po tom, čo sa malvér sám rozbalí v pamäti (Self-modifying code).
- **Výstupy analýzy:**
  - **IoCs (Indicators of Compromise):** IP adresy C2 serverov, hashe súborov, mutexy, cesty k súborom.
  - **TTPs (Tactics, Techniques, and Procedures):** Ako sa útočník pohybuje v sieti, ako eskaluje privilégiá a ako exfiltruje dáta (MITRE ATT&CK framework).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Architektúra bezpečného prostredia

- **Izolácia je kľúčová:**
  - Zabránenie úniku ("leak") malvéru do produkčnej siete (Host-Only networking, VLAN izolácia).
  - Ochrana integrity hostiteľského systému.
- **Virtualizácia (Hardware-Assisted):**
  - *Technológie:* KVM (Kernel-based Virtual Machine), Xen, VirtualBox, VMware.
  - *Výhody:* Vysoký výkon, priame využitie CPU (Intel VT-x / AMD-V).
  - *Nevýhody:* Zanecháva stopy (artefakty), ktoré malvér ľahko deteguje (špecifické inštrukcie CPU, I/O porty, názvy zariadení PCI).
- **Emulácia (Software-Based):**
  - *Nástroj:* QEMU (Quick Emulator).
  - *Princíp:* Kompletná softvérová simulácia hardvéru (CPU, RAM, chipset).
  - *Cross-architecture analýza:* Umožňuje analyzovať IoT malvér (architektúra MIPS, ARM) na bežnom x86 počítači.
  - *Nevýhody:* Výrazne pomalšie vykonávanie, náchylnosť na "timing attacks" (malvér zmeria čas vykonania inštrukcie a zistí, že beží príliš pomaly).
- **Bare-metal Sandbox:**
  - Analýza na fyzickom hardvéri (reštartovanie a obnova disku cez PXE/IPMI).
  - Najvyššia úroveň utajenia (stealth), ale náročné na správu a škálovanie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Automatizované analytické systémy

- **Cuckoo Sandbox:**
  - Dlhoročný priemyselný štandard pre automatizáciu - v súčasnosti nová verzia Cuckoo 3 (kompletná revízia).
  - *Architektúra:* Host (riadiaci server) + Guests (infikované VM).
  - *Metóda:* Injektuje monitorovací agent (zvyčajne DLL vo Windows, `.so` knižnice v Linuxe) do procesu malvéru.
- **CAPEv2 (Config And Payload Extraction) - de facto open-source štandard - v komunite nahradil Cuckoo:**
  - Pokročilý fork Cuckoo zameraný na extrakciu obsahu z pamäte.
  - *Memory Forensics:* Automaticky deteguje moment rozbalenia malvéru a vytvorí "dump" procesu.
  - *YARA integrácia:* Skenuje pamäťové stránky pomocou YARA pravidiel na identifikáciu rodiny malvéru.
  - *Debugger integrácia:* Dokáže dynamicky ovládať debugger pre obídenie jednoduchých anti-analytických trikov.
- **LiSa (Linux Sandbox):**
  - Špecializované riešenie pre Linux a IoT (ELF binárky).
  - *Kernel Instrumentation:* Namiesto user-space hook-ov využíva SystemTap pre inštrumentáciu priamo v jadre, čo je ťažšie detegovateľné.
  - Analyzuje systémové volania, sieťovú prevádzku a súborové operácie.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

"Stealth" analýza a VMI

- **Agentless Analysis (Bezagentová analýza):**
  - V cieľovom systéme (Guest OS) nebeží žiaden analytický softvér.
  - Eliminuje riziko detekcie agenta malvérom.
- **VMI (Virtual Machine Introspection):**
  - Sledovanie stavu virtuálneho stroja "zvonku", priamo z úrovne hypervízora (zvyčajne Xen).
  - Analytik vidí do pamäte virtuálneho stroja, ale virtuálny stroj nevidí analytika.
- **Technológia Drakvuf:**
  - *EPT (Extended Page Tables):* Využíva hardvérovú virtualizáciu pamäte na nastavenie pascí (traps) na špecifické stránky pamäte.
  - *Breakpoint Injection:* Vkladá breakpointy priamo do inštrukčného toku bez modifikácie jadra hostiteľského PC.
  - *Rekonštrukcia OS:* Používa LibVMI na preklad surových pamäťových adries na sémantické štruktúry OS (zoznam procesov, otvorené súbory).
- **Výhoda:** Takmer nemožné detegovať z user-space ani kernel-space malvéru (Blue Pill vs. Red Pill koncept).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Simulácia sieťových služieb (INetSim)

