Forenzička analiza kibernetičkih napada

Matić, Antonio

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Antonio Matić

FORENZIČKA ANALIZA KIBERNETIČKIH NAPADA

DIPLOMSKI RAD

Varaždin, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Antonio Matić

Matični broj: 0016143409

Studij: Informacijsko i programsko inženjerstvo

FORENZIČKA ANALIZA KIBERNETIČKIH NAPADA

DIPLOMSKI RAD

Mentor:

Doc. dr. sc. Igor Tomičić

Varaždin, srpanj 2024.

Antonio Matić

Izjava o izvornosti

Izjavljujem da je moj diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Ovaj rad istražuje evoluciju kibernetičkih napada s posebnim naglaskom na digitalnu forenziku i strategije kibernetičke sigurnosti. Analiziraju se različite vrste kibernetičkih napada te detekcijski mehanizmi koji se koriste za njihovo prepoznavanje i odgovaranje na prijetnje. Kibernetičke prijetnje postaju sve sofisticiranije zahvaljujući razvoju umjetne inteligencije i drugih tehnologija, što napadačima omogućuje učinkovitije zaobilaženje tradicionalnih sigurnosnih mjera. Rad započinje pregledom općih principa okvira kibernetičke sigurnosti te analizira faze napada prema MITRE ATT&CK okviru, pružajući detaljan pregled taktika, tehnika i procedura koje napadači koriste. Posebno se razmatraju faze kao što su pristup vjerodajnicama, otkrivanje sustava i lateralno kretanje, uz analizu detekcijskih mehanizama temeljenih na potpisima, anomalijama, statističkim metodama, znanju, rudarenju podataka i strojnom učenju. Kao konkretan primjer, detaljno se analizira zlonamjerni softver Redline, usmjeren na krađu podataka i korisničkih vjerodajnica. Uzorak softvera izvršava se u kontroliranom virtualnom okruženju kako bi se dobio dublji uvid u njegove radnje i utjecaj. Na temelju rezultata analize kreira se detekcijsko pravilo za implementaciju u alate za upravljanje informacijskom i kibernetičkom sigurnosti, olakšavajući otkrivanje i rješavanje budućih napada.

Ključne riječi: informacijska sigurnost; kibernetički napadi; forenzička analiza; mrežni promet; zlonamjerni softver; Redline

Sadržaj

1. Uvod

Ovaj rad ima za cilj istražiti kibernetičke napade i njihovu evoluciju s naglaskom na digitalnu forenziku i strategije kibernetičke sigurnosti. Rad će obuhvatiti različite vrste kibernetičkih napada i detekcijskih mehanizama koji se koriste za prepoznavanje i odgovaranje na te prijetnje. Kroz konkretne primjere napada, rad će prikazati kako se kibernetičke prijetnje razvijaju te identificirati uobičajene obrasce napada koji mogu poslužiti za unapređenje strategija kibernetičke sigurnosti.

U prvom dijelu rada bit će prikazani opći principi okvira kibernetičke sigurnosti te vrste i primjeri kibernetičkih napada. Analizirat će se faze napada prema MITRE ATT&CK okviru, pružajući detaljan pregled taktika, tehnika i procedura koje napadači koriste. Posebna pažnja bit će posvećena fazama kao što su pristup vjerodajnicama, otkrivanje sustava i lateralno kretanje. Također, bit će analizirani mehanizmi za detekciju napada, uključujući one temeljene na potpisima, anomalijama, statističkim metodama, znanju, rudarenju podataka i strojnom učenju.

Primjeri konkretnih napada ilustrirat će teorijske koncepte i omogućiti dublje razumijevanje stvarnih prijetnji. Kroz analizu uzorka Redline softvera, bit će prikazan detaljan proces forenzičke analize konkretnog malware napada, ali principi će se moći primijeniti na sve vrste napada. Analiza će se provoditi korištenjem tehnika statičke i dinamičke analize, uključujući pregled izvršne datoteke, identifikaciju vrste datoteke, generiranje sažetaka te dekompilaciju uzorka s pomoću alata kao što su Ghidra i IDA Pro. Dinamička analiza uključivat će izvođenje uzorka u kontroliranom okruženju te promatranje njegovog ponašanja, uključujući mrežni promet analiziran s pomoću Wiresharka.

Na kraju ove analize bit će prikazan proces kreiranja Sigma pravila za detekciju Redline softvera. Ovo pravilo omogućit će pravovremenu detekciju i odgovaranje na prijetnje, što je ključno za zaštitu organizacija od kibernetičkih napada. Osim toga, identificirani indikatori kompromitiranosti pružit će konkretne smjernice za unapređenje sigurnosnih mjera. Razumijevanje taktika i tehnika napadača ključno je za razvoj učinkovitih strategija zaštite i obrane, te doprinosi boljem razumijevanju suvremenih prijetnji informacijskoj sigurnosti. Sve to doprinosi jačanju sveukupne otpornosti organizacija i pojedinaca na kibernetičke prijetnje kroz razvoj kvalitetnih strategija kibernetičke sigurnosti i jačanje svijesti o kibernetičkoj sigurnosti.

2. Metode i tehnike rada

U ovome su radu pri razradi teme kroz analizu postojeće literature i razumijevanje iste objašnjene faze procesa kibernetičkih napada te su objašnjeni ključni pojmovi kako bi se omogućilo bolje razumijevanje sadržaja iz ove domene i samog rada.

Analizom studija slučaja, konkretnije na primjeru zlonamjernog softvera naziva Redline se kroz forenzičku analizu jedne varijacije Redline softvera u virtualnom okruženju u oblaku zaključilo o detaljima funkcioniranja tog softvera jednom kada je pokrenut na računalu. Dakle, uzorak jedne varijacije ovog softvera pokrenut je u virtualnom okruženju nakon čega se pratio i dokumentirao proces djelovanja samog softvera te je sve to dokumentirano i komentirano kroz rad. Redline je korišten u raznim napadima i još se uvijek često pojavljuje, a služi za krađu osjetljivih podataka poput osobnih podataka ili podataka za prijavu u razne sustave. Zbog toga je na primjeru ovog softvera kritički analizirana i dostupna literatura o utjecajnijim napadima koji su uključivali Redline softver, a sve to u svrhu prikazivanja evoluirajuće prirode kibernetičkih prijetnji i načina na koji se napadači, vrlo kreativno, dosjete zaobići postojeće tehničke mjere zaštite i ostvariti svoje zlonamjerne ciljeve. Ta je literatura najčešće rezultat provedenih istraživanja određenih napada ili konkretnog zlonamjernog softvera nekih od poznatih tvrtki za kibernetičku i mrežnu sigurnost koje imaju svoje laboratorije za razvoj i istraživanje unutar kojih stručnjaci pomno istražuju sve aspekte određenog napada.

Za statičku analizu koda korišten je alat Ghidra koji dekompilira izvršnu datoteku čime postaje vidljiv njen izvorni kod u C programskom jeziku, a za dinamičku analizu korištene su online platforme u oblaku Any.Run te Hybrid Analysis. Na te je platforme učitan uzorak Redline softvera koji je automatski izvršen te je analizirano njegovo ponašanje uključujući kreirane procese, uređene vrijednosti registara, kontaktirane domene te cijeli mrežni promet. Mrežni promet preuzet je s platforme u PCAP formatu nakon čega je analiziran kroz Wireshark alat za analizu mrežnog prometa.

Sve tehničke analize koje su rađene za potrebe ovog rada su izvršavane u kontroliranom i izoliranom okruženju bez opasnosti od zaraze drugih računala u mreži. Stručni članci, objavljeni materijali te sva druga korištena literatura naznačena citatima jest popisana na kraju ovoga rada u popisu literature za referencu na izvorni sadržaj iz kojega je određena izjava preuzeta.

