Sigurnosne prijetnje na Internetu

Crime-as-a-service

Luka Plantak, 16.10.2024.

Pregled predavanja

- Motivacija
- Pitanja za ispite
- Što je CaaS i što omogućuje?
- Kako funkcionira CaaS?
- Pet stupova širenja napadačkih kibernetičkih sposobnosti
- Primjer CaaS-a koristeći RaaS
- Preporuke za suzbijanje širenja napadačkih kibernetičkih sposobnosti
- Zaključak
- Literatura

Pitanja za ispite

- Što je CaaS?
- Što CaaS omogućuje?
- Kako funkcionira CaaS?
- Na koje 3 uloge možemo podijeliti pripadnike kriminalne organizacije koja pruža usluge kibernetičkog kriminala? Ukratko opišite te uloge.
- Nabrojite pet stupova širenja napadačkih kibernetičkih sposobnosti.

Motivacija

- Porastom korištenja Interneta i količine podataka na Internetu, dolazi i do porasta kibernetičkog kriminala
- Kibernetički kriminal sazrijeva i postaje veliki biznis pojavom kibernetičkog kriminala kao usluge (engl. Crime as a service - CaaS)
- U principu svatko s osnovnim poznavanjem kibernetičkog prostora može „naručiti” željeni napad i tako postati kibernetički kriminalac

Motivacija

- Tako kibernetički kriminal postaje organiziraniji, pristupačniji i automatiziraniji
- Bitno je razumjeti kako je to moguće i koje sve vrste napada se mogu „naručiti” kako bi se mogli bolje organizirati i uspješnije zaštititi od takvih prijetnji

Što je CaaS?

- Crime-as-a-service (CaaS) je poslovni model korišten na ilegalnom tržištu u kojem se kupcima pomaže u provođenju kibernetičkih napada na automatiziran način [1]
- Pojam CaaS je analogan softveru kao usluzi (engl. Software as a service - SaaS) - modelu isporuke softvera u kojem su usluge dostupne na zahtjev

Što omogućuje CaaS?

- Prvi kibernetički kriminalci uglavnom su bili hakeri koji su ulazili u kibernetički svijet radi izazova i uzbuđenja
- Ponekad su njihove akcije rezultirale značajnim financijskim gubitcima za žrtve, ali su oni sami imali malu ili nikakvu financijsku korist
- CaaS omogućuje kibernetičkim kriminalcima da ostvare značajnu dobit iznajmljujući svoje vještine ili svoje programe manje vještim kibernetičkim kriminalcima [1]

Kako funkcionira CaaS?

- Kriminalci s tehničkim znanjem razvijaju alate za kibernetičke napade koje mogu koristiti ostali kriminalci koji to znanje ne posjeduju
- CaaS razdvajanja tehničke kibernetičke vještine od tradicionalnijih, ne-kibernetičkih kriminalnih vještina, poput pranja novca [1]

Kako funkcionira CaaS?

- Sve što kupac treba učiniti jest kupiti željenu uslugu kibernetičkog napada i kompromitiranu infrastrukturu
- Kupac ne mora brinuti o kompromitiranju infrastrukture, umetanju virusa u sustav, pokretanju DDoS napada ili krađi podataka o kreditnim karticama jer to automatski obavlja kibernetički kriminalac koji pruža uslugu
- Tako nastaje „podzemni” poslovni sustav

Kako funkcionira CaaS?

- Kao i u legitimnim poduzećima, čelnici organizacije postavljaju poslovni model i infrastrukturu organizacije, donose odluke, nadziru operacije i osiguravaju da sve funkcionira bez problema [2]
- Kada pokrenu operaciju, prelaze na oglašavanje i poslovni razvoj, a „prljavi posao” prepuštaju „običnim vojnicima”
- Regruteri i pješadija