- **Problém konektivity:**
  - Malvér potrebuje internet (C2 príkazy, stiahnutie payloadu).
  - Povolenie plného prístupu je rizikové (útok na iné ciele, prezradenie IP adresy laboratória).
  - Úplné odpojenie spôsobí, že malvér nevykoná svoju činnosť.
- **Riešenie: INetSim (Internet Simulation):**
  - Softvér simulujúci bežné internetové služby na lokálnom rozhraní.
- **Kľúčové funkcionality:**
  - **Fake DNS:** Odpovedá na všetky DNS dopyty (napr. `evil.com`) svojou vlastnou IP adresou.
  - **HTTP/HTTPS Server:** Simuluje webové servery. Vráti preddefinovaný obsah alebo falošné súbory pri požiadavke GET.
  - **Service Simulation:** SMTP, FTP, POP3, TFTP, IRC (často používané botnetmi).
  - **Dummy Payload:** Keď malvér požiada o stiahnutie "ransomware.exe", INetSim mu podstrčí neškodnú binárku, aby proces pokračoval.
- **Logging:** Detailný záznam požiadaviek vrátane hlavičiek a payloadov, dešifrovanie SSL (ak je nainštalovaný MITM certifikát).
- **Transparent TLS Proxy** (napr. PolarProxy): Moderný prístup zachytávania HTTPS komunikácie. Umožňuje dešifrovať TLS prevádzku malvéru bez toho, aby malvér explicitne používal proxy server (zachytáva prevádzku priamo na sieťovej bráne a ukladá do PCAP formátu v plain-texte).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sledovanie systémových volaní

- **Rozhranie Kernel vs. User-space:**
  - Linux aplikácie komunikujú s hardvérom výhradne cez systémové volania (syscalls). Sledovanie tohto rozhrania odhalí 99% aktivity.
- **Nástroj `strace` (System Trace):**
  - Založený na `ptrace` API.
  - *Kľúčové prepínače:*
    - `-f`: Sledovanie všetkých vytvorených podprocesov (forks/threads).
    - `-e trace=network,file`: Filter pre zobrazenie len sieťových alebo súborových operácií.
    - `-s 2000`: Zväčšenie limitu pre výpis reťazcov (aby sme videli celé URL alebo dáta).
    - `-x`: Výpis ne-ASCII znakov v hexadecimálnom formáte.
  - *Detegované volania:* `openat` (súbory), `execve` (spúšťanie príkazov), `socket/connect` (sieť), `mmap/mprotect` (pamäť).
- **Nástroj `ltrace` (Library Trace):**
  - Sleduje volania dynamických knižníc (predtým, než sa stanú syscallmi).
  - Užitočné pre kryptografiu: `strcmp` (porovnávanie hesiel v plain-texte) alebo `SSL_write` (dáta pred zašifrovaním).
  - *Limitácia:* Nefunguje na staticky linkované binárky (časté u Go/Rust malvéru).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Dynamická binárna inštrumentácia

- **Koncept DBI:**
  - Vkladanie kódu do bežiaceho procesu a modifikácia jeho inštrukcií za behu (Runtime modification).
  - Nie je potrebný zdrojový kód ani rekompilácia.
- **Architektúra Frida:**
  - Client (Python/JS skript na PC) <-> Server (frida-server na zariadení/VM).
  - Injektuje JavaScript engine — štandardne Google V8, s alternatívou QuickJS pre resource-constrained platformy..
- **Príklady využitia v analýze:**
  - **SSL Pinning Bypass:** Hooknutie overovacích funkcií v `libssl` alebo `libcrypto` a vynútenie návratovej hodnoty `True` (valid certificate). Umožňuje odpočúvať HTTPS prevádzku cez Proxy (Burp Suite).
  - **Anti-Debug Bypass:** Hooknutie funkcie `ptrace` alebo čítania `/proc/self/status`. Keď malvér skontroluje, či je debugovaný, Frida vráti falošnú odpoveď.
  - **Memory Dumping:** Extrakcia dešifrovaných reťazcov alebo celých tried priamo z pamäte (napr. Java triedy v Android malvéri).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kernel-level Observability - eBPF

- **eBPF (extended Berkeley Packet Filter):**
  - Revolučná technológia v jadre Linuxu.
  - Umožňuje spúšťať sandboxovaný, užívateľom definovaný kód priamo v kernel space.
  - Bezpečnosť zaručená Verifierom (nedovolí poškodiť činnosť jadra).
- **Prečo eBPF pre analýzu malvéru?**
  - **Viditeľnosť:** Prístup ku kprobes (funkcie jadra), tracepoints, uprobes (funkcie aplikácií).
  - **Výkon:** Extrémne nízka réžia, spracovanie udalostí priamo v jadre bez prepínania kontextu (context switch) pre každý paket/udalosť.
  - **Stealth:** Malvér v user-space nemá priamu možnosť detegovať eBPF sondy, ak nemá root práva na inšpekciu jadra.
- **Nástroje:**
  - **bpftrace:** High-level skriptovací jazyk (podobný awk/C) pre rýchlu analýzu.
  - **BCC (BPF Compiler Collection):** Python nástroje pre komplexný monitoring (napr. `execsnoop`, `opensnoop`, `tcpconnect`).
- *Príklad:* Sledovanie všetkých spustených príkazov v systéme (aj krátkodobých) pomocou `execsnoop`, ktoré by štandardný logging nestihol zachytiť.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Evasion Techniky

