Ofenzivna sigurnost

Infrastruktura za napade

Luka Miličević, 10.11.2025.

Pregled predavanja

- Motivacija
- Pitanja za ispite
- Pregled i zahtjevi infrastrukture za napade
- Komponente sustava
- Prikrivenost i sigurnost
- Dobre prakse
- Zaključak
- Literatura i dodatna literatura

Motivacija

- Efikasno i kontrolirano izvođenje napada
- Izbjegavanje obrambenih sustava i osiguranje prikrivenosti
- Zadržavanje pristupa kompromitiranom sustavu i zaštita u slučaju razotkrivanja
- Zahtjeva veliku količinu tehničkog znanja, planiranja i konfiguracije

Pitanja za ispite

- Nabrojite barem 5 zahtjeva infrastrukture za napade.
- Koja su 2 osnovna tipa poslužitelja koja se koriste za napade?
- Koje su razlike između 3 osnovna tipa preusmjerivača?
- Koje su prednosti i mane jednostavnog "pipe" HTTPs preusmjerivača i RWP HTTPs preusmjerivača?
- Nabrojite barem 3 dobre prakse za osiguranje C2 poslužitelja.

Pregled i zahtjevi infrastrukture za napade

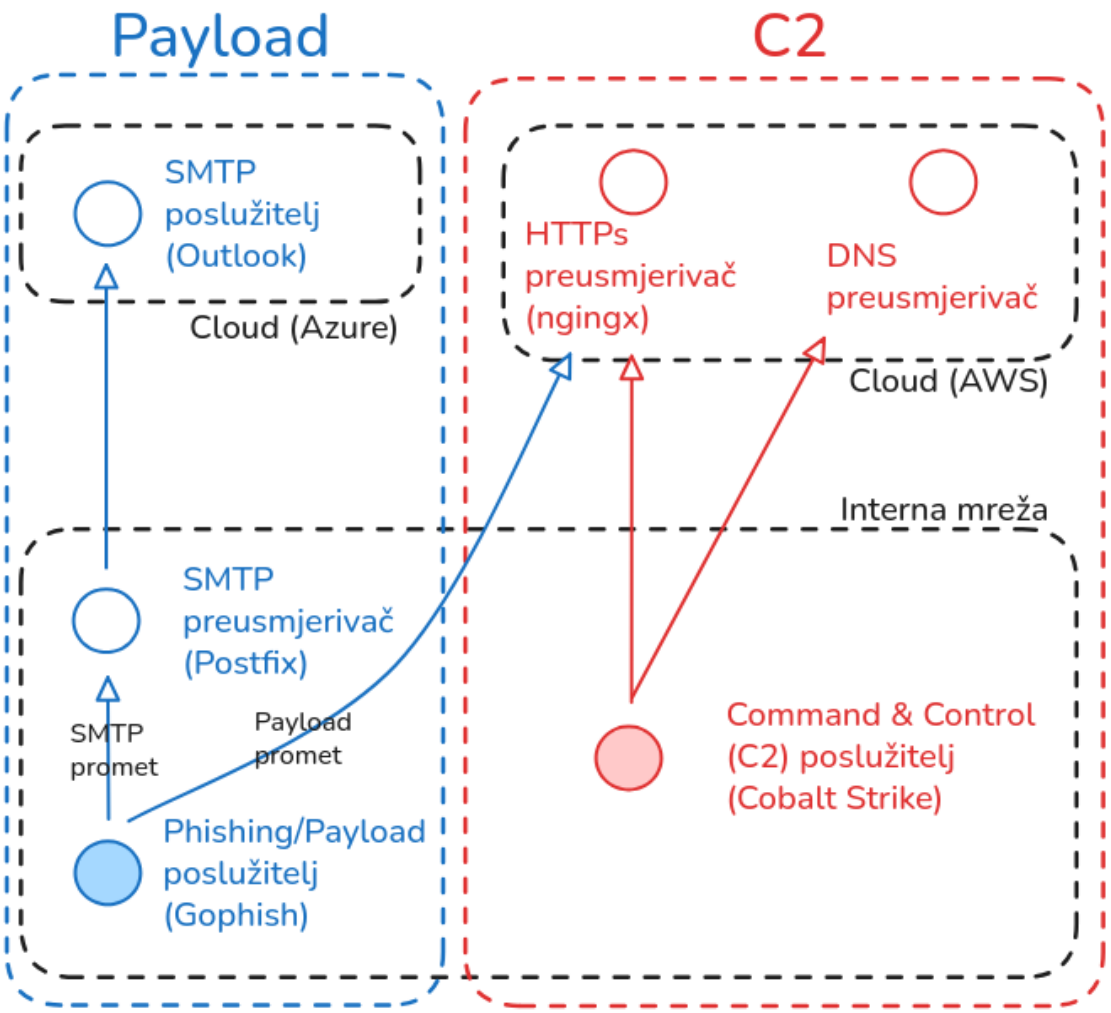
- Infrastruktura za napade uključuje alate, poslužitelje, domene i druge potrebne komponente za uspješno izvođenje napada
- Zahtjevi [1]
  - Funkcionalni
  - Sigurnosni
  - Ostali

