Sigurnosne Prijetnje na Internetu

Laboratorijska vježba
Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva

Analiza zloćudnog koda korištenog u MITM (čovjek-u-sredini) napadu

Ante Čavar

Zagreb, 10. Sječanj 2025

Uvod

SSL/TLS protokoli osiguravaju povjerljivost, integritet i autentifikaciju u mrežnim komunikacijama. MITM napadi mogu biti izuzetno neprimjetni što je razlog više zašto moramo podgnuti svijest o ovom problemu. Naime dolaze u raznim oblicima (fizički – danas rijetki; virtualni – sve prevalentniji i češći).
U predavanjima smo spomenuli različite zloćudne kodove koji se mogu osim MITM napada koristiti i u ostale svrhe no nama će fokus u ovoj vježbi biti na MITM napadima. MITM napadi mogu biti devastirajući iz više razloga. Osim što ih je teško za primijetiti, jednom kada se napadač „smjesti" ima pristup svoj komunikaciji (dolazećoj i odlazećoj) te se zapravo može umješati kada kod želi.
Cilj ove laboratorijske vježbe je:

- analizirati izvršnu datoteku i razumjeti barem okvirno što ona radi
- odrediti sa kojim domenama/adresama komunicira zloćudni kod

Zadatak

Zamislite da ste analitičar za računalnu sigurnost zaposlen u CERT (Computer Emergency Response Team) timu. Na Vašu analizu dolazi uzorak malicioznog softvera zvanog **Carberp**, za kojeg postoji sumnja da je dio napredne kampanje financijskog kriminala.

Vaš zadatak je:

1. Instalirati operativni sustav **REMnux OS** unutar VirtualBoxa (ili drugog hipervizora po izboru).
2. Preuzeti uzorak malicioznog softvera **Win32.Carberp** s ovog linka: Win32.Carberp - theZoo.
3. Provesti **reverzno inženjerstvo** koristeći alate dostupne na REMnux OS-u kako biste:
    - Identificirali domene i IP adrese s kojima maliciozni softver pokušava komunicirati.
    - Utvrdili svrhu tih domena i IP adresa, ako je moguće.

Za analizu koristite sljedeće alate dostupne na REMnux OS-u:

- **radare2** ili **Ghidra** za statičku analizu.
- **Wireshark** za praćenje mrežnog prometa u simuliranom okruženju.
- **strings** za jednostavnu pretragu ASCII i Unicode tekstualnih podataka u binarnom uzorku.

Na kraju, dokumentirajte sve korake analize, alate koje ste koristili te ključne rezultate.

Teorijska podloga

Što je Carberp?

Carberp je maliciozni softver (malware) koji pripada kategoriji trojanaca dizajniranih za financijski kriminal. Njegova glavna svrha je krađa osjetljivih podataka, poput vjerodajnica za prijavu na bankovne račune, pomoću tehnika poput **keylogginga**, **web injectova**, i manipulacije mrežnim prometom. Carberp je također poznat po tome što koristi **Command and Control (C2)** infrastrukturu za komunikaciju s napadačevim serverima, omogućujući mu preuzimanje dodatnog zlonamjernog koda ili slanje ukradenih podataka.

REMnux OS

REMnux je Linux distribucija posebno osmišljena za analizu malicioznog softvera i forenziku. Ova distribucija dolazi s bogatim setom alata za statičku i dinamičku analizu, među kojima su:

- **radare2** i **Ghidra** za statičku analizu binarnih datoteka, omogućujući dekompilaciju i pregled koda.
- **Wireshark** za analizu mrežnog prometa.
- **strings** za izdvajanje tekstualnih podataka iz binarnih datoteka.
  REMnux također podržava izolirano laboratorijsko okruženje koje minimizira rizik od "bijega" malicioznog softvera u produkcijsko okruženje.

Za instalaciju REMnux OS-a preporučuje se korištenje virtualizacijskih alata poput VirtualBoxa ili VMware-a. Detaljni vodiči za instalaciju dostupni su na službenim stranicama:

- Instalacija REMnux distribucije
- REMnux dokumentacija

Reverzno inženjerstvo i analitički alati

Reverzno inženjerstvo je proces analize binarnog koda kako bi se shvatilo njegovo ponašanje bez izvornog koda. Ovaj pristup koristi se za:

1. **Statičku analizu**: Pregled binarne datoteke bez izvršavanja, koristeći alate kao što su radare2 i Ghidra. Fokus je na otkrivanju C2 domena i IP adresa, kao i analiziranju maliciozne logike softvera.
2. **Dinamičku analizu**: Izvršavanje malicioznog koda u kontroliranom okruženju uz praćenje mrežnog prometa (Wireshark) i sistemskih promjena.

Kratki opisi ključnih alata:

- **radare2**: Napredni alat za statičku analizu, podržava dekompilaciju i rad s binarnim datotekama.
- **Ghidra**: Alat za statičku analizu razvijen od strane NSA, omogućuje pregled koda na višem nivou apstrakcije.
- **Wireshark**: Mrežni analizator koji omogućuje presretanje i analizu mrežnog prometa.

