Ofenzivna sigurnost

Inicijalni ulaz

Lovro Raguž, 27.10.2025.

Pregled predavanja

- Motivacija
- Elementi inicijalnog ulaza
- Društveni inženjering
- Tehnike i primjeri
- Zaključak

Motivacija (1/2)

- Prvi obavezan korak svakog napada
  - Izviđanje može doći prije, ali inicijalni ulaz je neophodan
- Smatra se visoko-rizičnim zadatkom
  - Prvi korak u kojem je moguća detekcija i neutralizacija zbog ostavljanja tragova
- Zahtjevan i kreativan zadatak
  - Nije svaki ulaz u ciljani sustav nužno dovoljan za daljnje korake napada

Motivacija (2/2)

- Taktika koja se kontinuirano razvija u oblicima društvenog inženjeringa
  - Ljudi su sve više na internetu i ostavljaju tragove koji su podložni iskorištavanju
- Sve češća upotreba metoda bez malicioznog programa
  - Iskorištavanje legitimnih profila

Pitanja za ispite

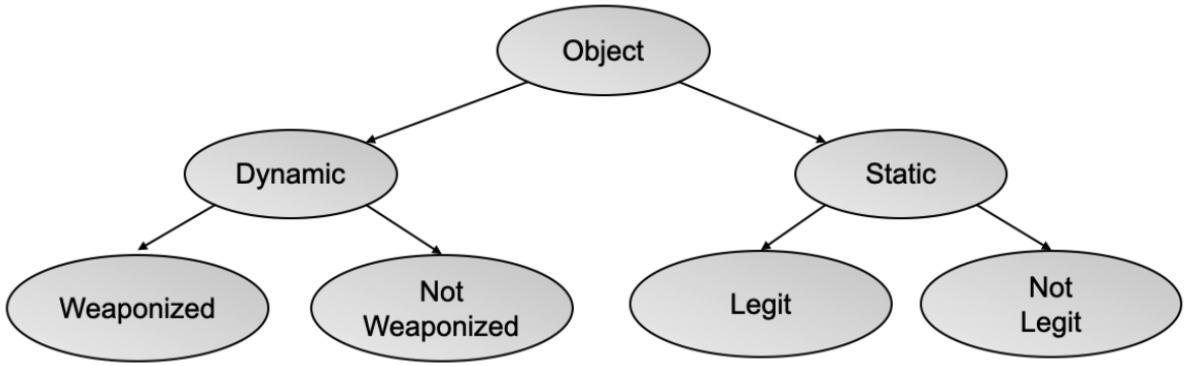
- Navedite tri ključna elementa za kompromitiranje cilja.
- Koje su dvije vrste vektora isporuke (*Delivery Vector*) i po čemu se razlikuju?
- Navedite barem tri tehnike inicijalnog ulaza.
- Navedi najčešću tehniku za inicijalni ulaz i opiši ju.
- Opiši tehniku legitimnih profila.

Obavezni elementi inicijalnog ulaza [2]

- Objekt (*Delivery Object)*
  - Koristi se za provalu ciljanog sustava
  - .exe, PDF, Word dokument, *Command Line* skripta
- Vektor isporuke (*Delivery Vector*)
  - Transport korišten za isporuku artefakta
  - USB, mail, opskrbni lanac
- Put isporuke (*Delivery Path*)
  - Način i put kojim artefakt dolazi do cilja
  - Zaposlenik otvara link, iskorištavanje vjerodajnica

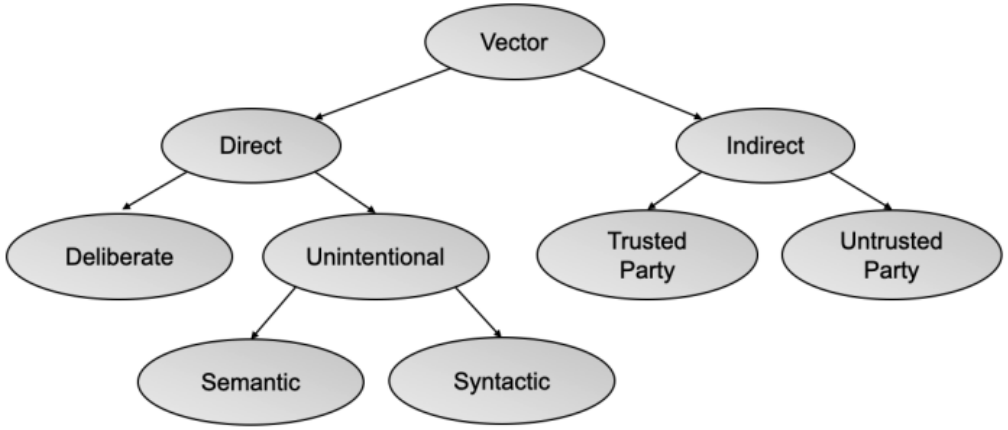
Objekt (*Delivery Object*)