Pregled i zahtjevi infrastrukture za napade

Funkcionalnost	Sigurnost i prikrivenost	Dodatno
Hosting i dostava payload-a i lažnih web stranica	Zaštita jezgrenih komponenti (preusmjerivači)	Modularnost
Command & Control (C2)	Izbjegavanje obrambenih sustava i detekcije	Fleksibilnost
Phishing – automatizirana isporuka, mogućnost primanja e-poruka...	Zaštita u slučaju detekcije	Jednostavan/automatiziran proces pripreme
Zadržavanje u kompromitiranom sustavu	"Hardened" poslužitelji	Sustavi za praćenje (logging, monitoring)
Spremanje podataka, vjerodajnica i sl.		

Glavne komponente

- Payload poslužitelji
- C2-poslužitelji
- Preusmjerivači (Redirectors)
- Dodatne komponente

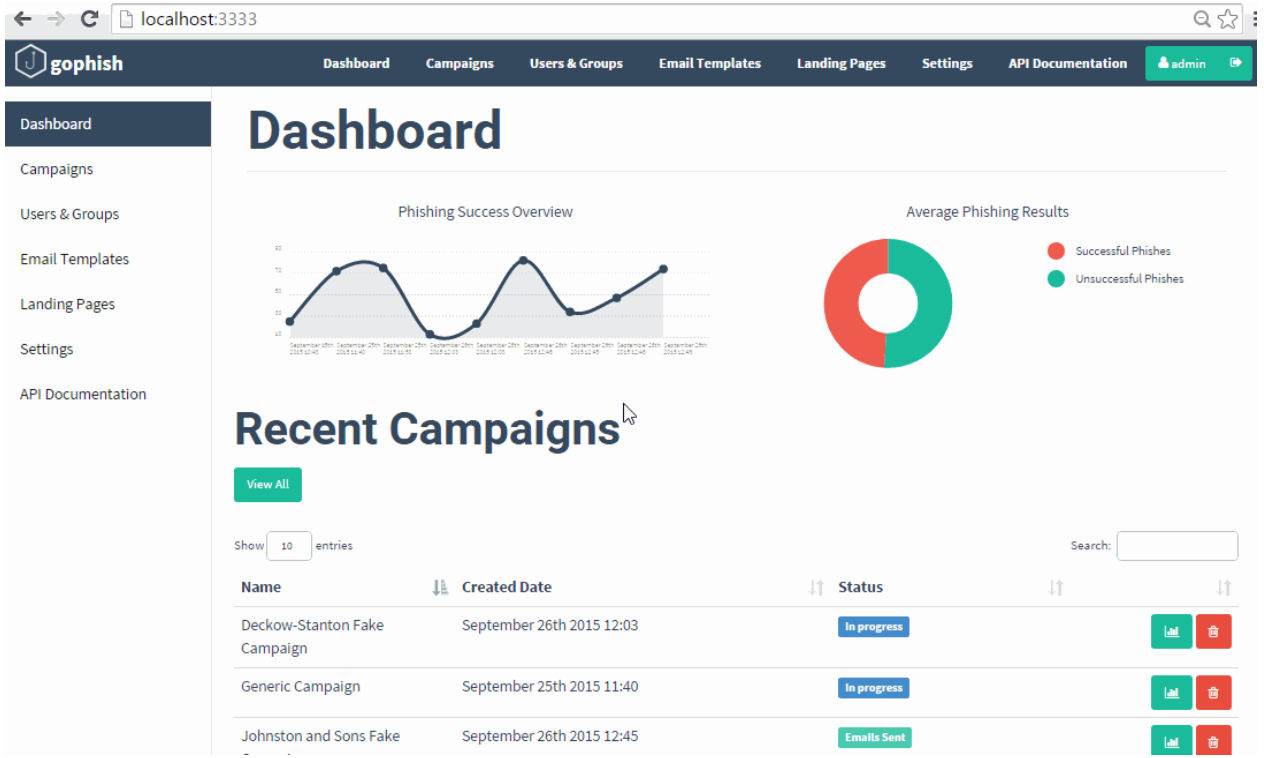


Payload poslužitelji

- Čuva i dostavlja payload za napad
  - Stage-0-payload – vrlo malen, prvi stiže na metu
  - Stage-1-payload – "pravi" payload koji se šalje nakon aktivacije stage-0
- Poslužitelj se mora dobro prikriti [2]