3. Digitalna Forenzika u kibernetičkoj sigurnosti

Digitalna forenzika je grana znanosti koja uključuje primjenu znanstvenih principa u istrazi artefakata prisutnih u jednom ili više digitalnih uređaja u svrhu razumijevanja i rekonstruiranja slijeda događaja koji su se morali dogoditi da bi se spomenuti artefakti generirali [1].

Digitalna forenzika uključuje različite domene poput forenzike mrežnih uređaja, baza podataka, mobilnih uređaja, sustava u oblaku, memorije i pohrane [2].

U ovome je smislu digitalna forenzika bitan element cjelokupne sigurnosti organizacija i njihovih zaposlenika te klijenata. Samim time, ključna je za pravilno rukovanje, prikupljanje i prezentaciju dokaza pred sudom u slučajevima kada je to potrebno. Budući da je to specifična domena unutar forenzike, mnogi su principi preneseni iz svijeta forenzike u svijet digitalne forenzike kao što je npr. fotografiranje stanja digitalnih uređaja na mjestu „zločina“, stavljanje dokaza u vrećice za dokaze što je dalje specificirano u slučaju digitalne forenzike na posebne vrste materijala koji su anti-statički, štite uređaje od vanjskih signala itd. Ta je povezanost vidljiva i u strogoj uređenosti digitalne forenzike različitim standardima kojima se osigurava maksimalan integritet samih dokaza te uspješnost procesa pronalaska digitalnih dokaza.

Istraživanja pokazuju eksponencijalni rast kibernetičkih prijetnji i napada te se zbog toga naglašava nužnost za forenzičkim stručnjacima i istražiteljima u procesima unutar kibernetičke sigurnosti. Ova se grana znanosti direktno veže na oporavak i prikupljanje podataka što znatno otežava stručnjacima ovoga područja zbog ubrzanog rasta količine podataka [2].

3.1. Osnovni procesi digitalne forenzike

Digitalna je forenzika višefazni proces koji započinje identifikacijom digitalnih medija s poprišta (odnosno mogućeg mjesta zločina) koji sadrže potencijalni dokaz do krajnje faze kada stručnjak taj dokaz prezentira pred sudom. Te faze su sljedeće: Identifikacija dokaza, Prikupljanje i očuvanje dokaza, Ispitivanje dokaza, Analiza dokaza, Dokumentacija te Prezentacija dokaza [1].

Dakle, nakon identifikacije relevantnih medija koji mogu sadržavati dokaze o izvršenim radnjama ili prikupljenim informacijama kao što su USB memorija, tvrdi diskovi, radna memorija uređaja itd. potrebno je prikupiti sve te medije na siguran način. Jedna od stavki koja je uvijek važna za istaknuti je da se operacije s direktnim pristupom izvoru dokaza svode na minimum, odnosno ne bi se nikada trebale odvijati. U slučaju nužnosti, takve operacije može izvesti samo potvrđeni stručnjak. Razlog tome je što se bilo kakvim direktnim pristupom dokazi mogu izmijeniti, obrisati ili se na bilo koji način može narušiti njihov integritet. Zato se na licu

mjesta koriste posebni uređaji i softveri za prikupljanje dokaza te kreiranje identičnih kopija izvornih diskova čime se osigurava da su izvorni dokazi nepromijenjeni i mogu služiti kao valjan dokaz na sudu, a cijela se analiza radi na identičnim podacima bez opasnosti narušavanja integriteta izvornih medija. Način očuvanja integriteta i način za dokazivanje da je npr. sadržaj kopije tvrdog diska identičan sadržaju na izvornom tvrdom disku je korištenje funkcija sažimanja (eng. *Hashing Functions*). Koristeći funkciju sažimanja nad obje pohrane dobivaju se dva sažetka. Ako su oni identični, to znači da je identičan i sadržaj na njima zbog prirode funkcija sažimanja koji za isti sadržaj na ulazu uvijek daju isti izlazni sažetak uz napomenu da i najmanja promjena sadržaja utječe na potpuno drukčiji sažetak. Primjer funkcije sažimanja koja se najčešće koristi je SHA256.

Cijeli proces kroz sve faze temelji se dakle na pronalaženju, prikupljanju te analizi i prezentaciji dokaza imajući na umu očuvanje integriteta svih dokaza. Kroz ovaj će se rad analizom različitih studija slučaja kibernetičkih napada prikazati njihova metodologija uz objašnjenje uloge forenzičke analize u različitim fazama napada imajući na umu prikupljanje indikatora kompromitacije, povezanih alata ili relevantnih digitalnih medija koji mogu biti izvor dokaza u različitim scenarijima.

4. Proces kibernetičkih napada

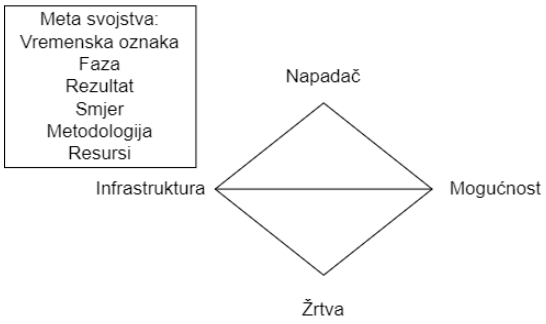
Da bi se neki proces mogao pratiti od početka do kraja klasificirajući određene aktivnosti u povezane cjeline sličnih aktivnosti, potrebno je imati dogovor o takvoj klasifikaciji. Kao i sve druge industrije, ovdje su prisutni određeni standardi koji klasificiraju korake kibernetičkih napada predstavljajući ih kao faze cjelokupnog procesa. Postoji više modela i okvira koji su priznati unutar industrije, međutim tri su najpopularnija: CKC model (eng. *Cyber Kill Chain*), MITRE ATT&CK okvir te Dijamantni model upada (eng. *Diamond Model of Intrusion*). U nastavku su svaki od navedenih modela ukratko objašnjeni, a na kraju je poglavlja objašnjena i glavna razlika između CKC modela i MITRE ATT&CK okvira. To će se znanje kasnije koristiti prilikom konkretne analize kibernetičkih napada kako bi se bolje razumjele aktivnosti, taktike i metode napadača te sustavno mapirale konkretne aktivnosti na faze napada. Iako su objašnjena sva tri modela, u radu će se fokus staviti na MITRE ATT&CK okvir zbog detaljnije razine klasifikacije faza napada u odnosu na druge okvire.

4.1. Dijamantni model upada

Predstavljen oblikom dijamanta prikazuje odnose unutar napada zasnovane na njegove 4 komponente, a to su napadač, infrastruktura, mogućnost te žrtva. Svaka od tih komponenti predstavlja po jedan vrh dijamanta u grafičkom prikazu.

Kako se navodi i u objavi SOCRadar-a [3], ovo je kognitivni model koji objašnjava kako napadač iskorištava mogućnost na infrastrukturi protiv žrtve, a sam model omogućava sigurnosnim stručnjacima organizirati velike količine povezanih elemenata.

Najčešće se koristi u prvom koraku analize za razumijevanje odnosa elemenata napada, a zatim se prelazi u detaljniju analizu prema fazama napada koje opisuju CKC Model te ATT&CK okvir opisani u nastavku.



