Ofenzivna sigurnost

Command and control

Ivan Đurić, 3.11.2025.

Pregled predavanja

- Motivacija
- Definicija
- Ciljevi i funkcije
- Prikrivanje prometa
- Modeli
- Mane
- Zaključak

Motivacija

- Potreban je trajni pristup kompromitiranim uređajima radi upravljanja, prikupljanja podataka i orkestriranja akcija
- Rješenja koja će biti jeftina za održavanje, fleksibilna, skalabilna, efikasna i teško uočljiva
- Maksimizirati učinak pri minimalnoj izloženosti
- Potreban je „daljinski”

Pitanja za ispite

- Koji su najčešći ciljevi i funkcije C&C komunikacije u kibernetičkom napadu?
- Na koji način se promet prikriva radi izbjegavanja otkrivanja?
- Kako napadači koriste javne servise i „dead drop“ mehanizme za dostavu instrukcija?
- Koji komunikacijski modeli se koriste i zašto?
- Koje su glavne mane C&C komunikacije?

Što je C&C?

- Faza napada u kojoj napadač komunicira sa zaraženim uređajima
- Skup tehnika koje napadač koristi za komunikaciju sa kompromitiranim uređajima
- Omogućava udaljeno upravljanje, nadzor i eksfiltraciju podataka
- Počinje nakon infekcije uređaja i prije eksfiltracije podataka

Ciljevi i funkcije

- Upravljanje i orkestracija aktivnostima
- Prikupljanje vrijednih podataka
- Održati pristup tijekom vremena radi kasnijih incidenata i prikupljanja podataka (perzistencija)
- Smanjiti trajanje i vidljivost svojih tragova i time minimizirati izloženost

Koncepti prikrivanja prometa

- Enkripcija i korištenje „normalnih” protokola
- Vremensko maskiranje
- Posredni kanali
- Fragmentacija poruka
- Rotacija identiteta

Prikrivanje enkripcijom

- Enkripcija skriva sadržaj poruke
- Izbjegavanje detekcije
  - Sprječava mrežne sigurnosne sustave uređaja koji čitaju i analiziraju pakete
  - Onemogućuje stvaranje, primjenu i detekciju potpisa
- Korištenje legitimnih protokola
  - HTTP/HTTPS - izgleda kao obično pregledavanje weba
  - DNS Tunneling – korištenje upita i odgovora DNS protokola

Prikrivanje vremenskim maskiranjem

- Manipulacija vremenom slanja C&C prometa
- Cilj je razbiti predvidljivost "beaconing" uzorka
- Izbjegavaju se uobičajeni obrasci detekcije
  - Umjesto fiksne frekvencije se koristi nasumično kašnjenje između poruka
  - Komunikacija se podudara s razdobljima najvećeg prometa

Prikrivanje posrednim kanalima (1)

- Korištenje posrednika umjesto direktne komunikacije
- Ciljevi
  - prikriti identitet i lokaciju C&C poslužitelja
  - promet pomiješati s legitimnim vezama
- Neke od metoda
  - Dead Drop Resolver (DDR)
  - Proxy lanac i Anonymizeri
  - Domain Fronting

Prikrivanje posrednim kanalima (2)

- Dead Drop Resolver (DDR)
  - Zloćudni kod nema adresu komandnog centra već se spaja na popularni servis (GitHub, Google Drive, Twitter…)
  - Sa servisa uzima šifriranu adresu, poruku ili čeka događaj
- Proxy lanac i anonimne mreže
  - Korištenje niza kompromitiranih servera (proxyja)
  - Korištenje anonimne mreže poput Tor-a

Prikrivanje posrednim kanalima (3)

- Domain Fronting
  - Skrivanje zlonamjernog prometa iza domene legitimnog CDN servisa
  - Npr. Cloudflare ili AWS
  - Na razini mreže se vidi samo veza prema legitimnom servisu
  - Zlonamjerna domena se šalje skrivena u HTTP zaglavljima

Prikrivanje fragmentacijom

- Izbjegavanje analize cjelovitog konteksta poruke u jednom paketu
- Neki detekcijski sustavi ne rekonstruiraju cijeli paket
  - Propuštaju fragmente jer niti jedan pojedinačni dio ne sadrži cijeli potpis

Prikrivanje rotacijom identiteta

- Česta promjena ključnih identifikacijskih elemenata C&C infrastrukture
- Onemogućava praćenje i blokiranje specifičnih adresa ili potpisa
  - Korištenje DGA (Domain Generation Algorithms) za stalno generiranje i korištenje novih domena
  - Korištenje novih TLS certifikata za svaku novu C&C domenu
- Često se koristi zajedno sa fragmentiranjem

Modeli C&C komunikacije (1)

- Centralizirani model
  - Odnos kao u klijent-poslužitelj modelu
  - Može biti više C&C poslužitelja
  - Izdavanje naredbi i kontrola je jednostavnije zbog centralne arhitekture
  - Poslužitelj je kritična točka, ako se ukloni ili blokira, komunikacija prestaje

Modeli C&C komunikacije (2)

- Peer-to-Peer (P2P)
  - Neki uređaji mogu funkcionirati kao server, ali nema središnjeg čvora
  - Inficirani uređaji međusobno komuniciraju
  - Teži prekid infrastrukture nego kod centraliziranog pristupa
  - Složenija distribucija i sinkronizacija mreže zaraženih uređaja

Modeli C&C komunikacije (3)

- Out of Band (neobični kanali)
  - Koristi se da bi se nešto potvrdilo preko drugog kanala
  - Korištenje društvenih mreža, gmail-a, blogova ili drugih javnih servisa za prijenos naredbi
  - Visoka razina prikrivenosti
  - Promet izgleda legitimno

Glavne mane

- Otkrivanje infrastrukture može dovesti do gubitka kontrole
- Korištenje javnih servisa smanjuje troškove, ali povećava otisak
- Previše dinamičnosti može alarmirati sustave
- Kompromis između brzine, prikrivenosti i održivosti

Zaključak

- Dobro vođen kanal upravljanja odlučuje o uspjehu ili neuspjehu operacije
- U pravim rukama i uz promišljenu strategiju, C&C može biti presudan
- Uspješno upravljanje zaraženim uređajima temelji se na kombinaciji kontrole, prikrivenosti i otpornosti

Literatura

- Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK®: https://attack.mitre.org/tactics/TA0011/
- What is a Command and Control Attack? - Palo Alto Networks: https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained
- What is C2? Command and Control Infrastructure Explained: https://www.varonis.com/blog/what-is-c2
  autor: Robert Grimmick zadnje mijenjano: 8. kolovoza 2022.

Literatura

- When Cybercriminals with Good OpSec Attack: https://youtu.be/zXmZnU2GdVk

  autori: Ryan MacFarlane, Liam O'Murchu
  publicirano: 27. veljače 2020.

Dodatna literatura

- What are C2 Frameworks? Types and Examples: https://hunt.io/glossary/c2-frameworks-explained
  publicirano: 4. studenog 2024.
- ms teams is now a C2 (command-and-control): https://www.youtube.com/watch?v=FqZIm6vP7XM
  autor: John Hammond publicirano: 18. ožujka 2025.

Hvala!