

Sigurnosne prijetnje na Internetu

Infrastruktura kibernetičkog kriminala

Damjan Sirovatka, 8.1.2025

Pregled predavanja

- Motivacija
- Pojam infrastrukture
- Razlog za nastajanje infrastrukture kibernetičkog kriminala
- Infrastruktura kibernetičkog kriminala
- Zaključak

Pitanja za ispit

- Navedi svojstva infrastrukture
- Zašto nastaje infrastruktura kibernetičkog kriminala
- Koji su tipovi infrastrukture korišteni u kibernetičkom kriminalu
- Što je zajedničko administratorima legitimnih i udomljenih nezakonitih foruma
- Koji su rizici kod infrastrukture za nezakonitu aktivnost

2

1. Ugrađenost, Transparentnost, Širok doseg, Učenje članstvom, Povezanost za konvencije, Ovisnost o standardima, Građeno na postojećoj osnovi, Postoji vidljiva u kvaru, Popravlja se u dijelovima
2. Zbog mogućnosti prodaje otkrivenih ranjivosti u obliku lako upotrebljivih alata, te potrebom za tržišnom infrastrukturom
3. Legitimna infrastruktura korištena u svrhe kriminalne aktivnosti i Infrastruktura izgrađena za kibernetički kriminal
4. Žele zaustaviti razgovore tema koje su otvoreno nezakonite, kako forum ne bi bio zatvoren
5. Poslužitelji koji ih neće blokirati, Pristupačnost infrastrukture za izgradnju velike zajednice, Izbjegavanje DDoS napada, Blokiranje automatiziranih čitača stranica

Motivacija

- Što je infrastruktura ?
- Hvatanje kibernetičkih kriminalca
- *Threat intelligence*
- Bolja koordinacija zaštite IS
- Kako utječe na svijet kibernetičkog kriminala ?

Pojam infrastrukture

- Općenito razumijevanje
 - ✓ Ceste,
 - ✓ Tračnice,
 - ✓ Cijevi,
 - ✓ Kanalizacija,
 - ✓ DNS
- Termin *INFRASTRUKTURA* ima značenje ovisno o području primjene

Relacijska definicija infrastrukture

- Definira se s obzirom u kakvom je odnosu sa svojim elementima i korisnicima
- Nisu dovoljni samo objekti, potrebna je i potporna aktivnost
- Definira je 9 svojstava

Svojstva infrastrukture

- Ugrađenost
 - ✓ Postoji kao dio većeg sustava
- Transparentnost
 - ✓ Krajnji korisnik ne vidi da postoji

Svojstva infrastrukture

- Širina dosega
 - ✓ Bavi se s više od jednog događaja ili jednog objekta
- Učenje članstvom
 - ✓ Izvana se čini kao jedan objekt, tek izravnim uvidom se uočava da se radi više nezavisnih objekata
 - ✓ Čija svojstva se uče osmozom

Svojstva infrastrukture

- Povezanost uz konvencije
 - ✓ Prijašnja infrastruktura utječe na konvenciju
 - ✓ Prošle konvencije oblikuju infrastrukturu
- Ovisnost o standardima
 - ✓ Međusobna komunikacija različitih sustava neovisna o konvencijama

Svojstva infrastrukture

- Građeno na postojećoj osnovi
 - ✓ Nova infrastruktura se gradi na osnovi postojećih objekata
- Postaje vidljiva u kvaru
 - ✓ Tek kada nešto prestane raditi, korisnik postaje svjestan postojanja infrastrukture

Svojstva infrastrukture

- Popravlja se u dijelovima
 - ✓ Vrlo kompleksna
 - ✓ Osobito složena kod veza s drugim infrastrukturama

Razlog za nastajanje infrastrukture

- Evolucija napada
 - ✓ Velika šteta, mali volumen
 - ✓ Mala šteta, veliki volumen
- Prepakiranje i prodaja alata
 - ✓ Povod za rast kriminalne ekonomije
- Potreba za sigurnom transakcijom ilegalnih dobara

Infrastruktura – Podjela u kontekstu kibernetičkog kriminala

- **Infrastruktura korištena u kriminalnim aktivnostima**
 - ✓ Tor, Kripto valute, Kripto mjenjačnice, javni forumi
- **Infrastruktura stvorena za kibernetički kriminal**
 - ✓ Deep web tržnice, Botnet, Usluge vezane za zloćudni kod

Infrastruktura korištena u kriminalnim aktivnostima

- Infrastruktura koja nije namijenjena kibernetičkom kriminalu:
 - anonimne komunikacijske mreže,
 - kripto valute,
 - anonimne valute,
 - društvene mreže i aplikacije

Dvije strane administracije

- **Administratori legalnih usluga**
 - Bave se održavanjem legitimnih usluga
 - Nisu vezani za kriminalnu aktivnost
 - Često pokušavaju zaustaviti ilegalnu aktivnost
- **Administratori ilegalnih udomljenih usluga**
 - Održavaju specifične forume (npr. Grupe na telegramu ili discord serveri)
 - Paze da tematika nije otvoreno ilegalna
 - Grade svoje kriterije na osnovi kriterija foruma

