Ofenzivna sigurnost

Naoružavanje

Lovro Magdić, 10.11.2025

Pitanja za ispite

- Navedi razliku između zlonamjernog softvera i naoružanog zlonamjernog softvera.
- Navedi tri grane taksonomije naoružanog zlonamjernog softvera u kibernetičkom ratovanju.
- Koja tri operativna cilja mora postići precizni naoružani zlonamjerni softver?
- Koja su kolateralna ograničenja koja naoružani zlonamjerni softver treba pratiti?
- Tijekom procesa naoružavanja, koja je uloga obfuskacije?

Pregled predavanja

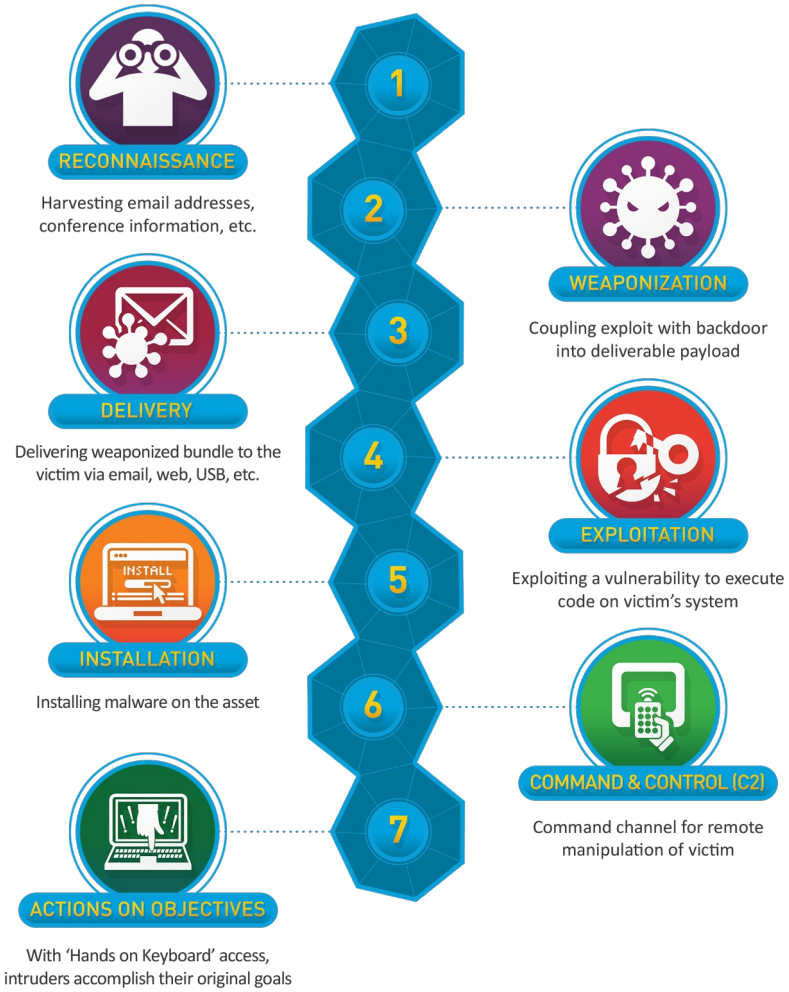
- Pitanja za ispit
- Motivacija
- Ključne definicije
- Taksonomija zlonamjernog softvera
- Taksonomija naoružanog zlonamjernog softvera
- Koraci naoružavanja
- Operativna ograničenja i rizici
- Stuxnet
- Zaključak

Motivacija

- Što čini naoružani zlonamjerni softver naoružanim?
  - tko i kako kreira naoružani zlonamjerni softver
- objasnit ćemo zašto nešto zlonamjerno treba pratiti ograničenja i koja
  - tehnička, pravna i strateška
- Kako izgleda sofisticirani naoružani zlonamjerni softver?