- Dinamički
  - Sadrže maliciozni program
  - Naoružan i nenaoružan
- Statički
  - Ne sadrže maliciozni program, ali se koriste za provalu
  - Legitimni i nelegitimni



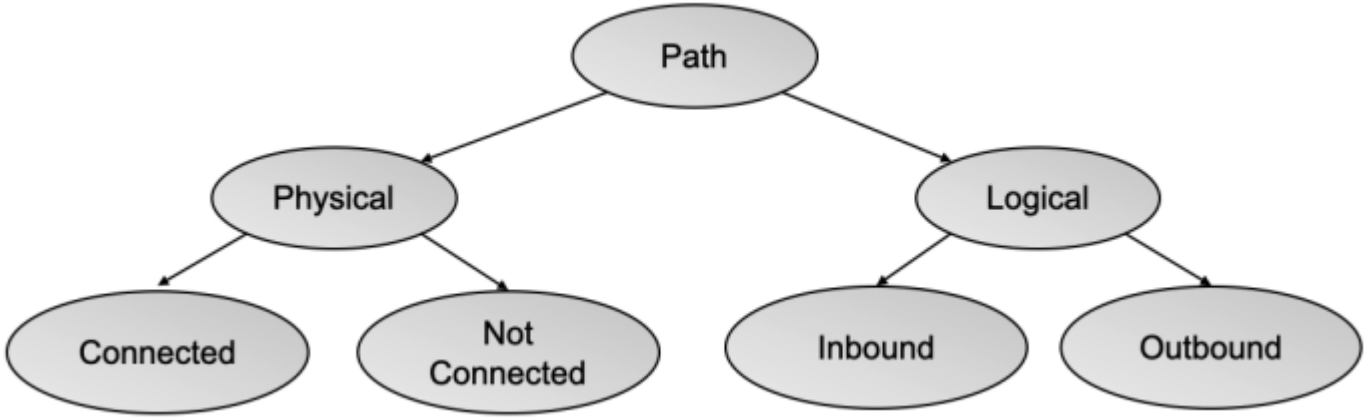
Vektor isporuke (*Delivery Vector)*

- Direktan
  - Pronalazak načina isporuke direktno cilju
  - Namjerni i nenamjerni
- Indirektan
  - Kompromitiranje preko trećih stranaka



Put isporuke (*Delivery Path*)

- Logički
  - Podjela ovisno o smjeru
- Fizički
  - Podjela ovisno o povezanosti



Društveni inženjering [5]

- Kontrola ljudskog ponašanja
  - Najčešće izazivanjem snažnih emocija
    - Pohlepa, simpatija, strah…
  - Naglasak na stvaranje uvjerljive priče
- Ljudski/tehnološki faktor
  - Zbog razvoja obrambenih sustava napadači se okreću prema društvenom inženjeringu

Phishing (T1566)

- Najčešći oblik inicijalnog ulaza
  - Poruka s namjerom dostavljanja malicioznog objekta
    - Artefakt: dinamičan i naoružan
    - Vektor isporuke: direktan i nenamjeran
    - Put isporuke: logički i izlazni
- *Spearphishing* s prilogom/poveznicom
  - Ciljani oblik *phishinga*

Primjeri - *Phishing*

- The Nordea Bank Heist - 2007 [6]
  - *Spearphishing* s prilogom
    - Korisnicima isporučen maliciozni program predočen kao besplatni anti-spam software
  - $1.2 milijuna ukradeno
- Google & Facebook – 2017 [7]
  - Lažno predstavljanje kao proizvođač
  - $100 milijuna ukradeno, ali i vraćeno

Povjerljiv odnos (T1199)

- Probijanje ili iskorištavanje organizacija s pristupom ciljanih žrtava
  - Pružen povišeni pristup partnerskim organizacijama
  - IT usluge, usluge sigurnosti, izvođači fizičkih radova
- POLONIUM grupa
  - Kompromiran OneDrive preko kojeg su dobili pristup brojnim Izraelskim organizacijama

Kompromitacija dobavnog lanca (T1195)

- Manipulacija proizvoda prije dostave
  - Dev alati, *source* kod repozitoriji, sustavi ažuriranja softwarea, *open-source* projekti
- Pod-tehnike
  - *Compromise Software Dependencies and Development Tools*
  - *Compromise Software Supply Chain*
  - *Compromise Hardware Supply Chain*