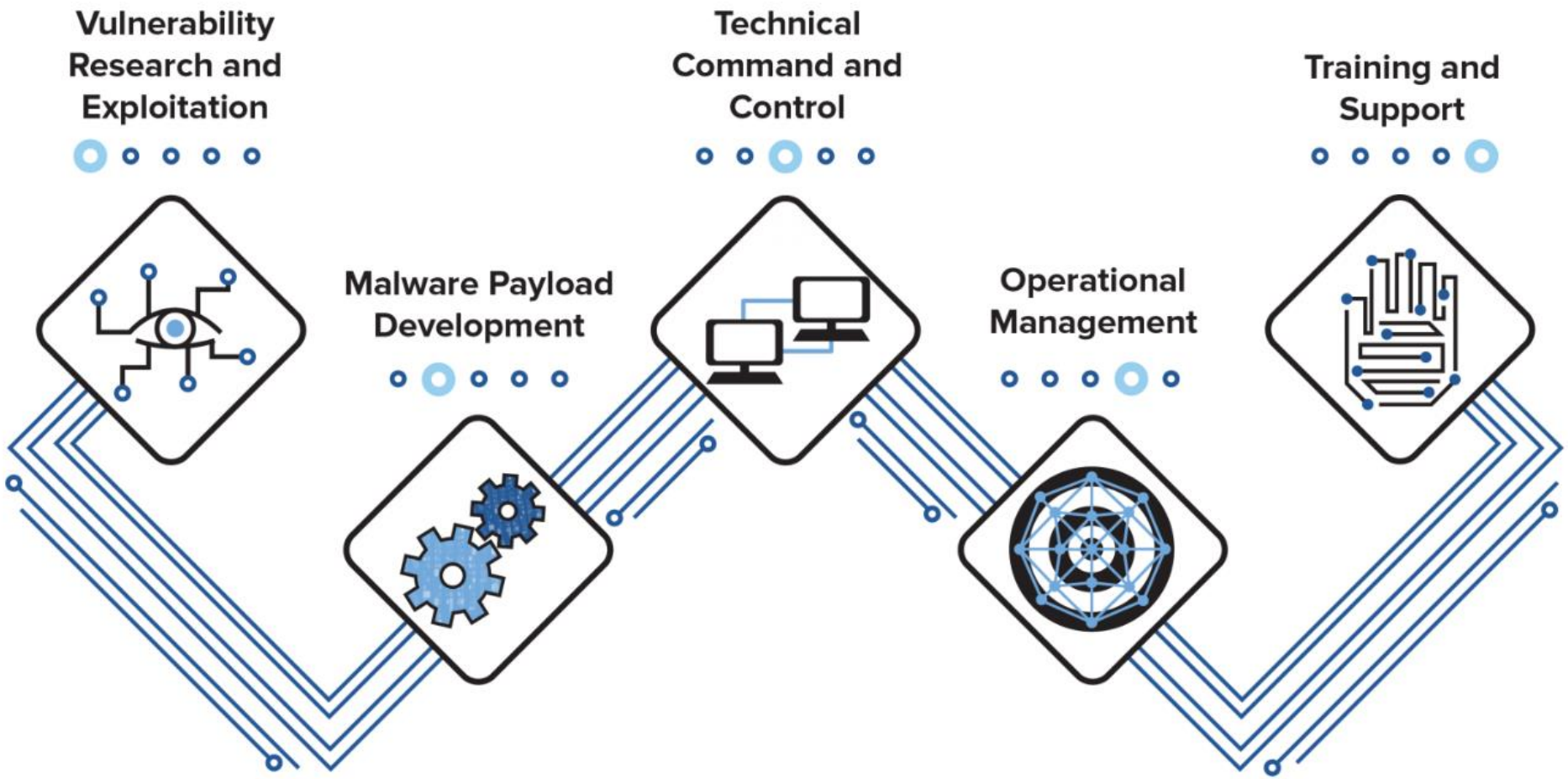
Regruteri

- Aktivno regrutiraju i upravljaju drugima kako bi za njih kompromitirali uređaje
- U operacijama velikih razmjera regruteri uspostavljaju programe regrutacije koje financiraju čelnici kibernetičke kriminalne mreže [2]