Ključne definicije

- kibernetički lanac napada
  - 7 koraka, Lockheed Martin
  - opis koraka kibernetičkog napada
- naoružavanje
  - druga faza kibernetičkog lanca napada, nakon izviđanja
  - proces dizajniranja i kreiranja zlonamjernog softvera koji cilja specifičnu ranjivost



Cyber Kill Chain, Lockheed Martin

Ključne definicije

- zlonamjerni softver
  - softver stvoren za izvođenje neželjenih, štetnih ili neovlaštenih radnji na nekom sustavu
- naoružani zlonamjerni softver
  - zlonamjerni softver dizajniran i kreiran za iskorištavanje specifične ranjivosti protiv profilirane mete
  - ranjivost otkrivena tijekom izviđanja mete

Taksonomija zlonamjernog softvera

- ponašanje
  - ransomware, crv, spyware...
- propagacija
  - putem mreže, fizičkih medija ili internetskih preglednika
- namjera
  - sabotaža, špijunaža, financijska dobit...
- tehničke karakteristike
  - obfuskiran, “glasan”, statičan ili samopromjenjiv kod

Taksonomija naoružanog zlonamjernog softvera

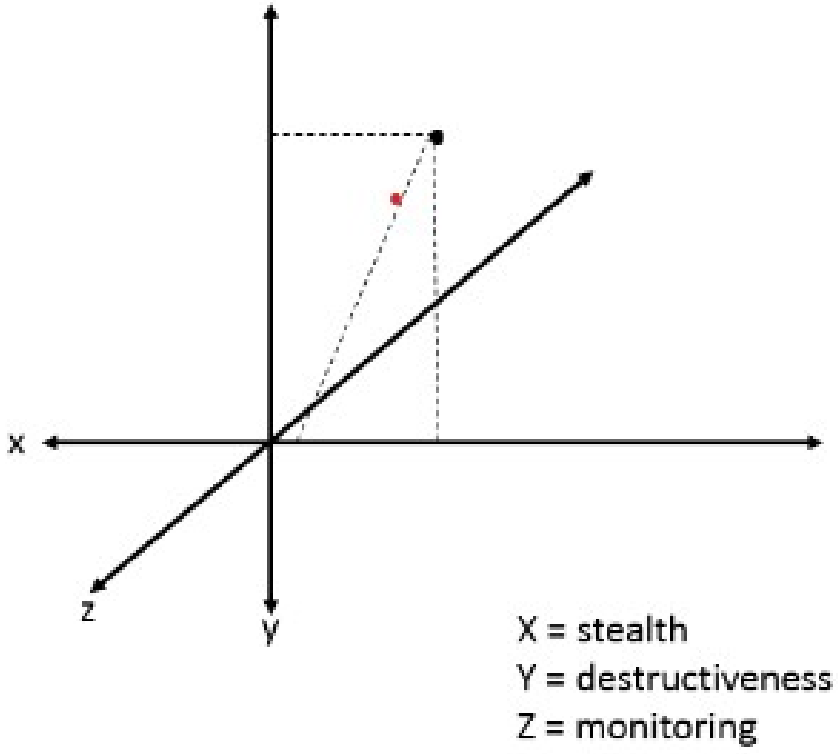
- prikrivenost
  - najniža razina – agresivna propagacija, bez pokušaja prikrivanja prisutnosti
  - najviša razina – samouništavanje, detektiranje virtualnih okruženja, diskriminacija mete...
- destruktivnost
  - najniža razina – bez nanošenje štete ili degradiranje performansi mete
  - najviša razina – nanošena šteta izvan opsega kibernetičkog prostora (prestanak rada energetskih sustava ili ostalih sustava koji mogu dovesti do gubitka ljudskog života)

Taksonomija naoružanog zlonamjernog softvera

- praćenje
  - najniža razina – ne prati i ne prikuplja podatke
  - najviša razina – prati i prikuplja te ekstrahira količinu podataka usporednu digitalnom forenzičkom pregledu
- prilagodljivost
  - najniža razina – ne prilagođava se, nedostatak perzistencije
  - najviša razina – potpuno autonomno, promjena digitalnih potpisa, enkripcija, polimorfizam, agent strojnog učenja