Infrastruktura građena sa svrhom nezakonite aktivnosti

- Dijeli se u tri kategorije
 1. Potpora za zloćudni kod
 2. Kriminal kao usluga
 3. Anonimna komunikacija i tržišta

1. Potpora za zloćudni kod

- Usluga prilagođavanja zloćudnog koda
- Tržišta konfiguracijskih datoteka
- Usluga smanjuje razinu znanja potrebnu za korištenje
 - ✓Transparentnost

PRIMJER: Zeus trojanski konj

- Napad na financijske institucije
- Konfiguracija opisuje strukturu sustava koji se napada
- Primjer prijelaza iz alata u infrastrukturu
 - ✓ U početku se prodaje sam kod
 - ✓ Nakon curenja koda, to tržište propada
 - ✓ Nastala usluga pisanja konfiguracijskih datoteka Zeusa
- Sam Zeus postaje tehnički aspekt infrastrukture
- Konfiguracija datoteka je potporni aspekt

2. Kriminal kao usluga

- Napadač nema izravan motiv
- Usluga koju prodaje:
 - Prodaje svoje vještine, alat ili sustav
 - Prodaje se upotreba sustava
 - ✓ Održavanje
 - ✓ Ažuriranje

Kriminal kao usluga - infrastruktura

- Održavanje upravljajućih poslužitelja
- Skeniranje Interneta
 - ✓ Potreban za otkrivanje ranjivih servisa
 - ✓ Zahtjeva svoje poslužitelje
- Pružanje potpore za korisnike
 - ✓ Problemi s plaćanjem
 - ✓ Pitanja u vezi upotrebe usluge

PRIMJER: BotNet

- Skup zaraženih računala
- Najčešće služe za DDoS napad
- Korist javnu mrežnu infrastruktura
- Potrebna zasebna infrastruktura za upravljanje i ponudu kao uslugu

3. Tržišta ilegalnih dobara i usluga, i komunikacija među kriminalcima

- Često se pristupa kroz Tor mrežu
 - Iako nije građena za nezakonitu aktivnost
- Anonimni forumi
 - Dijeljenje znanja i vještina, dijeljenje informacija o tržištima
- Crna tržišta
 - *Crime as a Service*
 - Droga, oružje, ukradeni autentifikacijski podatci
 - Prodaja zloćudnog koda i alata

Održavanje infrastrukture

- Raspon potrebnog znanja
 - ✓ Od visokog za izgradnju tržišta
 - ✓ Do niskog za administrativne poslove

Visoko znanje – potrebno zbog dodatnog rizika

- **Dodatni rizik**
 - ✓ Poslužitelji koji ih neće blokirati
 - ✓ Pristupačnost infrastrukture za izgradnju velike zajednice
 - ✓ Izbjegavanje DDoS napada
 - ✓ Blokiranje automatiziranih čitaća stranica

Visoko znanje – Što je potrebno znati

- Znanje kako upravljati povećanim rizicima
- Određivanje prihvatljivih tema
- Znanje kako upravljati novcem, u slučaju tržnice
- Znanje kako dobiti povjerenje i stvoriti dobru reputaciju

Nisko znanje – Što je potrebno znati

- Otkrivanje botova
- Upravljanje objavljenim sadržajem
- Uobičajeni poslovi moderatora foruma
- Ne tehnička podrška
- Ekstremno bitno za upotrebljivost

Bez ovog posla bi zajednica odumrla

Što sadrži rad na infrastrukturi

- Podržava nezakonitu aktivnost
- Bavi se stabilnosti
- Povodi centralizaciji
- Nije popularno hakerski
- Pažljivo izbjegavanje policije

Zaključak

- Infrastruktura
 - Skup objekata i akcije njihovog održavanja
 - Potporna aktivnost za rad sustava
- Nastaje iz mogućnosti prodaje vještina i usluga
- Razlikuje se općenita i ona građena za nezakonitu aktivnost
- Kao područje rada nije „cool” i dovodi do dosade

Literatura

- Collier, Benjamin, et al. "Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies." (2020)
- STAR, S. L. (1999). The Ethnography of Infrastructure. American Behavioral Scientist, 43(3), 377-391. <https://doi.org/10.1177/00027649921955326>
- Broadhurst, Roderic and Grabosky, Peter and Alazab, Mamoun and Bouhours, Brigitte and Chon, Steve, Organizations and Cybercrime (October 11, 2013). Available at SSRN: <https://ssrn.com/abstract=2345525> or <http://dx.doi.org/10.2139/ssrn.2345525>

Dodatna literatura

- Clayton, R., Moore, T., & Christin, N. (2015). Concentrating correctly on cybercrime concentration. In Workshop on the Economics of Information Security.
- Moore, T., Springer-Verlag New York (2010). Economics of Information Security and Privacy
- Brunt, R., Pandey, P., & McCoy, D. (2017). Booted: An analysis of a payment intervention on a DDoS-for-hire service. In Workshop on the Economics of Information Security.

Hvala!