Pješadija

- Na dnu zapovjednog lanca
- Regrutiraju ih regruteri za izvođenje napada
- Snage na terenu koje iniciraju stvarni napad na žrtvinom uređaju koristeći jednu ili više poznatih metoda [2]

Pet stupova širenja napadačkih kibernetičkih sposobnosti



[3]

Pet stupova širenja napadačkih kibernetičkih sposobnosti

1. Istraživanje i iskorištavanje ranjivosti [3]
   - Obično u sklopu višefazne operacije
   - Pojedinci, a ponekad i mali timovi, otkrivaju ranjivosti i pišu exploite kako bi ostvarili dodatan pristup ili uporište u ciljanom programu ili uređaju
   - Obuhvaća same ranjivosti, kao i programe za otkrivanje ranjivosti i istraživačke organizacije koje olakšavaju širenje otkrivenih ranjivosti i napisanih exploita

Pet stupova širenja napadačkih kibernetičkih sposobnosti

2. Razvoj malicioznih programa [3]

- Središnji dio mnogih napadačkih kibernetičkih kampanja
- Obuhvaća sve maliciozne programe i alate za njihovu izradu koje napadači koriste u provođenju kibernetičkih napada kao i sve aktivnosti koje potiču ili omogućuju razmjenu tih programa

Pet stupova širenja napadačkih kibernetičkih sposobnosti

3. Tehnička zapovjedna i kontrolna infrastruktura [3]

- Omogućuje napadačima koordinaciju i upravljanje napadima u stvarnom vremenu, održavanje komunikacije sa zaraženim sustavima te provođenje daljnjih operacija bez ometanja, često koristeći alate koji ih štite od pravnih i tehničkih odgovornosti
- Obuhvaća nabavu raznih tehnologija koje podržavaju kibernetičke napade

Pet stupova širenja napadačkih kibernetičkih sposobnosti

4. Upravljanje operacijom [3]

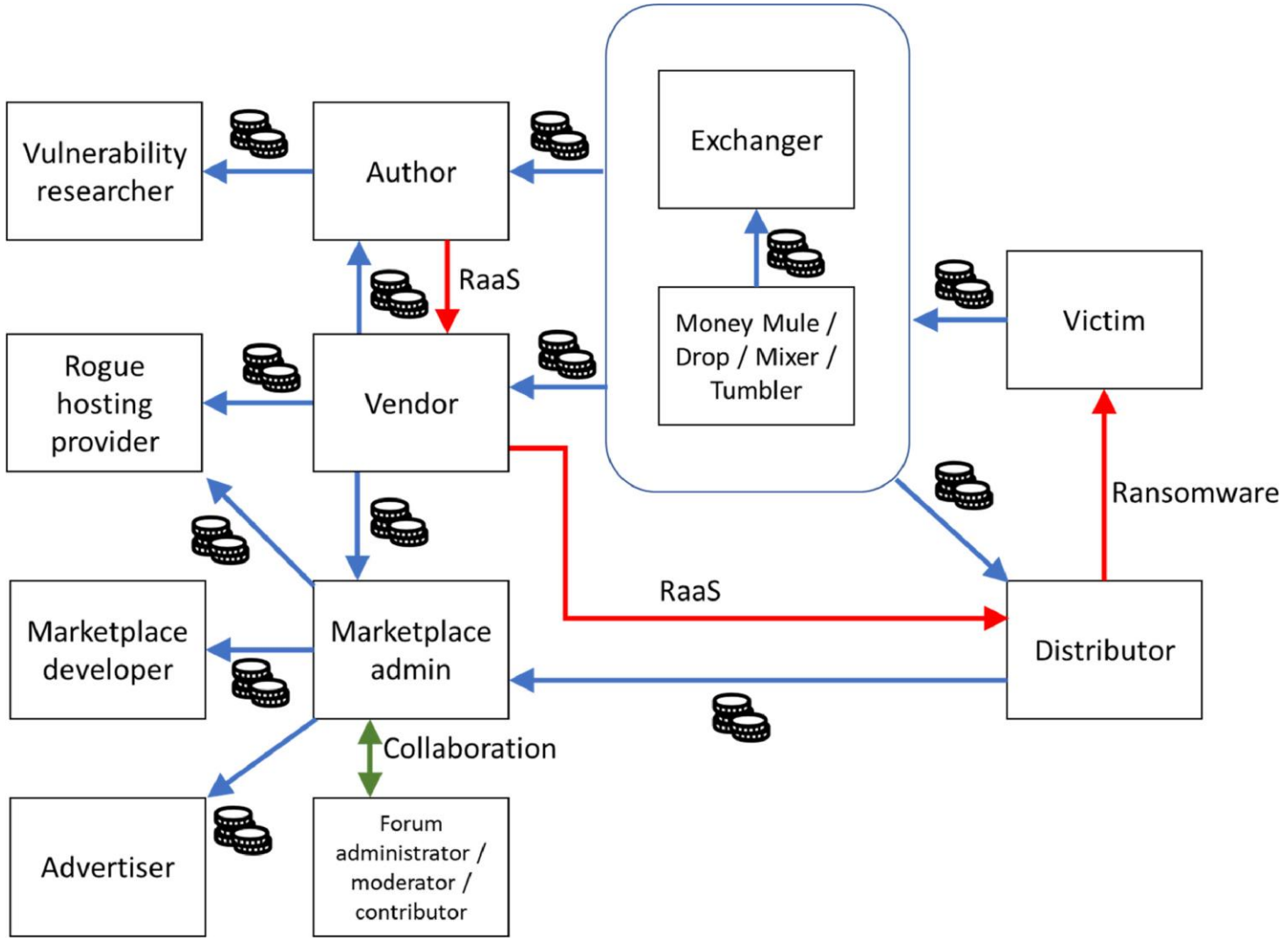
- Osigurava da su resursi i ljudi raspoređeni na način koji omogućuje uspješnu izvedbu napada
- Obuhvaća ljudski aspekt operacija, uključujući upravljanje operacijama, strateško organiziranje resursa i timova, donošenje početnih odluka o ciljevima te ostale funkcije potrebne za učinkovito vođenje organizacije koja provodi kibernetičke napade