Taksonomija naoružanog zlonamjernog softvera

- precizni naoružani zlonamjerni softver
  - zadovoljava tri operativna cilja – diskriminacija, konzistentno ponašanje, prikrivenost diktirana operativnim ciljem
- taksonomijski trodimenzijski prostor
  - prikrivanje, destruktivnost i praćenje
  - koristan u komparativnoj analizi naoružanih zlonamjernih softvera



Easttom, C. "An examination of the operational requirements of weaponised malware." Journal of Information Warfare 17.2 (2018)

Koraci naoružavanja

- analiza rezultata izviđanja
  - popis ranjivih servisa, verzije softvera
- definicija cilja
  - eksfiltracija, sabotaža, špijunaža
- definiranje ponašanja
  - prikrivanje, destruktivnost, praćenje i prilagodljivost

Koraci naoružavanja

- kreiranje softvera i planiranje infrastrukture
  - kreiranje programa za isporuku (eng. Dropper) i zlonamjernog paketa (eng. Payload)
  - osiguravanje kanala za kontrolu i dostupnost zlonamjernog paketa
- pakiranje i usklađivanje s vektorom isporuke
  - prilagodba formata za e-poštu, instalacijski paket, obfuskacija (polimorfizam, enkripcija...)
- testiranje i verifikacija
  - provjera funkcionalnosti u izoliranim okruženjima

Koraci naoružavanja

- procjena rizika i odluka
  - vrednovanje pravnih i etičkih ograničenja te operativnih rizika
  - konačna odluka (“go or no-go”)

Operativna ograničenja i rizici

- Međunarodno pravo
  - poštivanje suveriniteta i teritorijskog integriteta (UN Charter, Article 2(4)), uporabe sile, zabrana intervencije u unutarnje poslove
- Pravo oružanih sukoba
  - diskriminacija mete – isključivo vojne mete
  - proporcionalnost – minimalna kolateralna žrtva s obzirom na vojni uspjeh
  - nužnost i humanost – legitimni vojni ciljevi, indirektna patnja civila i civilnih sustava

Operativna ograničenja i rizici

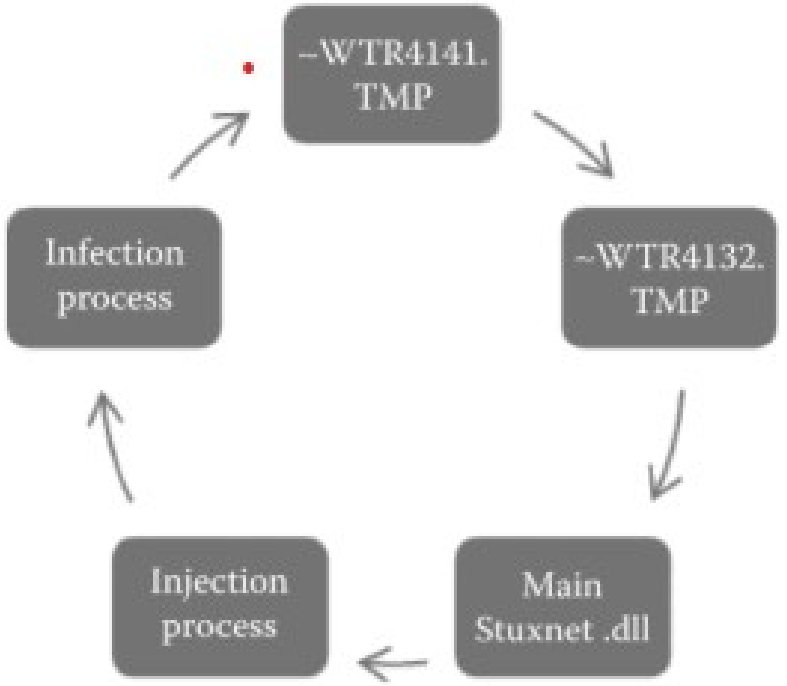
- nacionalni nadzor i ovlasti
  - nadzor i odgovornost (parlamentu, nadzornim tijelima...), pravila vođenja borbe (eng. Rules of engagement)
- atribucija i odgovornost
- kolateralna ograničenja
  - ograničavanje širenja, zaštita kritične infrastrukture (tijekom mira), zaštita opskrbnog lanca (globalna prijetnja), diskriminacija
- etičke i političke norme
  - izbjegavanje eskalacije, geopolitičke posljedice i potencijal za odmazdu