Slika 1 Dijamantni modela upada (Prema CyCraft, 2022. [4])

4.2. Cyber Kill Chain Model

Ovaj se model zasniva na fazama i osmišljen je da bi pomogao sigurnosnim stručnjacima razumjeti napad te ga raščlaniti na sedam koraka prema kojima mogu razviti obranu koja se temelji na ometanju bilo kojeg od sljedećih koraka napada [5]:

Tablica 1 Faze napada prema CKC modelu

Naziv faze	Opis
Izviđanje (eng. *Reconnaissance*)	Prikupljanje informacija, istraživanje mete i ranjivosti koje mogu biti iskorištene. Koriste se alati za automatsko skeniranje ili ručno skeniranje
Naoružavanje (eng. *Weaponization*)	Kreira se zlonamjerni softver da bi se eksploatirale identificirane ranjivosti
Dostava (eng. *Delivery*)	Dostavlja se zlonamjerni softver prema meti
Eksploatacija (eng. *Exploitation*)	Eksploatiraju se ranjivosti koristeći dostavljeni zlonamjerni softver da bi se dobio veći pristup unutar mreže
Instalacija (eng. *Installation*)	Instaliraju se dodatni programi koji omogućuju perzistentnost i nedetektirani pristup
Zapovijedanje i upravljanje (eng *Command and Control*)	Napadač uspostavlja komunikaciju za upravljanje kompromitiranim sustavima i upravlja njima putem tog komunikacijskog kanala
Djelovanje prema ciljevima (eng. *Actions on objectives*)	Napadač poduzima sve potrebne radnje da bi ostvario ciljeve napada koji mogu biti eksfiltracija, modifikacija, uništenje ili enkripcija podataka ili nešto drugo

(Prema: Naik et al., 2022 [5])

4.3. MITRE ATT&CK Okvir

Ovaj je okvir globalno pristupačna baza znanja napadačkih taktika i tehnika koje su zabilježene u stvarnom svijetu. Zapravo pruža strukturiranu listu poznatih ponašanja napadača koje su svrstane u taktike i tehnike te prikazane kao slijed matrica [4].

Različite tehnike upada svrstane su u 14 različitih taktika kako slijedi u tablici [5]:

Tablica 2 Faze MITRE ATT&CK okvira

Naziv faze	Opis
Izviđanje (eng. *Reconnaissance*)	Prikupljanje informacija o meti
Razvoj resursa (eng. *Resource Development)*	Prikupljanje i osiguravanje resursa za buduće radnje u svrhu ostvarenja ciljeva
Inicijalni pristup (eng. *Initial access*)	Ostvarenje inicijalnog pristupa
Izvršenje (eng. *Execution*)	Pokretanje zlonamjernog softvera
Perzistentnost (eng. *Persistence*)	Održavanje kontinuiranog pristupa sustavu
Eskalacija privilegija (eng. *Privilege Escalation*)	Ostvarenje viših privilegija unutar sustava od početno ostvarenih
Izbjegavanje obrane (eng. *Defense evasion*)	Izbjegavanje postavljenih mjera zaštite i obrane raznim tehnikama
Pristup vjerodajnicama (eng. *Credential Access*)	Preuzimanje korisničkih vjerodajnica za pristup tom ili drugim sustavima
Otkrivanje (eng. *Discovery*)	Detaljnije istraživanje sustava i okruženja
Lateralno kretanje (eng. *Lateral Movement*)	Kretanje kroz okruženje i sustave s istim pravima (bez eskalacije privilegija)
Prikupljanje (eng. *Collection*)	Prikupljanje informacija relevantnih za cilj
Zapovijedanje i upravljanje (eng. *Command and Control*)	Komuniciranje napadača s kompromitiranim sustavima uz uspostavu kontrole
Eksfiltracija (eng. *Exfiltration*)	Krađa podataka s kompromitiranog sustava
Utjecaj (eng. *Impact*)	Manipulacija, ometanje, uništavanje sustava

(Prema: Naik et al., 2022 [5])

5. Okvir kibernetičke sigurnosti

Okvir kibernetičke sigurnosti (eng. *Cybersecurity Framework*) u ovome smislu je okvir koji ima za cilj obranu od kibernetičkih kriminalaca. Sastoji se od pet faza: identifikacija, zaštita, detekcija, odgovor i oporavak [6].

Kada se govori o strategijama kibernetičke sigurnosti pojedinih organizacija, bitno je naglasiti da se one trebaju temeljiti na općeprihvaćenim standardima, okvirima ili drugim idejama unutar industrije. Time se osigurava sustavan pristup određenoj domeni, a u ovome slučaju to je pristup obrani od kibernetičkih napada odnosno jačanju sigurnosne posture cjelokupne organizacije.

5.1. Faze i aktivnosti unutar okvira kibernetičke sigurnosti

Dakle, kako se navodi u uputama NIST-a (eng. *National Institute of Standards and Technology*) [7], prvi je korak u implementaciji kibernetičkih mjera identifikacija i razumijevanje fizičkih i logičkih resursa kojima se raspolaže i o kojima se treba voditi računa, čimbenicima rizika kao npr. tko ima pravo pristupa informacijama, postavljenim politikama, identifikacijom ranjivosti na identificiranim resursima itd. To je naravno vrlo bitno jer da bi se nešto zaštitilo, mora se znati što se uopće štiti.

Nakon toga slijedi odgovarajuća zaštita tih resursa kroz npr. ograničavanje fizičkog i logičkog pristupa, postavljanje email filtera ili konfiguracija pravila vatrozida, primjena enkripcijskih mehanizama, naročito nad povjerljivim informacijama, zaštita bežičnih pristupnih točaka, održavanje resursa kroz redovito ažuriranje, primjene sigurnosnih zakrpa i druge procese redovnog održavanja. Za fazu zaštite važno je reći i da je potrebno provoditi pravilnu i temeljitu edukaciju ljudi o kibernetičkim prijetnjama i sigurnosti jer su oni danas najčešća meta kada je u procesu napada potrebno osigurati inicijalni pristup, prikupiti informacije ili čak izvršiti eskalaciju privilegija.

U fazi detekcije koriste se različiti tzv. detekcijski mehanizmi koji omogućavaju i reaktivnu i proaktivnu zaštitu organizacije. U ovoj fazi važno je osigurati da se svako pojavljivanje sigurnosnog događaja ispravno identificira te se vrši kontinuiran nadzor, a to se postiže aktivnostima poput implementacije odgovarajućih detekcijskih mehanizama koji identificiraju i izbjegavaju maliciozne datoteke. Takvi su mehanizmi npr. politike antivirusnog softvera, nadzor logova itd. Više o samim detekcijskim mehanizmima bit će opisano u nastavku.

Faza odgovora uključuje aktivnosti poduzimanja radnji u odgovoru na detektirani kibernetički incident. Ovime se podržava mogućnost smanjenja utjecaja potencijalnog incidenta. Radnje koje se kao primjer navode u NIST dokumentu [6] su osiguravanje da su

tijekom i nakon incidenta izvršeni svi procesi iz dokumenta s planom odgovora, upravljanje komunikacijama tijekom i nakon događaja sa svim sudionicima, državnim službenicima te vanjskim sudionicima prema potrebi. Osim toga, analiza treba biti izvršena tako da osigurava učinkovit odgovor i podržava aktivnosti oporavka uključujući i forenzičku analizu kao i određivanje utjecaja incidenta. Nakon toga, potrebno je implementirati poboljšanja u okruženje koristeći sve naučene lekcije iz proteklog incidenta, uočiti što je moglo biti bolje i to poboljšati te uočiti što je bilo dobro i to nastaviti raditi.

U fazi oporavka organizacija se vraća u normalno, uobičajeno funkcioniranje, a aktivnosti koje tu spadaju su osiguravanje da organizacija implementira procese iz dokumenta planiranja oporavka kao i procedure za vraćanje sustava i drugih resursa pogođenih napadom u normalno stanje u kakvom su bili prije napada, poboljšanja na temelju naučenih lekcija itd.

5.2. Detekcijski mehanizmi

Moguće je podijeliti mehanizme u nekoliko vrsta na temelju načina na koji detektiraju potencijalne prijetnje te procesu na koji se pri tome oslanjaju. To su sljedeće vrste: Mehanizmi temeljeni na potpisu (eng. *Signature-based Mechanisms*), Mehanizmi temeljeni na anomalijama (eng. *Anomaly-based Mechanisms*), Tehnike temeljene na statistici (eng. *Statistical-based Detection Techniques*), Tehnike temeljene na znaju (eng. *Knowledge-based Techniques*), Tehnike temeljene na rudarenju podataka (eng. *Data mining-based Techniques*), Tehnike temeljene na strojnom učenju (eng. *Machine Learning-based Techniques*).

Za svaku navedenu vrstu ovaj članak [7] daje detaljnije objašnjenje:

- **Mehanizmi temeljeni na potpisu**
    - Detektiraju poznate napade usporedbom s prethodnim obrascima. Prepoznaju samo poznate napade i zahtijevaju redovito ažuriranje. Imaju nisku stopu lažno pozitivnih rezultata, ali zahtijevaju veliku procesorsku snagu.
- **Mehanizmi temeljeni na anomalijama**
    - Detektiraju nepoznate napade analizom sumnjivog ili neobičnog ponašanja. Potrebna je obuka s uobičajenim obrascima ponašanja. Imaju visoku stopu lažno pozitivnih rezultata jer svako odstupanje od normalnog može biti identificirano kao napad.
- **Tehnike temeljene na statistici**
    - Grade model koristeći statističke osobine poput srednje vrijednosti i varijance. Mogu otkriti napade nultog dana (eng. *Zero-day Attacks*) bez poznavanja obrasca napada, ali zahtijevaju veliku procesorsku snagu.

- **Tehnike temeljene na znanju**
    - Detektiraju napade koristeći znanje iz prethodnih napada i ranjivosti. Koriste se u potpisnim i anomalijskim mehanizmima. Imaju nisku stopu lažnih alarma, ali zahtijevaju veliku procesorsku snagu i stalno ažuriranje podataka.
- **Tehnike temeljene na rudarenju podataka**
    - Pomažu u otkrivanju unutarnjih napada analizom obrazaca prethodnih napada koji su bili uspješni. Koriste metode stabla odluke, tehnike grupiranja i rudarenje pravila udruženja. Zahtijevaju veliku pohranu za obradu i izračun rezultata.
- **Tehnike temeljene na strojnom učenju**
    - Detektiraju napade koristeći okvire izgrađene na temelju prethodnih znanja o napadima. Dijele se na nadzirano i nenadzirano učenje. Nenadzirane tehnike mogu detektirati napade nultog dana.

5.3. Preporuke za unapređenje strategije kibernetičke sigurnosti

Formiranje i održavanje učinkovite strategije kibernetičke sigurnosti ključno je za zaštitu organizacije od rastućih prijetnji. Implementacijom sveobuhvatnog pristupa koji uključuje tehničke, administrativne i fizičke kontrole, te kontinuirano praćenje i reviziju sigurnosnih mjera, organizacije mogu značajno smanjiti rizik od kibernetičkih napada i osigurati kontinuitet poslovanja. Sve to može se zaključiti u sljedećih 5 procesa:

1. **Proaktivno praćenje prijetnji**: Uvođenje naprednih sustava za praćenje prijetnji i obavještavanje o potencijalnim rizicima.
2. **Stalna edukacija zaposlenika**: Kontinuirano obrazovanje i osvježavanje znanja o sigurnosnim prijetnjama i praksama.
3. **Redovita ažuriranja i zakrpe**: Osiguravanje da su svi sustavi i softveri redovito ažurirani kako bi se smanjio broj ranjivosti unutar sustava, a time i površina napada.
4. **Integracija sigurnosnih alata**: Korištenje alata kao što su KAPE, FTK Imager, Volatility i Autopsy za učinkovitu analizu i odgovor na incidente.
5. **Suradnja i dijeljenje informacija**: Aktivno sudjelovanje u zajednicama za kibernetičku sigurnost i razmjena informacija o prijetnjama i najboljim praksama

6. Kibernetički napadi

Kibernetički napadi sve su češći, a definiraju se većinom kao zlonamjerni pokušaji malicioznih činitelja da pristupe, oštete ili ometaju računalne sustave, mreže ili uređaje, često s ciljem krađe podataka, narušavanja rada sustava i ljudi ili ostvarivanja financijske koristi. S trendom rasta digitalizacije poslovanja dolazi do sve veće količine informacija u digitalnom obliku koji kao meta malicioznih činitelja posljedično kreiraju rast broja kibernetičkih napada. Inovativnim pristupom konstantno se nalaze novi načini zaobilaženja postavljenih mjera zaštite te se ugrožava sigurnost pohranjenih informacija, a samim time i sigurnost te privatnost pojedinaca i organizacija.

6.1. Vrste kibernetičkih napada

Kibernetički su napadi većinom podijeljeni u nekoliko vrsta kako bi se lakše organizirale metode, principi te pristupi strategijama sigurnosti prema svakoj od njih. Ukratko, kako navodi Microsoft [8] to su M*alware* napadi, Napadi (SQL) injekcijom, *Phishing* napadi, Botnet napadi, XSS napadi (eng. *Cross-site scripting attacks*), DoS i DDoS napadi (eng. *(Distributed) Denial of Service Attacks*).

6.1.1. *Malware* napadi

Ovo je jako široka vrsta napada u smislu da se može dogoditi na bilo kakvom uređaju ili operacijskom sustavu. Česti su zbog toga što napadač razvija i instalira neželjeni softver koji mu omogućava dobivanje nezamijećenog pristupa ciljanom sustavu. Glavni cilj ovakvih napada je pristup žrtvinim osobnim informacijama, vjerodajnicama ili drugim povjerljivim informacijama, kreiranje štete na sustavu, pristup sustavu te na kraju financijsku dobit [7].

Iz ovoga je jasno da su ovakvi napadi usmjereni i na pojedince, a ne samo na organizacije i velika okruženja. Uz napomenu da se ne radi uvijek o specifičnim pojedincima nego meta može postati bilo tko, razumljivo je da je broj ovakvih kibernetičkih napada velik i u stalnom je porastu.

U ovoj vrsti napada koristi se i Redline maliciozni softver koji će kasnije u radu biti detaljnije analiziran. Međutim, drugi primjer je i Qbot malware, kako navodi CheckPoint [9], najčešće zabilježeni malware u lipnju 2023. godine. Ovaj je malware također obogaćen funkcionalnostima krađe osobnih podataka s uređaja, a najčešća mu je svrha dostavljanje i učitavanje drugog malicioznog softvera na uređaje. U istom izvještaju [9] stoji da su najčešće iskorištene ranjivosti unutar web poslužitelja, web aplikacija, ranjivosti u softveru koje

omogućavaju udaljeno izvršavanje naredbi itd. Sve to moguće je izbjeći ili smanjiti vjerojatnost događanja takvog incidenta kroz implementaciju sustava za detekciju anomalija, redovito ažuriranje softvera, primjenu sigurnosnih zakrpa te provođenjem provjera i konfiguracije pravila vatrozida što je moguće i automatizirati korištenjem naprednijih alata za upravljanje sigurnošću koji primjenom umjetne inteligencije dinamički prema različitim indikatorima određuju je li promet maliciozan ili ne te ovisno o konfiguraciji obavještavaju o takvom mrežnom prometu ili ga sprječavaju što uvelike pomaže sigurnosnim stručnjacima.

6.1.2. Napadi SQL Injekcijom

SQL injekcijski napadi iskorištavaju ranjivosti u bazi podataka koristeći SQL upite za dobivanje neovlaštenog pristupa. Napadači mogu dobiti pristup, mijenjati ili brisati povjerljive podatke, što može uzrokovati značajne promjene u aplikacijama. Također mogu stvoriti stražnje ulaze za buduće napade. Vrste SQL injekcijskih napada uključuju: izmjenu SQL upita za pristup skrivenim rezultatima, omogućavanje izmjene logike aplikacije, ali svakako ekstrakciju podataka iz različitih tablica. Glavni ciljevi ovakvih napada su zaobići autentikaciju, dohvatiti, izmijeniti ili obrisati podatke te na posljetku dobiti administrativni pristup sustavu.

Neki od nedavnih napada SQL injekcijom koji iskorištavaju ranjivosti pronađene u 2024. godini navedeni su na web stranici *bleepingcomputers* [10], a u nastavku su opisana 3 napada:

- **F5 BIG-IP Ranjivosti:** Otkrivene su dvije visoko rizične ranjivosti u BIG-IP Next Central Manageru koje omogućuju preuzimanje administratorske kontrole i stvaranje lažnih računa na upravljanim resursima. Time napadači sebi mogu kreirati perzistentan pristup sustavu, a ključna ranjivost je nastala u API sučelju preko kojega je omogućeno udaljeno izvršavanje naredbi na uređajima koji nemaju primijenjenu sigurnosnu zakrpu za ove ranjivosti.
- **WP Automatic Plugin:** Kritična ranjivost u ovom dodatku za WordPress iskorištava se za stvaranje korisničkih računa s administrativnim privilegijama i postavljanje *backdoor*-a za dugoročni pristup. Postupak autentikacije unutar ovog dodatka može se zaobići SQL injekcijom kojom se kreira novi korisnik s administratorskim privilegijama što otvara mogućnost kreiranja i ubacivanja zlonamjernih procesa ili drugih korisničkih računa za ostvarivanje perzistentnog pristupa okruženju.
- **LayerSlider Plugin:** Premium dodatak za WordPress podložan je neovlaštenoj SQL injekciji kojom se bez autentikacije mogu dohvatiti osjetljivi podaci kao što su sažetci lozinki. Ova je ranjivost nastala zbog pogreške u logici izvršavanja programa, odnosno u rukovanju parametrima što je vrlo često u programiranju te je zbog toga potrebno provoditi vrlo detaljne i kvalitetne analize kvalitete programskog koda. Ova ranjivost

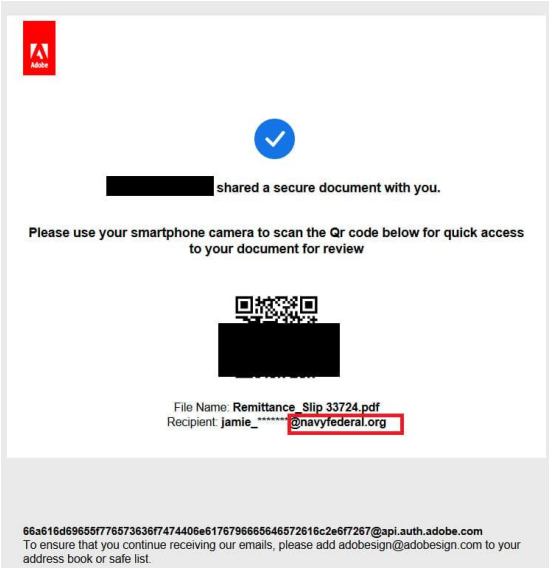
naravno, kao i sve ostale, zahtijeva od administratora sustava da brzo primijene sigurnosna ažuriranja.

6.1.3. Phishing napadi

Napadači oponašaju legitimne izvore i kloniraju web stranice kako bi prevarili žrtve da, vjerujući da je izvor legitiman, pokreću maliciozne datoteke ili otvaraju maliciozne poveznice što dovodi do kompromitacije infrastrukture. Cilj phishing napada je krađa povjerljivih i osobnih informacija, poput prijava i financijskih podataka. Ovo su najčešći napadi danas jer ciljaju na ljudski čimbenik koji je zbog naprednih tehničkih mjera zaštite postao jedan od najranjivijih čimbenika u procesu kibernetičkih napada [7].

Neki od nedavnih većih phishing napada koji su zabilježeni opisani su na web stranici *bleepingcomputers* [11], a u nastavku su opisana 3 napada:

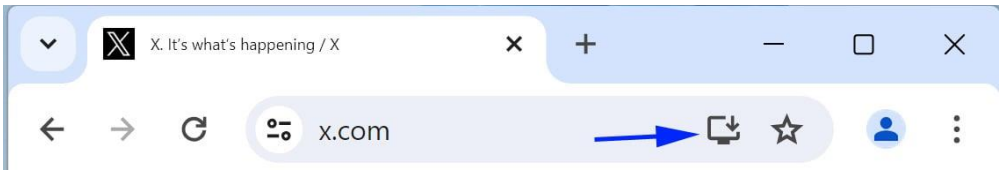
- **Phishing-as-a-Service (PhaaS) ONNX Store:** Cilja Microsoft 365 račune zaposlenika financijskih firmi koristeći QR kodove u PDF privitcima. Mailovi su napravljeni da izgledaju kao da ih je poslao netko iz odjela ljudskih resursa pod krinkom pokrenutog procesa povećanja plaće za ciljanog zaposlenika kako bi korisnici otvorili dokument iz privitka i skenirali QR kod koji ih nadalje vodi na malicioznu stranicu koja izgleda kao legitimna stranica za prijavu u Microsoft servise. Nakon što korisnik unese podatke i klikne gumb za „prijavu“, podaci se šalju napadaču čime je uspješno izvršen napad, a izgled PDF dokumenta također je prikazan u izvještaju [12]:



Slika 2 - PDF Dokument s malicioznim QR kodom [12]

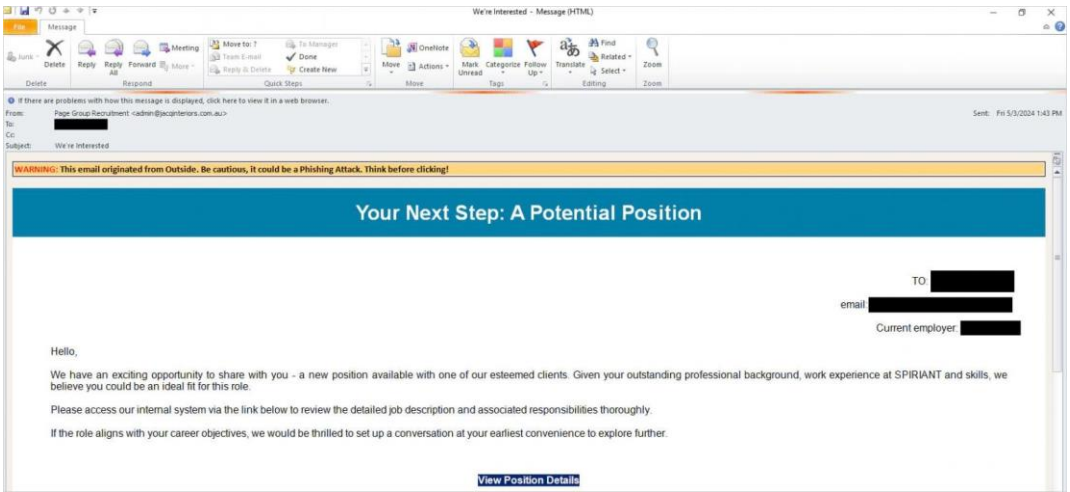
- **Phishing alat za progresivne web aplikacije (PWAs):** Omogućava stvaranje uvjerljivih korporativnih prijavnih obrazaca za krađu vjerodajnica. Kao i ONNX

platforma za kreiranje i provedbu phishing kampanja, ovaj phishing alat pruža uvjerljive obrasce koji izgledaju potpuno identično kao legitimni prijavni obrasci. Novost i najveća opasnost kod ovog napada je to što je moguće kreirati maliciozne stranice koje izgledaju kao legitimne, a adresa u adresnoj traci također može prikazivati bilo koji tekst, pa tako i adresu legitimne stranice. U primjeru je dan prikaz otvorene stranice koja izgleda kao stranica društvene mreže X prema adresi u adresnoj traci, ali traži pristup za instaliranje softvera koji je zapravo maliciozan [13]:



Slika 3 - Maliciozna stranica s "legitimnom adresom" [13]

- **Warmcookie malware:** Distribuira se putem lažnih phishing kampanja s ponudama za posao kako bi se omogućio neautoriziran pristup u korporativne mreže. Ovo je također klasični pristup phishing kampanjama koje unutar mail poruke uključuju poveznicu na malicioznu web stranicu, međutim posebno je korištenje Warmcookie softvera koji se instalira na računalo i omogućava perzistentnost kreirajući vremenski zakazan zadatak koji se pokreće svakih 10 minuta, a sam softver omogućava pristup sustavu i funkcionalnosti poput dohvaćanja podataka o IP adresi, dostupnim resursima zaraženog uređaja, snimanje zaslona, podatke o instaliranim programima ili izvršavanje naredbi u naredbenom retku. Primjer mail poruke dan je i u izvještaju [14] te izgleda ovako:



Slika 4 - Primjer phishing mail poruke [14]

6.1.4. Botnet napadi

U botnet napadima, napadač kompromitira više računala instaliranjem zlonamjernog softvera i preuzima kontrolu nad sustavima žrtava. Napadači, poznatiji pod engleskim terminom kao *botmasteri*, koriste kontrolu za generiranje zlonamjernih aktivnosti bez znanja žrtve. Glavni cilj botnet napada je ometanje redovitih poslovnih procesa, financijska dobit i dobivanje pristupa kao root korisnik. Faza iz MITRE ATT&CK okvira koja je ovdje najizraženija jest faza upravljanja i zapovijedanja [7].

Neki od nedavnih događanja vezanih za botnet mreže koja su zabilježena opisana su na web stranici *bleepingcomputers* [15], a u nastavku su opisana 3 od njih:

- **Pumpkin Eclipse: Botnet 'Pumpkin Eclipse'** izazvao je misteriozni destruktivni događaj 2023. godine, uslijed kojeg je 600.000 *SOHO* internet rutera isključeno kroz destruktivno djelovanje velikog broja uređaja uključenih u botnet, a samim time narušena je dostupnost rutera, a time i interneta velikom broju korisnika.
- **Operation Endgame:** Međunarodna policijska operacija 'Operation Endgame' zaplijenila je preko 100 servera širom svijeta koje su koristili zlonamjerni programi poput *IcedID, Pikabot, Trickbot, Bumblebee, Smokeloader i SystemBC.*
- **911 S5 Proxy Botnet:** Američko Ministarstvo pravde i međunarodni partneri uništili su botnet pod nazivom 911 S5 proxy te uhitili administratora tog botneta.

6.1.5. XSS napadi

U XSS napadima, napadač izvršava zlonamjerni kod u web pregledniku žrtve putem ugrađenog koda u web aplikaciju. To su klijentski napadi koji se aktiviraju kada žrtva pristupi zlonamjernoj aplikaciji. XSS napadi mogu biti [7]:

- Pohranjeni XSS: Zlonamjerni kod trajno pohranjen na ciljanom poslužitelju, npr. u bazi podataka.
- Reflektirani XSS: Zlonamjerna skripta isporučena žrtvi putem poruke o grešci, e-pošte ili posebno oblikovane poveznice.

Neki od nedavnih većih phishing napada koji su zabilježeni opisani su na web stranici *bleepingcomputers* [16], a u nastavku su opisana 3 napada:

- **GitLab XSS Ranjivost:** Neautenticirani napadači mogu preuzeti korisničke račune putem XSS napada. Ranjivost je bila prisutna u web verziji programskog okruženja alata VSCode.
- **WordPress Popup Builder:** Napadači kompromitiraju WordPress stranice iskorištavajući ranjivost u zastarjelim verzijama Popup Builder dodatka inficirajući preko 3300 web stranica zlonamjernim kodom koji se sprema u tablice unutar baza podataka. Taj kod je definiran kao kod koji se aktivira na određeni događaj (eng. *Event Handler*).

Time se osigurava pokretanje koda kada se događaju različite radnje poput otvaranja i zatvaranja prozora ovog dodatka.

- **Joomla CMS Ranjivosti:** Otkriveno je pet XSS ranjivosti koje bi mogle omogućiti udaljeno izvršavanje koda (eng. *Remote Code* Execution) na web stranicama s određenom verzijom Joomla upravitelja sadržajem.

6.1.6. DoS i DDoS napadi

U DoS i DDoS (eng. *(Distributed) Denial of Service*) napadima, napadač legitimnim korisnicima onemogućava pristup sustavima i aplikacijama generiranjem velikog broja lažnih zahtjeva. Cilj je usporiti ili prekinuti proces obrade stvarnih zahtjeva.

- DoS napadi: Napadi generirani iz jednog izvora.
- DDoS napadi: Napadi generirani iz brojnih izvora, često koristeći *botnete*.

Cilj ovakvih napada je također generiranje financijske dobiti ometajući usluge velikih poslovnih organizacija.

Jedan od najvećih zabilježenih DDoS napada ciljao je Google usluge te je dosegao promet od 2,54 Tbps. Napadači su slali maliciozne pakete prema 180 000 web poslužitelja koji su slali odgovore prema Google uslugama što je dovelo do velikog opterećenja cjelokupnog okruženja [17]. U ovome izvještaju tvrtke CloudFlare [17] također se spominju DDoS napadi velikih razmjera koji su ciljali platforme poput Amazon Web Servisa (AWS) i GitHub-a. Te su platforme često mete napada zbog svih informacija koje korisnici na njima mogu pohranjivati, ali i zbog popularnosti među korisnicima jer velik broj korisnika osigurava veliku površinu napada i veću potencijalnu korist nakon uspješno izvršenog napada.

7. Analiza kibernetičkih napada

Nakon teorijskog uvoda o modelima relevantnim za analizu faza kibernetičkih napada, u ovome će poglavlju po fazama napada prema MITRE ATT&CK okviru biti analizirani kibernetički napadi koji su se dogodili nedavno i ostavili ili još uvijek ostavljaju posljedice svoga djelovanja.

U nastavku će biti analizirano nekoliko različitih napada koji su koristili Redline zlonamjerni softver za krađu podataka sa sustava. Razlog tome je što se sami napadi razlikuju u svojim procesima unutar faza iako se u svakome od njih koristi isti softver. Time se nastoji prikazati evoluirajuća priroda kibernetičkih prijetnji i njihovih taktika i tehnika izvršenja napada kojima nastoje zaobići postavljene tehničke mjere zaštite i obrane ili pak ostvariti različite ciljeve u čemu im je zlonamjerni softver samo jedno od sredstava postizanja tih ciljeva. Nakon

toga će biti forenzički analiziran jedan od uzoraka Red-line zlonamjernog softvera u izoliranom i virtualiziranom rješenju da bi se dobio detaljniji uvid u općenito funkcioniranje ovoga softvera.

7.1. Redline i svrha u kibernetičkim napadima

U ovome će se poglavlju ukratko predstaviti Redline zlonamjerni softver te konkretno analizirati skoriji kibernetički napadi koji su ga u nekoj od svojih faza koristili.

Redline je dizajniran za krađu osjetljivih informacija na kompromitiranim sustavima, a uobičajeno se distribuira *phishing* e-mail porukama, taktikama socijalnog inženjeringa te kroz maliciozne URL poveznice. Vrlo je fleksibilan kada je u pitanju krađa vjerodajnica koja prouzrokuje financijske gubitke i curenje podataka. U 2020. je postojala kampanja koja je ovim zlonamjernim softverom ciljala na osobne uređaje kao i uređaje organizacija. Mnoge su industrije bile meta, ali najveći utjecaj se dogodio u zdravstvenom i građevinskom sektoru. Često se koristi u kombinaciji s drugim zlonamjernim softverima i jedan je od najčešćih softvera ove vrste [18].

Iz ovoga se da zaključiti da je velik broj napadača koji se žele okoristiti ovim softverom, a posljedično je broj žrtvi pogođenih napadima puno veći. Budući da su kibernetički napadi jako složeni i sastoje se od više faza kao što se moglo vidjeti u uvodnim poglavljima ovog rada, korištenje ovog zlonamjernog softvera u većim kibernetičkim napadima većinom se svodi na samo jednu, „glavnu“ fazu, a to je faza pod nazivom pristup vjerodajnicama (eng. *Credential Access*). Ta faza uključuje 43 tehnike, a služi, kao što i sam naziv kaže, za pristup vjerodajnicama koje mogu biti razne; od podataka za prijavu na sustave unutar mreže do podataka za prijavu na društvene mreže, kripto-novčanike i slične platforme. U manjim napadima se Redline može koristiti i zasebno, ali takvi napadi većinom služe samo za prikupljanje informacija o mogućim metama većih napada te za kreiranje boljeg i uspješnijeg većeg napada na ciljane mete.

Budući da je sada ukratko predstavljen Redline zlonamjerni softver, u idućem je poglavlju detaljnije analiziran cijeli proces napada uz navode konkretnih primjera iz stvarnog života.

7.2. Analiza procesa napada

Kibernetički napadi često su vrlo složeni, pogotovo ako se radi o visokim udjelima i vrijednim metama. Zbog toga će se ovo poglavlje baviti detaljnijom analizom procesa kibernetičkih napada u kojima je korišten Redline zlonamjerni softver kroz konkretne primjere napada na različite industrije uz usporedbu njihovih međusobnih razlika i sličnosti. Bitno je napomenuti da MITRE ATT&CK matrica podrazumijeva da se faze ne moraju izvoditi slijedno nego se redoslijed može razlikovati te se faze mogu koristiti više puta tijekom napada. Međutim, zbog bolje organiziranosti rada, faze će biti opisane slijedno kako su prikazane u matrici.

7.2.1. Izviđanje (eng. *Reconnaissance*) i Razvoj resursa (eng. *Initial access*)

Kroz početnu fazu izviđanja napadači pokušavaju otkriti što više dostupnih informacija o meti napada. MITRE [19] prepoznaje 10 različitih tehnika koje se koriste u ovoj fazi, a to su: prikupljanje informacija o: žrtvinim uređajima, osobnim podacima, mrežnom okruženju i organizaciji. Zatim se navode aktivno skeniranje, korištenje *phishing* tehnika, pretraživanje javno dostupnih baza podataka, web stranica te web stranica koje su u vlasništvu mete napada, kao i pretraživanje javno nedostupnih izvora.

Već se i iz samih naziva može zaključiti što se u svakoj od njih radi. Korištenjem različitih alata u kombinaciji s najčešće javno dostupnim informacijama poznatijim pod pojmom OSINT (eng. *Open Source Intelligence*) nastoji se prikupiti što više informacija o meti kako bi se što bolje pripremio i organizirao napad za sljedeće faze. Prilikom aktivnog skeniranja npr. nastoji se vidjeti opseg mete, koliko je IP adresa dostupno, u vlasništvu mete, što je sve pokrenuto, odnosno što stoji iza tih IP adresa, postoje li ranjivosti koje se mogu iskoristiti za početni pristup sustavu i dostavu malicioznog softvera za buduće faze itd.

U fazi izviđanja, napadači rijetko ostavljaju digitalne tragove koje forenzički istražitelji mogu koristiti jer se najčešće početno prikupljanje informacija radi iz vana, bez direktnog kontakta s okruženjem tvrtke, međutim u drugim fazama je itekako moguće pronaći digitalne tragove. No, konkretno u ovoj fazi najčešći su izvori informacija, tj. pokazatelja malicioznih aktivnosti informacije o aktivnostima na mrežnim uređajima (vatrozid, web-proxy) ili sustavima za detekciju ili prevenciju mrežnih upada (eng. *Intrusion Detection and Prevention Systems*). To je zapravo i očekivano jer se sva aktivnost prema okruženju, ako se radi o aktivnom skeniranju okruženja, a ne korištenju pasivnih metoda bez interakcije s okruženjem, bilježi na mrežnom perimetru. Međutim, potrebno je osigurati da svi uređaji korektno bilježe informacije o aktivnostima te da je moguće njihove logove pravovremeno dobiti na pregled. Naravno, svi

pronađeni artefakti trebaju se dokumentirati zajedno sa svojim sažetkom, vremenima pronalaska itd. Dokumentiranjem, ali i korištenjem sažetaka forenzički istražitelji mogu osigurati integritet podataka čime se svaka promjena u prikupljenim artefaktima može lako detektirati.

Sa svim prikupljenim informacijama kreće se u razvoj resursa u kojemu se, kako navodi MITRE u svojoj dokumentaciji [20], nastoji osigurati sve resurse potrebne za uspješan napad, a što uključuje kreiranje, kupovinu, krađu ili kompromitiranje resursa koji će biti korišteni. Takvi resursi podrazumijevaju infrastrukturu, korisničke račune ili druge tehničke mogućnosti, a podupirat će druge faze napada kao što je npr. kupovina domene koja će se koristiti u fazi zapovijedanja i upravljanja, email računi za *phishing* napade unutar faze inicijalnog pristupa ili krađa certifikata za potpisivanje kako bi se mogao potpisati zlonamjerni programski kod za potrebe faze izbjegavanja obrane.

Napadači u ovim fazama biraju optimalne tehnike za svoje operacije. Što se tiče Redline zlonamjernog softvera, tehnika povezana s njim je osiguravanje mogućnosti: *malware* (eng. *Obtain Capabilities: Malware*) što je i očekivano jer je to faza u kojoj napadač koristi zlonamjerni softver kako bi mogao podržati svoje operacije tijekom napada.

Jedan od primjera je LAPSUS$ kibernetička kriminalna grupa koja je aktivna najranije od sredine 2021. godine i oni su konkretnije povezani s korištenjem Redline softvera u svojim napadima za krađu lozinki s kompromitiranih sustava kako piše MITRE [21], a otkriveni su upravo zahvaljujući detaljnim vođenjem evidencije o artefaktima napada koji su uspoređeni s već postojećim. U tome je napadu bio prepoznat uzorak ponašanja, korištenih tehnika i taktika te alata koji su upućivali na operacije ove grupe. To je primjer kako MITRE ima bazu podataka prepoznatih operacija i grupa te ih je lako pronaći prema korištenom softveru, taktikama i tehnikama i drugim specifičnostima.