  - Idealno u privatnoj mreži, skriven iza preusmjerivača i legitimnog poslužitelja (npr. Outlook poslužitelj e-pošte)

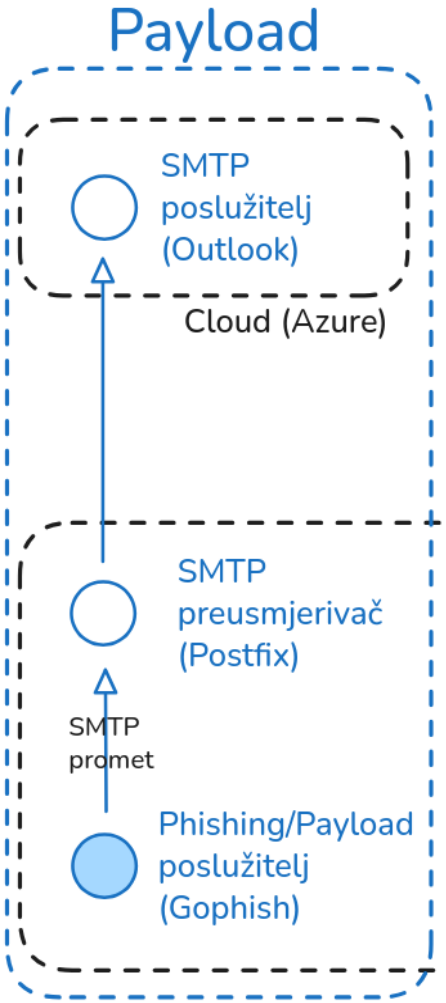
Payload poslužitelji - primjer

- Primjer: Gophish
  - De facto standard
  - Slanje phishing e-poruka, izrada i posluživanje lažnih web stranica, praćenje ponašanja mete...
  - Uz to sve, posluživanje stage-1-payload-a



Payload poslužitelji - prikrivanje

- **Presumjerivač**
  - Hvata e-poruke poslužitelja, miče potencijalno neželjene dijelove (npr. "Gophish" zaglavlje...)
  - Primjer: Postfix
- **SMTP poslužitelj**
  - Najbolje koristiti legitmni SMTP server - djeluje vjerodostojno i omogućuje pregled pretinca e-pošte
  - Primjer: Outlook na Azure-u



Payload poslužitelji - priprema

- Registrirati domenu i pribaviti potrebne DNS zapise (A, NS...)[3]
- Pribaviti licencu za SMTP server (npr. Office365/Outlook, CloudFront, DigitalOcean...)
- Konfigurirati poslužitelj i preusmjerivač u lokalnoj mreži te ih uputiti na SMTP server