Stuxnet

- Stuxnet, 2009. – suradnja SAD-a i Izreala
  - operacija olimpijske igre
  - cilj sabotaža i onemogućavanje daljnjeg obogaćivanja urana

Stuxnet

- “fire and forget” – propagacija u ciljanoj organizaciji kroz neciljane mete
  - samorepliciranje kroz fizičke medije
  - kroz LAN mrežu
  - kroz SMB (Server Message Block)
- program za isporuku – windows sustavi
- zlonamjerni paket – industrijski kontrolni sustavi



Životni ciklus Stuxnet-a

Vinay, Makkuva Shyam, and Manoj Balakrishnan. "A comparison of three sophisticated cyber weapons." Managing Trust in Cyberspace (2013)

Stuxnet

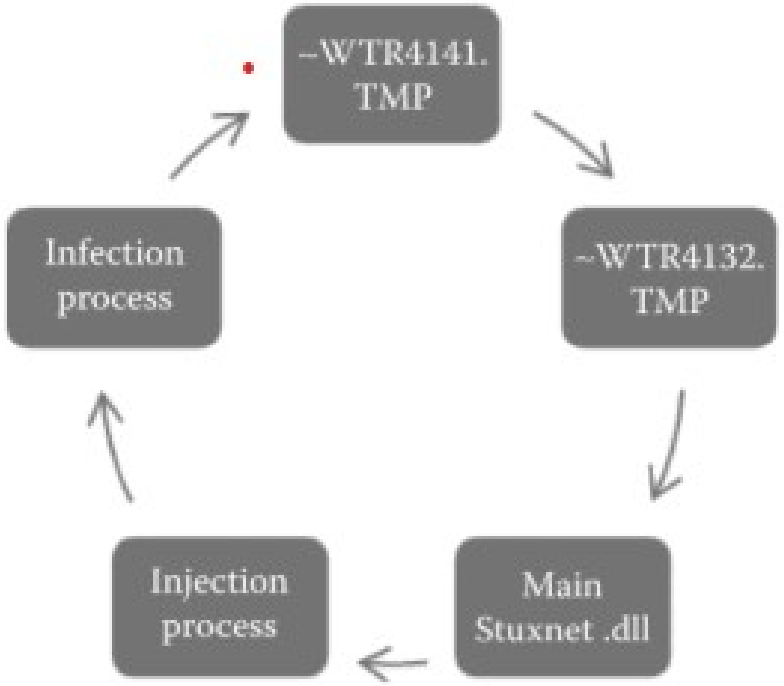
- ranjivost nultog dana, softvera za prikrivanje (eng. rootkit), izbjegavanje antivirusa i korištenje „ukradenih” digitalnih potpisa
- ažuriranje kroz P2P (peer-to-peer)
- injekcija u antivirusne sustave

Injection Targets

Security Product	Injection Target
McAfee	Winlogon.exe
KAV v1 to v7	Lsass.exe
KAV v8 and v9	KAV process
Symantec	Lsass.exe
ETrust v5 and v6	Injection is not possible
BitDefender	Lsass.exe

Mete injekcije procesa

Vinay, Makkuva Shyam, and Manoj Balakrishnan. "A comparison of three sophisticated cyber weapons." Managing Trust in Cyberspace (2013)