- **Anti-Debugging:**
  - `ptrace(PTRACE_TRACEME, 0, 0, 0)`: Proces sa pokúsi debugovať sám seba. V Linuxe môže mať proces len jedného debuggera. Ak volanie zlyhá (-1), znamená to, že proces už niekto sleduje (napr. `strace` alebo `gdb`) -> malvér sa ukončí.
  - **Kontrola statusu:** Čítanie `/proc/self/status` a hľadanie poľa `TracerPid`. Ak je > 0, proces je sledovaný.
- **Detekcia Virtualizácie (Anti-VM):**
  - **CPUID inštrukcia:** Kontrola bitu hypervízora.
  - **Hardvérové artefakty:** Kontrola MAC adries (08:00:27 pre VirtualBox), prítomnosť súborov ovládačov (`vboxguest`, `vmtoolsd`), špecifické PCI zariadenia.
  - **I/O Porty:** VMware používa špecifické komunikačné porty ("Backdoor I/O ports"), ktoré malvér testuje.
- **Timing Attacks:**
  - `RDTSC` (Read Time-Stamp Counter): Malvér zmeria počet cyklov CPU potrebných na vykonanie bloku kódu. Vo VM je tento čas výrazne dlhší (kvôli návratu do hypervízora). Ak je rozdiel veľký, malvér deteguje VM.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Techniky perzistencie v Linuxe

- **User-space perzistencia a skrývanie:**
  - **LD_PRELOAD:** Environmentálna premenná alebo globálna konfigurácia v `/etc/ld.so.preload`.
  - *Princíp:* Núti dynamický linker načítať škodlivú knižnicu *pred* všetkými ostatnými (napr. libc).
  - *Zneužitie:* Útočník prepíše funkcie ako `readdir` (aby `ls` nevypísal súbory malvéru), `open` alebo `pam_authenticate` (univerzálne heslo).
  - Toto je základ pre tzv. **Userland Rootkity** (napr. Jynx2, Azazel).
- **Kernel-space perzistencia:**
  - **LKM (Loadable Kernel Modules):** Tradičné rootkity, vyžadujú presnú verziu jadra.
  - **eBPF Rootkity (Boopkit, TripleCross):** Moderná hrozba.
    - Nepotrebujú kompiláciu pre konkrétny kernel (CO-RE - Compile Once, Run Everywhere).
    - Hookujú syscalls ako `sys_getdents64` priamo v jadre na skrytie procesov a súborov.
    - Dokážu modifikovať sieťovú prevádzku pred firewallom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Prípadová štúdia - BPFDoor

- **Profil:** Sofistikovaný Linux backdoor, pripisovaný čínskym APT skupinám (Red Menshen), aktívny roky bez detekcie.
- **Technická analýza:**
  - **Socket Filtering:** Namiesto otvorenia TCP portu (čo by zachytil `netstat` alebo Nmap), malvér otvára **Raw Socket (`AF_PACKET`)**.
  - **cBPF / LSF (Classic BPF / Linux Socket Filtering):** Zásadný rozdiel oproti modernému eBPF. BPFDoor zneužíva historickú funkcionalitu jadra (dostupnú už desaťročia). Pripája starý BPF filter priamo na Raw Socket, čo je nenáročnejšie na privilégiá (často nevyžaduje plný root prístup, ak má CAP_NET_RAW) a obchádza tak moderné ochrany eBPF Verifiera.
  - **Magic Packet:** Backdoor sa aktivuje len vtedy, ak paket obsahuje špecifickú sekvenciu bajtov (heslo) na určitej pozícii. Ostatné pakety ignoruje a prepúšťa do systému.
- **Firewall Bypass:** Keďže používa raw socket na nižšej vrstve, často vidí pakety ešte predtým, než ich zahodí `iptables`.
- **Anti-Forensics:**
  - Preberá názvy legitímnych procesov (napr. `/sbin/udevd`, `/usr/libexec/postfix/master`).
  - **Timestomping:** Mení časové značky binárky, aby vyzerala ako starý systémový súbor.
  - Zmazanie binárky z disku ihneď po spustení (beh len v RAM - "delete self").

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Záver a budúce trendy

- **Súhrn:** Prechod od jednoduchých user-space nástrojov (`strace`) k pokročilému kernel-level monitorovaniu (`eBPF`, `Drakvuf`). Pochopenie, že malvér sa aktívne bráni.
- **Výzvy do budúcnosti:**
  - **Fileless Malware v Linuxe:** Spúšťanie kódu priamo z pamäte (`memfd_create`), bez použitia disku (+ process hollowing cez ptrace a zneužitie prctl(PR_SET_NAME)).
  - **AI-driven Malware:** Malvér, ktorý sa učí z prostredia a mení svoje správanie, aby obišiel detekciu anomálií.
  - **Supply Chain útoky:** Infekcia zostavovacích (build) pipelines a kontajnerov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť.