KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1. Úvod do štúdia reverzného inžinierstva a analýzy malvéru

Definícia a epistemológia

- **Reverzné Inžinierstvo (RE):** Systematický proces dekonštrukcie hotového artefaktu (softvéru) s cieľom odhaliť jeho vnútornú architektúru, funkčnosť a dizajn bez prístupu k pôvodnej dokumentácii.
- **Smer toku informácií:**
  - **Forward Engineering:** Myšlienka > Logika > Kód > Binárka.
  - **Reverse Engineering:** Binárka > Disassembly > Logika > Rekonštrukcia myšlienky.
- **Kľúčové oblasti využitia:**
  - **Analýza Malvéru:** Porozumenie vektorom infekcie a C2 protokolom.
  - **Incident Response:** Extrakcia IoC (Indicators of Compromise).
  - **Security Audit:** Black-box testovanie proprietárnych knižníc.
  - **Interoperabilita:** Tvorba ovládačov pre nezdokumentovaný hardvér (napr. projekt Nouveau pre NVIDIA).

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

Teoretické limity analýzy

- **Frederick B. Cohen (1984–1987):** Definoval počítačový vírus (1984) a vo svojej dizertácii (1986) a následnej publikácii (1987) predložil formálny dôkaz o nerozhodnuteľnosti detekcie počítačových vírusov.
- **Vzťah k Halting Problému (Turing):**
  - Ak by existoval dokonalý detektor D, ktorý pre každý program P určí, či je vírus, mohli by sme vytvoriť vírus V, ktorý sa správa ako vírus len vtedy, ak D(V) povie, že vírus nie je. (Paradox).
- **Obfuskácia (Zatemnenie):** Transformácia programu P na O(P), kde funkčnosť ostáva, ale čitateľnosť klesá k nule.
  - **Polymorfizmus:** Meniaci sa dešifrovací kľúč a slučka.
  - **Metamorfizmus:** Prepísanie tela vírusu (Dead-code insertion) pri každej infekcii.
- **Resume:** Súboj nie je o matematickej istote, ale o ekonomike času (Cost of Attack vs. Cost of Defense).

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

Architektúra Linux binárky (ELF)

- **ELF (Executable and Linkable Format):** Binárny štandard pre Unix/Linux.
- **Dva pohľady na súbor:**
  - **Linking View (Sekcie):** Pre kompilátor a linker (statický pohľad).
  - **Execution View (Segmenty):** Pre zavádzač (loader) a OS (dynamický pohľad).
- **Kľúčové komponenty:**
  - **ELF Header:** Magic bytes (`0x7F ELF`), Entry Point address.
  - **Program Headers (`PT_LOAD`):** Určujú, ktoré časti súboru sa mapujú do RAM.
  - **Section Headers:**
    - `.text`: Vykonateľný kód (Read+Execute).
    - `.rodata`: Konštanty, reťazce (Read-Only).
    - `.data`: Inicializované globálne a statické premenné (Read+Write).
    - `.bss`: Neinicializované dáta (nezaberajú miesto na disku, len v RAM).

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

Dynamické linkovanie a útoky

- **Princíp zdieľaných knižníc:** Aby boli binárky malé, funkcie ako `printf` alebo `connect` sú v `libc.so`, nie v programe.
- **Lazy Binding:** Adresy sa nevypočítavajú pri štarte (čo by spomalilo štart), ale až pri prvom volaní.
- **Mechanizmus:**
  - Kód zavolá `printf@plt` (v `.plt` sekcii).
  - Skok na adresu v `.got.plt`.
  - Prvýkrát: Adresa v GOT ukazuje späť do PLT => volá sa Dynamic Linker (`_dl_runtime_resolve`).
  - Linker nájde `printf`, zapíše skutočnú adresu do GOT.
  - Druhýkrát: Skok z PLT ide cez GOT priamo na `printf`.
- **Útok (GOT Poisoning) - klasický vektor útoku (historický koncept):** Útočník prepíše adresu v GOT tabuľke. Namiesto `printf` sa vykoná `system("/bin/sh")`.
- **Obrana:** RELRO (Relocation Read-Only) - Full RELRO robí GOT "read-only" po štarte.

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

Typológia hrozieb - Botnety

- **Mirai (2016):** Jeden z najvýznamnejších a najdeštruktívnejších IoT botnetov, ktorý priniesol bezprecedentnú škálu DDoS útokov.
- **Architektúra útoku:**
  - **Infection Vector:** Telnet/SSH brute-force (slovník najčastejšie používaných hesiel ako `admin:1234`).
  - **C2 Komunikácia:** Pôvodne nešifrovaná, novšie varianty (Satori, Okiru) používajú šifrovanie alebo Tor.
- **Modulárna štruktúra:**
  - **Scanner:** Asynchrónny, stateless SYN skener (veľmi rýchly). Náhodne generuje IP, vyhýba sa `127.0.0.0/8`, `10.0.0.0/8` a napríklad sieťam DoD, USPS …
  - **Attack Module:** Implementuje DDoS metódy (UDP flood, SYN flood, GRE flood, Valve Source Engine flood).
  - **Killer Module:** Identifikuje iné botnety (anime malware) a zabíja ich procesy podľa názvu alebo portu (23, 48101).
- **Perzistencia:** Žiadna. Po reštarte routera zmizne (memory-resident). Ale router je do minúty infikovaný znova (opäť využitím “Infection Vector”).

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

Rootkity a eBPF

- **Cieľ Rootkitu:** Udržať prístup (backdoor) a skryť prítomnosť (stealth).
- **Klasické LKM (Loadable Kernel Modules):**
  - Manipulácia `sys_call_table`.
  - Príklad: `Diamorphine` (skrýva modul poslaním signálu 31 procesu, stáva sa root-om poslaním signálu 63; procesy sa skrývajú cez magický prefix). Aktualizácia (2024): Avast objavil novú variantu Diamorphine in-the-wild, čo potvrdzuje, že tento rootkit je stále aktívne využívaný.
  - Detekcia: Kontrola integrity tabuľky systémových volaní, `lsmod`.
- **Moderné hrozby: eBPF (Extended Berkeley Packet Filter):**
  - Pôvodný účel: Bezpečný, efektívny monitoring a filtrovanie sieťových paketov v jadre OS.
  - Zneužitie (malware): Útočník načíta eBPF program, ktorý modifikuje návratové hodnoty systémových volaní (napr. `getdents64` pre výpis súborov).
  - **Prečo je to nebezpečné?**
    - Kód eBPF beží v jadre.
    - Nemusí byť zavedený ako modul (nevidno v `lsmod`).
    - Obchádza tradičné bezpečnostné nástroje.

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

Návrh bezpečného laboratória (Infraštruktúra)

- **Bezpečnostné pravidlá:**
  - Fyzická izolácia (dedikovaný počítač - bare metal) vs. virtualizácia.
  - **Nikdy** nepripájať infikovaný stroj do produkčnej siete.
- **Architektúra virtualizácie:**
  - **Hypervízor:** KVM/QEMU (Linux host), alebo VMware Workstation, prípadne VirtualBox.
  - **Sieťovanie:** Host-Only Network (vytvorí virtuálny switch bez prístupu mimo laboratórnu sieť).
- **Topológia laboratória:**
  - **Victim VM:** Ubuntu, Debian, Alpine (často cieľom botnetov). Snapshoty v stave "Clean".
  - **Gateway/Analysis VM: REMnux** (distribúcia založená na Ubuntu s predinštalovanými nástrojmi).
    - Funguje napríklad ako DNS server, Gateway, Log collector pre Victim VM.
- **Opatrenia:** Vypnúť "Shared Folders", "Drag & Drop", "Shared Clipboard" (pri prístupe k victim VM).

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

Simulácia Internetu

- **Problém:** Malvér je "shy" (hanblivý). Ak zistí, že nemá prístup na Internet, nemusí sa spustiť payload. Ak má skutočný Internet, zaútočí na cudzie ciele (právny problém).
- **Riešenie: INetSim (Internet Services Simulation Suite):**
  - Emuluje bežné služby: HTTP/HTTPS (falošné IIS/Apache hlavičky), DNS, FTP, IRC, SMTP.
  - **DNS Fake:** Na všetky dotazy (napr. `badguy.com`) odpovedá IP adresou REMnux VM.
- **Konfigurácia smerovania (iptables):**
  - Na REMnux stroji: `iptables -t nat -A PREROUTING -i eth0 -j REDIRECT`.
  - Všetka sieťová prevádzka z Victim VM je spracovávaná cez INetSim.
  - Upozornenie: Odporúča sa však špecifikovať vybrané porty, nie presmerovať celú prevádzku.
- **Limity:** HTTPS (SSL pinning) – malvér môže odmietnuť falošný certifikát. Vtedy je nutná analýza cez MITM proxy (Burp Suite) alebo dešifrovanie v pamäti.