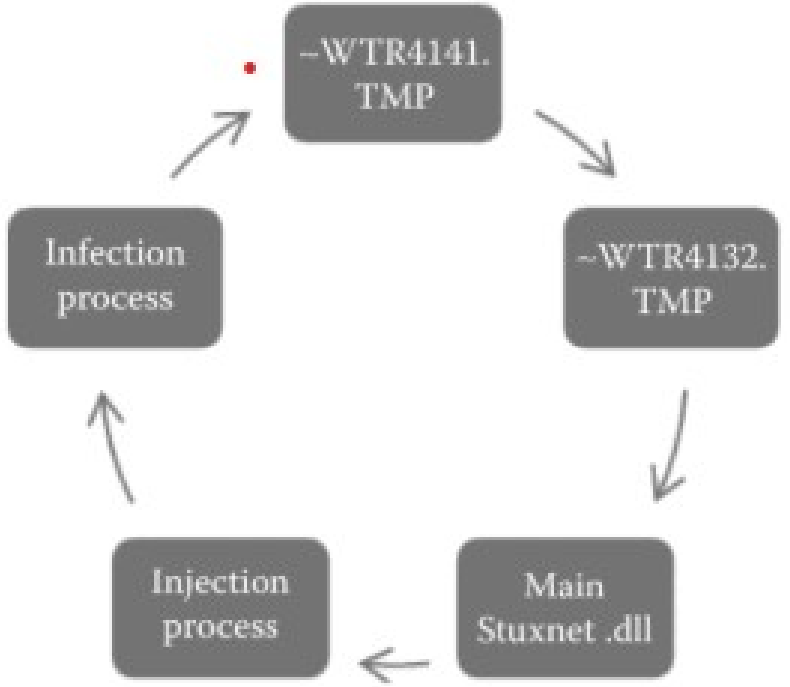


Životni ciklus Stuxnet-a

Vinay, Makkuva Shyam, and Manoj Balakrishnan. "A comparison of three sophisticated cyber weapons." Managing Trust in Cyberspace (2013)

Stuxnet

- kroz daljnju propagaciju pronalazak ciljane PLC konfiguracije (Siemens PLC)
  - ubrzavanje i usporavanje brzine rotora centrifuge do fizičkog oštećenja
  - slanje lažne telemetrije senzorima – napad posrednika (man-in-the-middle)
- operativan uspjeh (diskutabilno): sabotaža ali ne i zaustavljanje programa obogaćivanja urana
- otkrila tvrtka VirusBlokAda, 2010. godine



Životni ciklus Stuxnet-a

Vinay, Makkuva Shyam, and Manoj Balakrishnan. "A comparison of three sophisticated cyber weapons." Managing Trust in Cyberspace (2013)

Zaključak

- izrazito kompleksan i multidisciplinaran posao
- dugotrajan ciklus razvoja i testiranja
- potreba za iskustvom i kreativnošću
- zadovoljavanje ograničenje i izbjegavanje rizika
- cilj opravdava sredstva

Literatura

- Easttom, C. "An examination of the operational requirements of weaponised malware." Journal of Information Warfare 17.2 (2018)
- Subrahmanian, V. S., et al. "Types of malware and malware distribution strategies." The Global Cyber-Vulnerability Report (2015)
- Vinay, Makkuva Shyam, and Manoj Balakrishnan. "A comparison of three sophisticated cyber weapons." Managing Trust in Cyberspace (2013)
- Wangen, Gaute. "The role of malware in reported cyber espionage: a review of the impact and mechanism." Information 6.2 (2015)
- How to Break the Cyber Attack Lifecycle, Paloalto Networks
- Develop Capabilities, T1587, MITRE ATT&CK
- Hotspot Analysis: Stuxnet, 2017, Risk and Resilience Team, ETH Zurich

Dodatna literatura

- “this MP3 file is malware”, John Hammond

Hvala!