Primjer – *SolarWinds compromise*

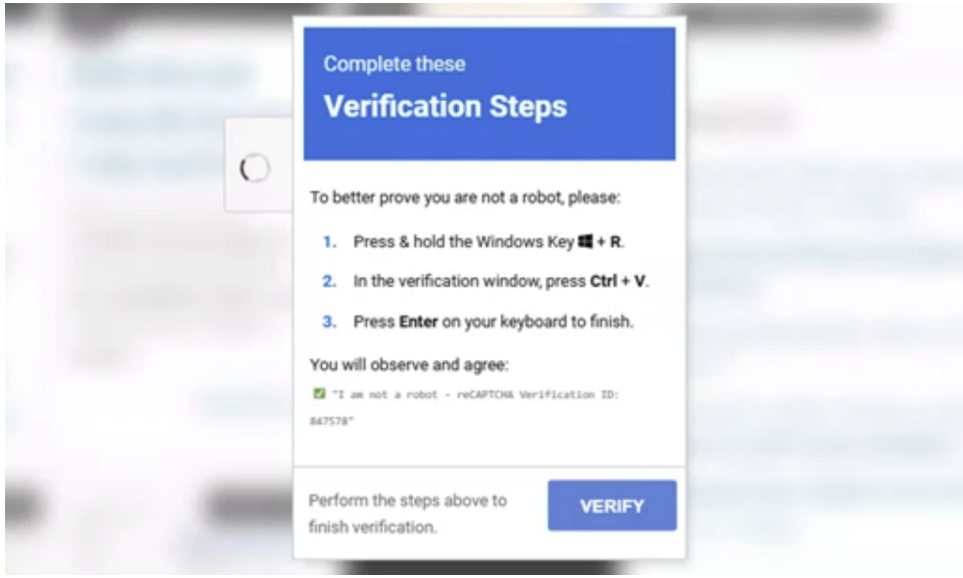
- Kompromitacija dobavnog lanca softwarea
  - Trojanizirano ažuriranje *SolarWinds Orion* programa
- Ažuriranje je izgledalo potpuno legitimno
  - Sa službene stranice
  - Digitalno potpisano
- Korištena maliciozna komponenta na razvojnom okruženju *SolarWinds Orion* programa za kompromitiranje ažuriranja

Legitimni profili (T1078)

- Dohvaćanje i iskorištavanje vjerodajnica postojećih profila
  - Inicijalni ulaz, ali i povišenje privilegija napadača
  - Iskorištavanje neaktivnih profila kako bi dulje prošli nedetektirani
- Primjeri
  - Napad na ukrajinsku električnu mrežu 2015
  - StellarParticle kampanja – aktivno mijenjanje vjerodajnica (*Credential hopping)*

Drive-by kompromitacija (T1189)

- Kompromitacija putem posjete web-stranice
  - Putem legitimnih stranica, maliciozne reklame
  - Često se oslanjaju na stare verzije browsera s ranjivostima
- Primjer – *LummaStealer* (lažni CAPTCHA)



Ostale tehnike

- Ubacivanje sadržaja
- Iskorištavanje javnih aplikacija/udaljenih usluga
- Dodavanje hardwarea
- Razmnožavanje pomoću prenosivog medija

Zaključak

- Kritična točka svakog napada
  - Napad staje nakon neuspješnog ulaza te nekad moraju pričekat više mjeseci kako bi ponovno probali
  - Najčešće korišteni: *Phishing*, *Drive-by* kompromitacija, Legitimni profili
- Zbog *phishinga* je edukacija korisnika iznimno važna
- Budućnost: *Phishing* potpomognut AI modelima

Literatura

1. Initial Access (TA0001) – MITRE ATT&CK
2. A Taxonomy for Threat Actors' Delivery Techniques – MDPI (Applied Sciences)
3. Lumma Stealer: Breaking Down the Delivery Techniques and Capabilities of a Prolific Infostealer – Microsoft Security Blog
4. What Are the Most Common Methods Used for Malware Attacks? – NEBRC (North East Business Resilience Centre)
5. A Taxonomy for Social Engineering attacks – AIS Electronic Library (CONF-IRM 2011)
6. The Phishing Swindle That Conned $100 Million Out of Google and Facebook – Bitdefender Hot for Security Blog
7. Famous Phishing Incidents from History – Town of Hempstead Official Website
8. AI Phishing Attacks – Hoxhunt Blog

Hvala!