Izvori informacija

Za potrebe ove vježbe, studenti bi trebali istražiti sljedeće:

1. Kako funkcionira Command and Control (C2) infrastruktura i kako malware koristi DNS i IP za komunikaciju.
2. Osnovne tehnike statičke i dinamičke analize binarnih datoteka.

Preporučeni izvori za dodatno istraživanje:

- The Zoo GitHub repozitorij - arhiva uzoraka malicioznog softvera.
- REMnux dokumentacija - vodiči za korištenje alata na REMnux OS-u.
- Ghidra službena stranica - dokumentacija za Ghidru.
- Wireshark službena stranica - vodiči za analizu mrežnog prometa.

Primjena u stvarnom svijetu

Analiza malicioznog softvera poput Carberpa od ključne je važnosti za zaštitu organizacija i krajnjih korisnika od napada. Razumijevanje načina na koji malware komunicira omogućuje sigurnosnim timovima da:

- Kreiraju pravila za detekciju na mrežnim vatrozidima i IDS/IPS sustavima.
- Izgrade učinkovite strategije za uklanjanje prijetnji.
- Razviju prevencijske mjere za zaštitu od budućih napada.

Postavke za vježbu

Potrebno je osigurati virtualni stroj koji koristi **REMnux OS**. Postavljanje se može izvršiti pomoću bilo kojeg popularnog hipervizora, poput:

- **VirtualBox** (besplatno dostupan)
- **VMware Workstation Player** (besplatno za osobnu upotrebu)

Koraci za postavljanje REMnux OS-a:

1. Preuzmite REMnux virtualni stroj s službene stranice.
2. Uvezite preuzeti `.ova` ili `.ovf` datoteku u VirtualBox ili VMware Player.
3. Provjerite da je mrežna kartica virtualnog stroja postavljena na način koji omogućuje internet konekciju (npr. NAT ili Bridged).
4. Pokrenite REMnux virtualni stroj i osigurajte pristup administrativnim privilegijama.

Malware uzorak

Potrebno je preuzeti uzorak malwarea **Win32.Carberp** iz javnog repozitorija:

- Link za preuzimanje: Win32.Carberp - theZoo.
- Upozorenje: Uzorak malicioznog softvera može biti opasan, stoga je obavezno korištenje izoliranog laboratorijskog okruženja. Nikada ne pokrećite malware na sustavima izvan izoliranog okruženja.

Alati za analizu

REMnux dolazi s unaprijed instaliranim alatima potrebnima za vježbu. Osigurajte da su sljedeći alati dostupni i spremni za upotrebu:

- **radare2** ili **Ghidra** za statičku analizu binarnih datoteka.
- **Wireshark** za praćenje mrežnog prometa.
- **strings** za jednostavnu analizu tekstualnih podataka unutar binarnih datoteka.

Dodatna priprema

- Provjerite jesu li svi paketi i alati na REMnux OS-u ažurirani pomoću naredbe:

  ```
  $ sudo apt update && sudo apt upgrade -y
  ```
  i

  ```
  $ remnux upgrade
  ```

- Instalirajte dodatne pakete ako je potrebno za specifične analize (npr. `net-tools`, `tcpdump`).
- Osigurajte snapshot virtualnog stroja prije pokretanja malwarea kako biste mogli vratiti sustav na početno stanje u slučaju bilo kakvih problema.

6. Sigurnosne mjere

- Obavezno isključite opciju dijeljenja mapa između domaćinskog i virtualnog stroja.
- Onemogućite internet vezu tijekom pokretanja malwarea ako ne želite dopuštati komunikaciju s pravim C2 serverima.

Ovdje su ponuđene samo neke od ideja. Sjetite se ovo nije nepoznat software i imate pravo koristiti što god vam je na raspolaganju ne bi li saznali više o njemu (kodu). Nemojte se limitirati jer je za rješenje ove vježbe potrebno out-of-the-box razmišljanje ne biste li ju rješili.

Rješenje vježbe

Statička analiza (Ghidra)

1. **Pokretanje Ghidre**:
   - Otvorite Ghidru na REMnux OS-u pomoću naredbe:

     ```
     ghidra
     ```

   - Kreirajte novi projekt i uvezite binarni uzorak iz **Win32.Carberp.zip**-a pod nazivom AAA._xe
2. **Pregled binarnog koda**:
   - Analizirajte ulazne točke programa (`entry point`) kako biste identificirali ključne funkcije koje upravljaju mrežnom komunikacijom.
   - `Koristite funkciju` **`"Search for Strings"`** `kako biste pronašli potencijalne domene, IP adrese ili nazive funkcija vezanih za mrežnu komunikaciju, poput socket, resolveHostName, resolveAddress ...`
   - Ako pronađete šifrirane sekcije, dokumentirajte lokacije kako biste ih kasnije mogli analizirati.