Pet stupova širenja napadačkih kibernetičkih sposobnosti

5. Obuka stručnjaka i međusobna podrška [3]

- Ključno za širenje stručnog znanja jer omogućuje sve većem broju pojedinaca uključivanje u provođenje sofisticiranih kibernetičkih napada i stvaranje mreža organizacija koje jačaju kibernetičke operacije kroz kontinuiranu razmjenu znanja i vještina
- Obuhvaća svaki program obuke ili edukaciju koju jedna skupina pojedinaca pruža drugoj u procesu provođenja kibernetičkih napada

Primjer strukture CaaS-a koristeći RaaS



[4]

Primjer strukture CaaS-a koristeći RaaS

- Vulnerability researcher - otkrivaju i prodaju informacije o zero-day ranjivostima drugima koji mogu napisati kod za eksploataciju; veoma stručne osobe, često bivši administratori sustava u uglednim tvrtkama
- Author - profesionalni programeri koji kreiraju maliciozni program koji koristi ranjivosti, od kojih se neke kupuju od Vulnerability researchera
- Vendor – bave se marketingom i prodajom na tržištima ili na vlastitim privatnim web stranicama; mogu biti autori, ali većinom imaju malo programerskog znanja
- Distributor - nabavljaju RaaS i inficira žrtvin uređaj; dijele iskustva i povratne informacije o kupovini ransomwarea
- Victim - pate od infekcija ransomwareom i mogu izgubiti svoje podatke ili platiti otkupninu (ili oboje); ponekad traže pomoć Exchangera kako bi dobili iznos otkupnine u kriptovalutama
- Exchanger - posjeduju verificirane račune i koriste svoj imunitet kako bi nudili usluge mjenjača valuta kibernetičkim kriminalcima ili žrtvama