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

Statická analýza

- **Cieľ:** Získať informácie bez vykonania inštrukcií.
- **Fáza 1: Identifikácia a Triage:**
  - **Hashing:** MD5/SHA256 (pre VirusTotal), ale aj **Fuzzy Hashing (SSDEEP)** – porovnáva podobnosť kódu, nie identitu bitov (detekcia variantov).
  - **Strings:** `strings -n 10 malware.bin` (napr. hľadanie hardcoded IP, URL, chybových hlášok, ciest k súborom …).
  - **Packer Detection:** `die` (Detect It Easy), `binwalk` (extrakcia vnorených súborov). Vysoká entropia textu indikuje šifrovanie/kompresiu.
- **Fáza 2: Disassembly a Decompilation (Ghidra):**
  - **Ghidra (NSA):** Open-source framework. Kľúčová vlastnosť: Synchronizácia medzi grafom, disassemblerom a dekompilátorom.
  - **Analytický proces:**
    - Nájsť `main` alebo `entry_point`.
    - Sledovať toky dát (XREFs - Cross References).
    - Premenovávanie premenných a funkcií na základe kontextu (reverzná tvorba symbolov).

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

Dynamická analýza

- **Princíp:** Sledovanie správania malvéru v reálnom čase v kontrolovanom prostredí (Sandbox).
- **System Call Tracing (`strace`):**
  - Linux kernel je brána k hardvéru. Aplikácia musí požiadať kernel o všetko (sieť, disk, procesy …) - akékoľvek systémové prostriedky.
  - **Dôležité parametre:**
    - `-f`: Sledovať forknuté procesy (malvér sa často stáva démonom - stáva sa službou na pozadí).
    - `-s 2000`: Zväčšiť limit pre výpis reťazcov (aby sme videli celé URL/dáta).
    - `-y`: Dekódovať file descriptory (namiesto `write(3, ...)` vidíme `write(/tmp/malware, ...)`).
- **Vzorce správania (Heuristika):**
  - **Ransomware:** Rekurzívny `getdents` (výpis adresárov) + `open` + `read` + `write` (šifrovanie) + `unlink` (zmazanie originálu).
  - **Dropper:** `open` (vytvorenie súboru) + `write` (zápis payloadu) + `fchmod` (pridanie +x práv) + `execve` (spustenie).
  - **Spyware:** `connect` (C2 server) + čítanie `/etc/passwd` alebo `.ssh/id_rsa`.

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

Pokročilé techniky: Injection a Anti-Debugging

- **Process Injection (Fileless Malware):**
  - Malvér beží len v RAM iného procesu (napr. `nginx` alebo `bash`).
  - Technika (akademický príklad - aktuálne blokované Yama modulom) cez `ptrace`:
    - `PTRACE_ATTACH`: Zastaví cieľový proces.
    - `PTRACE_POKETEXT`: Prepíše inštrukcie (často prepíše začiatok funkcie skokom na shellcode).
    - `PTRACE_DETACH`: Proces pokračuje, ale vykonáva malvér.
- **Anti-Debugging a Anti-Analysis:**
  - **`ptrace(PTRACE_TRACEME)`:** Klasický trik. Proces môže byť debuggovaný len raz. Ak to malvér zavolá prvý a zlyhá to (lebo ho už drží `strace` alebo `gdb`), malvér vie, že je sledovaný => `exit()`.
  - **Kontrola prostredia:** Čítanie `/proc/self/status` (pole `TracerPid`), kontrola MAC adresy (virtuálne karty), kontrola CPU inštrukcií (niektoré inštrukcie sú vo VM pomalšie - Timing attacks cez `rdtsc`).
- **Bypass:**
  - `LD_PRELOAD`: Načítanie vlastnej knižnice pred štartom, ktorá "hookne" `ptrace` a vždy vráti úspech (0), aj keď “klame”.
  - Úprava binárky: Prepísanie podmieneného skoku, ktorý nasleduje po kontrole návratovej hodnoty ptrace. Mohlo by to byť JE => JNE alebo JZ => JNZ (sú to aliasy) — alebo sa celá kontrola nahradí inštrukciami NOP.

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

Záver, budúcnosť a diskusia

- **Evolúcia Malvéru:**
  - Od jednoduchých skriptov k sofistikovaným binárkam v Go a Rust (ťažšie na RE kvôli veľkým runtime knižniciam).
  - **Server-Side Polymorfizmus:** Útočník generuje unikátny hash pre každú obeť. Tradičné AV signatúry sú na ústupe.
  - **Supply Chain Attacks:** Infekcia build pipeline (napr. SolarWinds, xz utils backdoor).
- **Budúcnosť Obrany:**
  - **Behaviorálna analýza:** Detekcia anomálií, nie vzorov kódu.
  - **Automated RE:** Využitie AI na automatické generovanie popisov funkcií v assembleri.
- **Zhrnutie kurzu:**
  - Statická analýza dáva prehľad.
  - Dynamická analýza dáva kontext.
  - Bezpečné prostredie je nutnosť.
- **Priestor na otázky (Q&A).**

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.