C2 poslužitelji

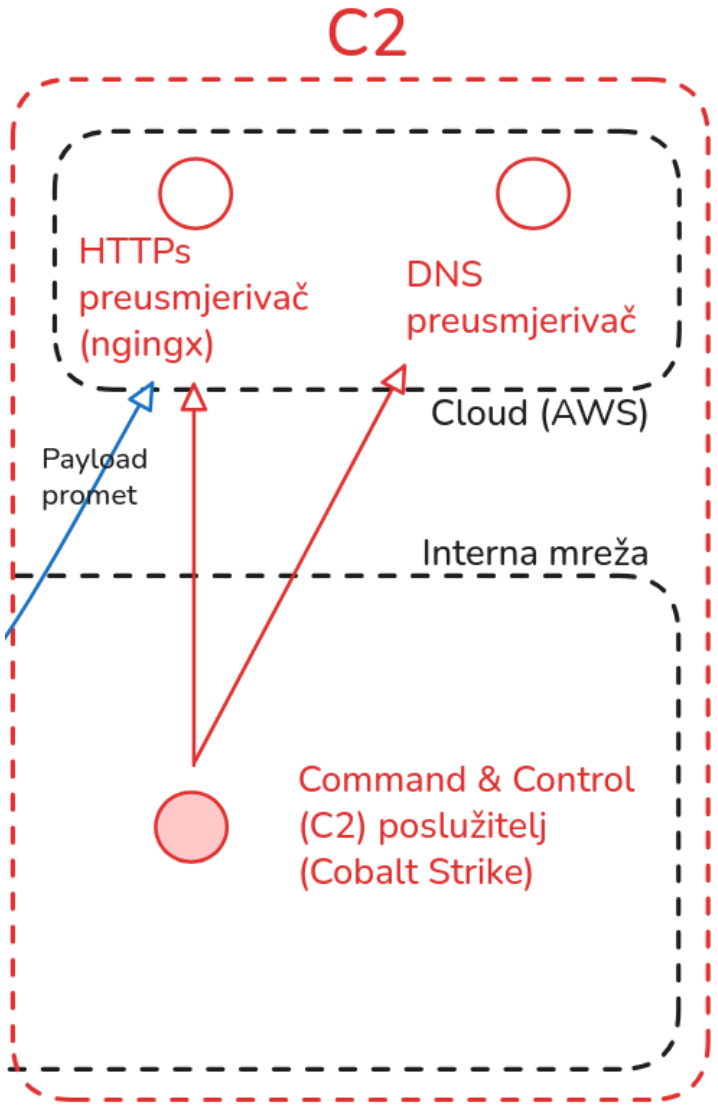
- Nakon inicijalnog ulaza, potrebna je efikasna i prikrivena komunikacija
- Najčešće: neki C2-framework
  - Cobalt Strike, Silver...
  - Manje popularni = manje istraženi mehanizmi detekcije i obrane
- Više instanci poslužitelja iza više preusmjerivača

C2 poslužitelji - odabir framework-a

- Plaćene opcije često imaju GUI, podršku za više komunikacijskih kanala, operacijskih sustava ili korisnika, ugrađene mehanizme izbjegavanja...
- Naravno, moguće i paralelno korištenje više sustava
- Postoje sveobuhvatne usporedbe na internetu[4]

C2 poslužitelj - prikrivanje

- Najbitnije je skriti poslužitelj (koji je idealno u privatnoj mreži) iza jednog ili više HTTPs preusmjerivača
- Maskirati promet (npr. Malleable C2 profiles – Cobalt Strike)[5]
- Korištenje 3rd Party C2 kanala (Domain Fronting)[3]



Preusmjerivači

- Djeluju kao proxy za poslužitelje
- U slučaju da se detektiraju, mogu se ugasiti i zamijeniti