Primjer strukture CaaS-a koristeći RaaS

- Marketplace admin - osigurava tržišnu platformu koju dobavljači i distributeri mogu koristiti za trgovinu; trebao bi biti pouzdana treća strana koja upravlja novčanim transakcijama (ponekad pobjegnu s novcem)
- Marketplace developer - osoba sa tehničkim znanjem koja razvija platforme tržišta za administratore; zahtijeva visoku sigurnosnu kompetenciju
- Advertiser - objavljuje Darknet poveznice na površinskom webu i prima novčanu proviziju kada dođe do uspješnih transakcija proizašlih iz tih poveznica (npr. DeepDotWeb)
- Forum admin/moderator / contributor - osobe odgovorne za upravljanje sadržajem foruma i pružanje pristupa članovima; često imaju blizak odnos s administratorom jednog ili većeg broja tržišta
- Rogue hosting provider - pružaju usluge hostinga web stranica na Darknetu koje smanjuju rizik da će kriminalci biti uhvaćeni
- Money Mule / Drop / Mixer / Tumbler – prenose transakcije primljene od žrtava; ili profesionalni perači novca ili netko tko nesvjesno prosljeđuje novac

Preporuke za suzbijanje širenja napadačkih kibernetičkih sposobnosti

1. Razumijevanje i udruživanje [3]

- Izgradnja koalicije država istomišljenika
- Širenje vijesti o kibernetičkim napadima na međunarodnim forumima kako bi se pokušalo posramiti napadače
- Usvajanje zakona ili regulativa „poznaj svojeg dobavljača” za lakšu provjeru lanca opskrbe (veću transparentnost i pomoć u ograničavanju CaaS transakcija s dobavljačima koji posluju sa kriminalnim organizacijama)

Preporuke za suzbijanje širenja napadačkih kibernetičkih sposobnosti

2. Oblikovanje [3]

- Priznavanje postojanja tržišta za Caas usluge, infiltriranje na to tržište i razvijanje lista zabrane za dobavljače uhvaćene u prodaji kriminalnih usluga
- Poticanje poduzeća da imaju etički odbor koji objavljuje polugodišnja javna izvješća o tvrtki kao uvjet podobnosti za državne ugovore
- Ograničavanje prodaje poduzećima koja imaju poznate veze sa CaaS organizacijama

Preporuke za suzbijanje širenja napadačkih kibernetičkih sposobnosti

3. Ograničavanje [3]

- Ograničavanje širenja relevantnih alata i stručnjaka CaaS-a, koliko je to moguće
- Uspostava ograničenja nakon prestanka radnog odnosa za bivše vladine zaposlenike zadužene za kibernetičku sigurnost
- Pokretanje pravnih postupaka protiv pružatelja CaaS usluga i njihovih suradnika

Zaključak

- Pomisao da zbog CaaS-a svatko može uz dovoljno financijskih sredstava lako postati kibernetički kriminalac zastrašujuća je
- Takva vrsta kibernetičkog kriminala neprestano se širi zbog prihoda koje stvara kibernetičkim kriminalcima
- Još uvijek nije prekasno za sprječavanje širenja CaaS-a korištenjem danih preporuka

Literatura

- [1] Sood, Aditya K., and Richard J. Enbody. "Crimeware-as-a-service—a survey of commoditized crimeware in the underground market." International journal of critical infrastructure protection 6.1 (2013): 28-38
- [2] Manky, Derek. "Cybercrime as a service: a very modern business." Computer Fraud & Security 2013.6 (2013): 9-13
- [3] DeSombre W., Shires J., Work JD, Morgus R., Howell O'Neill P., Allodi L. and Herr T. „Countering cyber proliferation: Zeroing in on Access-as-a-Service", 1.3.2021., pristupljeno: 13.10.2024., poveznica: https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/
- [4] Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. "The Ransomware-as-a-Service economy within the darknet." Computers & Security 92 (2020): 101762.

Dodatna literatura

- Šembera, Vít, et al. "Cybercrime specialization: An exposé of a malicious Android Obfuscation-as-a-Service." 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2021.
  → primjena CaaS-a za obfuskaciju Android aplikacija

Hvala!