3. **Ograničenja**:
    - Carberp koristi napredne tehnike obfuskacije i šifriranja, što može uvelike otežati statičku analizu (činjenica da je izvorni kod na rusom ne pomaže)
    - Mnogo informacija može biti dinamički generirano, zbog čega je potrebna dodatna analiza prilikom izvršavanja programa (debugger)
    - ne morate sami rješavati ovo razmislite o dodatnim načinima na koje si možete pomoći

Dinamička analiza (Wireshark)

1. **Priprema mreže**:
    - Konfigurirajte mrežnu postavku REMnux OS-a na **Host-Only** ili **NAT**.
    - Pokrenite **Wireshark** i filtrirajte promet prema specifičnim protokolima, poput DNS, HTTP ili TCP:

      ```
      dns || http || tcp
      ```

2. **Pokretanje uzorka malwarea**:
    - U sigurnom laboratorijskom okruženju pokrenite Carberp uzorak.
    - Pratite mrežni promet pomoću Wiresharka i bilježite sve sumnjive zahtjeve, uključujući domene, IP adrese i obrasce mrežne komunikacije
3. **Analiza mrežnog prometa**:
    - Identificirajte DNS zahtjeve i odgovore koji mogu otkriti C2 domene.
    - Pregledajte HTTP ili TCP promet za potencijalne naredbe ili odazive
4. **Ograničenja**:
    - Carberp može koristiti šifrirani promet, što otežava interpretaciju podataka u mrežnom prometu.
    - Ako malware ne može komunicirati s pravim C2 serverima (npr. zbog nepostojećih domena), analiza može biti ograničena

Alternativa: Analiza izvornog koda

Ako je analiza binarnog uzorka prekomplicirana zbog obfuskacije i šifriranja, predlažem korištenje dostupnog izvornog koda:

- Preuzmite **izvorni kod Carberpa** s GitHub repozitorija: Carberp - Original Source.
- Pregledajte funkcije povezane s mrežnom komunikacijom kako biste identificirali domene i IP adrese.
- Analiza zahtijeva dobro poznavanje jezika u kojem je napisan (C++).

Krajnja opcija

Carberp pripada naprednim prijetnjama te vam svaka čast ukoliko ste ju uspjeli u potpunosti sami razraditi. Međutim, sve potrebne informacije (domenama i IP adresama) bile su dostupne na internetu, primjerice na platformama poput **VirusTotal** ili specijaliziranim blogovima i bazama podataka o malwareu.

Iako je vježba možda zahtijevala puno vremena i napora, bitno je usvojiti širu perspektivu i razmišljati "izvan okvira" što je posebno teško palo autoru vježbe. Pohvale svima koji su na samom početku iskoristili dostupne online resurse za rješavanje zadatka! (Nadam se da me kolege neće zamrziti zbog ovog jer je štoviše ovo najviše meni bila lekcija...)

Zaključak

Tijekom ove vježbe studenti su naučili postaviti izolirano laboratorijsko okruženje za analizu malicioznog softvera koristeći REMnux OS i virtualizaciju. Kroz statičku analizu uz pomoć alata Ghidra, upoznali su se s tehnikama obfuskacije i izazovima analize binarnih datoteka. Dinamičkom analizom mrežnog prometa uz Wireshark stekli su uvid u metode koje malware koristi za komunikaciju s udaljenim poslužiteljima.

Vježba je također naglasila važnost razmišljanja "izvan okvira", jer je tražene informacije bilo moguće pronaći na internetu, čime se pokazala vrijednost korištenja dostupnih resursa. Ključna lekcija ove vježbe je da je za uspješnu analizu zloćdnog softvera potrebno kombinirati tehničke vještine, znanje, kreativnost i proaktivno traženje informacija na internetu.

Literatura

https://docs.remnux.org/install-distro/get-virtual-appliance - pristupljeno 3.1.

https://docs.remnux.org/ - pristupljeno 3.1.

https://cloud.google.com/blog/topics/threat-intelligence/carbanak-week-part-one-a-rare-occurrence/ - pristupljeno 4.1., autori: Michael Bailey, James T. Bennett

https://cloud.google.com/blog/topics/threat-intelligence/carbanak-week-part-two-continuing-carbanak-source-code-analysis/ - pristupljeno 4.1., autori: Michael Bailey, James T. Bennett

https://cloud.google.com/blog/topics/threat-intelligence/carbanak-week-part-three-behind-the-backdoor/ - pristupljeno 5.1., autori: Michael Bailey, James T. Bennett

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Mal~Carberp-E/detailed-analysis – pristupljeno 5.1., Sophos

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Carberp-K/detailed-analysis – pristupljeno 5.1.; Sophos

https://www.virustotal.com/gui/file/4297ad0f5bb72616337d88f14c07a6c6d6e0c93d2a9bb5eaa7e09219556aafdb/detection – pristupljeno 5.1.; VirusTotal; sken AAA._xe datoteke

https://github.com/ytisf/theZoo/tree/master/malware/Source/Original/Carberp – pristupljeno 3.1.; theZoo Github repo