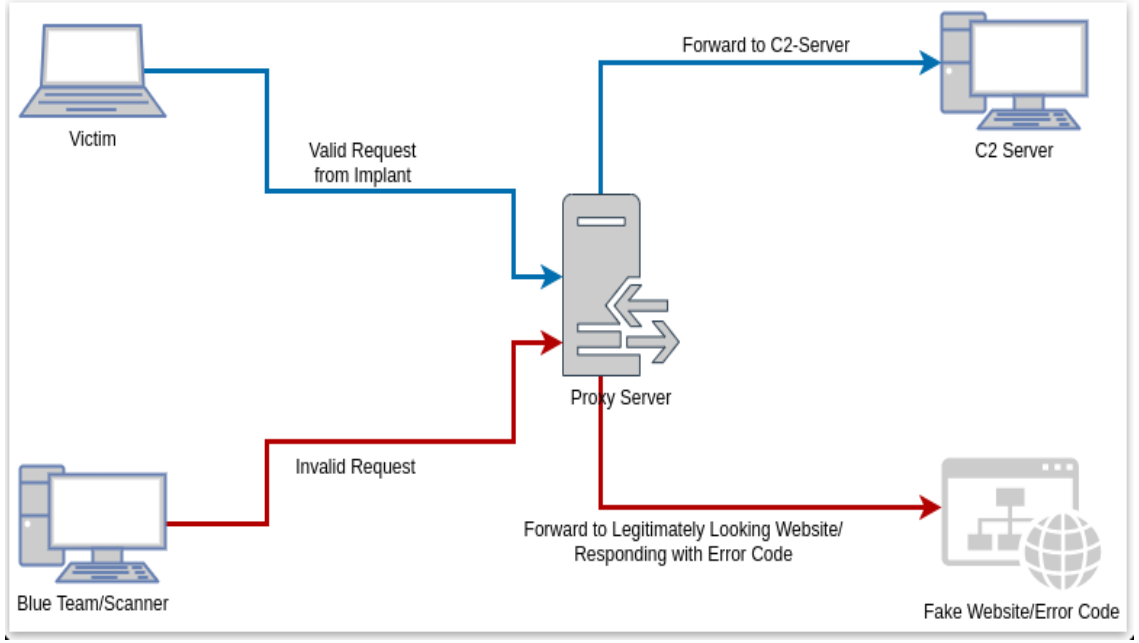
SMTP	HTTPs	DNS
Kratkotrajni (short-haul)	Kratkotrajni (short-haul)	Dugotrajni (long-haul)
Payload (npr. Phishing e-poruke)	C2 + payload (npr. Phishing web stranice)	C2
Više nadgledani	Više nadgledani	Manje nadgledani

HTTPs preusmjerivači

- Dva glavna tipa: jednostavni (pipe) ili reverse web proxy
- **Pipe preusmjerivači**
  - Samo prosljeđuju sav promet koji dolazi do njih dalje
  - Bez kompleksnih pravila i filtriranja prometa
  - Jednostavni za postaviti i upogoniti
  - socat ili iptables

HTTPs preusmjerivači

- **Reverse Web Proxy**
  - Više mogućnosti, npr. filtriranje prometa po geolokaciji, user-agent-u (botovi)...
  - Lakše maskiranje web-prometa i sigurnija dostava implanta (korištenje lažne web stranice)
  - Npr. Apache, nginx ili Caddy



HTTPs preusmjerivači - priprema

- Uvijek HTTPs (ne-enkriptirani promet je sumnjiv i vidljiv na mreži)
- Ne koristiti self-signed certificates, generirati ih sam ili kupiti legitimne
- Moraju se kamuflirati kao stvarni web promet (lakše uz kvalitetan odabir lažnih domena)

Domene

- OSINT (open source intelligence gathering) - koje domene bi mogle funkcionirati za operaciju
  - expireddomains.net, catmyfish, DomainHunter...[3]
- Generalno:
  - Financije, zdravstvo - često izbjegnu filtere (pravni problemi ili osjetljivi podaci)
  - Relevantne teme, npr. Božić
  - Stranice koje izgledaju kao druge (npr. snaphcat.com)
  - Ne koristiti već blacklist-ane domene
  - DGAs - Domain Generation Algorithms

Domene – primjer

- Primjer: Operation Cloud Hopper [7]
  - Globalna kampanja koju je provodila kineska hakerska skupina APT10 (povezana s kineskim Ministarstvom državne sigurnosti)
  - Gađali poslužitelje velikih globalnih pružatelja IT usluga u svrhu krađe informacija o klijentima
  - Koristili domene poput "mailserever.com", "mailsserver.com", "mailvserver.com"...
  - Imali >1300 različitih imena domena

DNS preusmjerivači

- Jednostavnije preusmjeravanje prometa
- Često promakne obrambenim timovima (više se prate drugi oblici mrežnog prometa)
- Može se koristiti za dugotrajno zadržavanje na metinim računalima
- socat ili iptables

Ostale komponente

- Sigurno spremanje podataka - npr. Vaultwarden za vjerodajnice
- SOC softver za praćenje infrastrukture, detekciju njuškanja...
- Alati za automatizaciju
  - Npr. Terraform za podizanje cloud usluga, Vagrant za internu mrežu, Ansible za instalaciju softvera

Dobre prakse - prikrivenost

- Napadčke sustave često je lako identificirati (poslužitelji ne izgledaju legitimno, često su "šuplji")
- Dobri preusmjerivači su ključni (domene, promet koji izgleda legitimno)
- Prikrivanje C2 framework-a i C2 prometa

Dobre prakse - sigurnost

- Infrastruktura za napade je poput bilo kojeg drugog sustava - ranjiva na napade
- Pažljivo filtrirati web promet prema poslužiteljima
- Dobro podesiti dozvole na poslužiteljima, u slučaju kompromitacije (SSH limited-rights, MFA...)

Dobre prakse - sigurnost

- Pratiti nove verzije softvera i zakrpe
- Promjena default postavke, brisanje nepotrebnih datoteka, metapodataka...
- Na kraju, pokušati probiti server (ili dati nekome da to napravi)

Dobre prakse - ostalo

- Dokumentirati sve
- Koristiti postojeće alate i tehnike, osobito ako iskorištavaju poznate slabosti u sustavu
- Pratiti log-ove (SMTP, Apache, tcpdump...)
- Event alerting - npr. pratiti kad se dogodi novo preuzimanje vjerodajnica...
- Istražiti obrambeni odziv
  - Namjerno aktivirati obrambenu reakciju i dobiti uvid u obrambenu infrastrukturu i akcije

Zaključak

- Dobra infrastruktura za napade je "kičma" operacije na koju se sve oslanja
- Postoji mnoštvo postojećih alata i opcija koji olakšavaju dizajn i podešavanje
- Potrebno je obratiti posebnu pozornost na prikrivenost i sigurnost infrastrukture

Literatura

1. systemsecurity.com: "Building a Red Team Infrastructure in 2023", André Tschapeller: https://systemsecurity.com/blog/building-a-red-team-infrastructure-in-2023/
2. medium.com, "Building a Modern Red Team Infrastructure", CYE: https://medium.com/cyesec/building-a-modern-red-team-infrastructure-e5501784a287
3. github.com, "Red Team Infrastructure Wiki": https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
4. C2 Decision Matrix: https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit?gid=0#gid=0
5. Malleable Command & Control, Cobalt Strike: https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/malleable-c2_main.htm?cshid=1062
6. linkedin.com, "Configure your Red Team Operations Infrastructure", Joas A Santos : https://www.linkedin.com/pulse/configure-your-red-team-operations-infrastructure-1-joas-a-santos-a5dsf/
7. "Designing Attack Infrastructure for Offensive Cyberspace Operations", G. Huskaj, I. A. Iftimie, R. L. Wilson: https://www.diva-portal.org/smash/get/diva2:1680076/FULLTEXT01.pdf

Dodatna literatura

- Red Team Notes, "Automating Red Team Infrastructure with Terraform": https://www.ired.team/offensive-security/red-team-infrastructure/automating-red-team-infrastructure-with-terraform
- WithSecure Labs, "Detecting Exposed Cobalt Strike DNS Redirectors": https://labs.withsecure.com/publications/detecting-exposed-cobalt-strike-dns-redirectors
- MaxMind prostorna baza podataka za filtriranje po geolokaciji: https://www.maxmind.com/en/home
- BlueScreenOfJeff, "Invalid URI Redirection with Apache mod_rewrite": https://bluescreenofjeff.com/2016-03-29-invalid-uri-redirection-with-apache-mod_rewrite/

Hvala!