7.2.2. Inicijalni pristup (eng. *Initial Access*) i Izvršenje (eng. *Execution*) i Perzistentnost (eng. *Persistence*)

Nakon prikupljenih informacija i osiguranih resursa, kreće se u izvršavanje konkretnog napada, točnije u osiguravanje inicijalnog pristupa. Deset je tehnika koje se tu svrstavaju, ali najčešće korištene u napadima u kojima je zabilježeno korištenje Redline zlonamjernog softvera su *Phishing* te Kompromitiranje pri prolasku (eng. *Drive-by Compromise*).

Phishing je prema definiciji s MITRE dokumentacije [22] slanje poruka preko različitih komunikacijskih kanala, najčešće putem maila u svrhu dobivanja pristupa sustavu. U tim se *phishing* porukama nalaze najčešće maliciozne poveznice ili prilozi koji imaju svrhu zavarati korisnika da su legitimni kako bi ih korisnik otvorio i time pokrenuo maliciozni kod.

Kompromitiranje pri prolasku je, također prema MITRE dokumentaciji [23], definirano kao dobivanje pristupa sustavu tako da korisnik koji posjećuje web stranicu u normalnim okolnostima preuzima sadržaj, a često su to web stranice koje posjećuje određena grupa ljudi, a moguće je i korištenje malicioznih reklama koje se reklamiraju putem legitimnih kanala.

U fazi izvršenja najčešće je korištena tehnika zakazanih zadataka (eng. *Scheduled Task/Job*). U njoj napadači mogu zloupotrijebiti funkcionalnost vremenskog zakazivanja zadataka da bi dobili inicijalno ili ponavljajuće izvršenje malicioznog koda [24]. Istom se tehnikom najčešće osigurava i perzistentnost jer zadatak vremenski pokreće zlonamjerni softver tako da osigurava perzistentan pristup sustavu.

U ovim fazama istražitelji nad logovima prikupljenim s nadziranih uređaja koriste i razne forenzičke alate kako bi proveli adekvatnu analizu, identificirali ključne artefakte kao indikatore kompromitacije te ih dokumentirali i očuvali njihov integritet za dalji proces forenzičke analize. Koriste se razni alati, a jedan od popularnijih za analizu mailova je *PhishTool*. Njime se sumnjivi mail može automatski analizirati i dobiti detaljne informacije o indikatorima malicioznosti čime se ubrzava proces istrage. U fazama izvršenja i perzistentnosti koriste se razni forenzički alati poput EnCase-a i FTK-a. Ovi alati omogućavaju dubinsku analizu svih artefakata spremljenih na digitalnim uređajima koji mogu pomoći u otkrivanju tragova napadača. Provodeći analizu na snimkama cjelokupnog stanja uređaja u vremenu detektiranog napada, moguće je vidjeti procese povezane s internetskim preglednikom, uspostavljene veze prema web stranicama, povijest preuzimanja datoteka s Interneta itd. Također je moguće preuzete datoteke rekonstruirati i prebaciti na izolirano okruženje u kojemu će se datoteka na siguran način izvršiti i analizirati. Sve to daje uvid u porijeklo datoteke i potencijalnog napada, načina na koji je napadač ostvario pristup sustavu i što je inicijalno radio. Osim toga, analizirajući procese koji su se odvijali u dano vrijeme, moguće je utvrditi (ne)postojanje malicioznih procesa koji služe očuvanju perzistentnosti. Često je to proces koji nosi sličan naziv kao i neki od uobičajenih sustavskih procesa kao što je npr. *svchost.*exe. Razne su metode kojima se napadači služe, ali najčešće je to neka vrsta zamjene slova pa je naziv procesa zapravo *svch0st.exe*.

Zato je važno dobro poznavati arhitekturu sustava jer se u ovome slučaju maliciozni proces *svch0st.exe* može otkriti i prema roditeljskom procesu. Naime, roditeljski proces legitimnog *svchost.exe* processa je uvijek *services.exe.* Osim toga, legitimnost procesa može se utvrditi i provjerom putanje. Naime, legitimni se proces *svchost.exe* uvijek pokreće iz *C:\Windows\System32* ili *C:\Windows\SysWOW64* putanje te ako je ta putanja drukčija za neki proces koji se pokušava sakriti kao *svchost.exe*, on je definitivno maliciozan i treba ga detaljnije istražiti. [25]

U primjeru nedavnih napada (Travanj, 2024.) na industriju videoigara čija su meta sami igrači, prema izvještaju kojeg je objavio McAfee Labs [26], napadači su zloupotrijebili platformu GitHub kako bi zlonamjerni softver bio poslužen putem službenog Microsoft računa u *vcpkg*

repozitoriju kao zapakirana arhiva. Unutar arhive je *MSI* Instalacijska datoteka s dvije izvršne datoteke te jednom tekstualnom datotekom. U tekstualnoj je datoteci postavljena *lua* datoteka, odnosno *bajtkod* (eng. *Bytecode*), a druge dvije izvršne datoteke koje su inače legitimne, su izmijenjene kako bi uključivale i kod iz „tekstualne“ datoteke.

Dakle, koristeći legitimne platforme s ciljanom grupom igrača videoigara, napadači su postavljali maliciozne datoteke koje su korisnici pokretali na svojim računalima što odgovara ranije opisanoj definiciji ove tehnike. Sam softver koji se u ovome slučaju oglašavao jest softver za varanje u igrama odnosno za njihovu modifikaciju čime se igra ne bi ponašala kao što je zamišljeno, ali u pozadini je Redline zlonamjerni softver koji ima za cilj ukrasti sve vjerodajnice, a posebno se cilja na vjerodajnice za pristup računima na platformama za kupovinu videoigara koje često imaju spremljene podatke o karticama ili velika salda. U tome je, kako se i u izvještaju [26] navodi, zapravo najveća novost u ovome napadu jer se do sada Redline najčešće dostavljao na sustave putem maila ili drugih zlonamjernih softvera koji bi najprije iskoristili postojeće ranjivosti te onda pokrenuli Redline i aktivirali ga. Ovo također prikazuje inovativnost u modificiranju svojih taktika i tehnika koju napadači pokazuju i iskorištavaju za svoje maliciozne ciljeve. Osim toga, izvršna datoteka je nakon pokretanja malicioznog koda u *lua* jeziku koji je zapisan u tekstualnoj datoteci postavljala vremenski zakazan zadatak koji pokreće Redline zlonamjerni softver te osim izvršenja osigurava i perzistentnost što se odnosi na sljedeću fazu napada.

U izvještaju kojeg je objavila tvrtka Trend Micro [27], napadači su koristili certifikate produljene validacije za potpisivanje programskog koda. Nije razjašnjeno kako je napadač dobio pristup privatnom ključu, no ovo je jedan od primjera korištenja takve tehnike za inicijalni pristup sustavu. U analiziranim napadima, ove su datoteke dostavljene putem *phishing* mailova. A za inicijalni pristup korištene su *phishing* tehnike opisane kasnije u ovome poglavlju u kojemu je mail izgledao kao izvještaj o žalbi poznate tvrtke za putovanja [27].

Budući da je spomenuto i maliciozno korištenje oglašavanja, ovaj članak [28] pokazuje kako su napadači željeli iskoristiti popularni „val umjetne inteligencije“ na temelju kojega su kroz maliciozne oglase nudili besplatne verzije popularnih *chatbot*-ova kao što su ChatGPT i Google Bard. Korisnici su zapravo preuzimali Redline koji je po pokretanju preuzimao sve korisničke podatke spremljene na uređaju u bilo kojem obliku što naravno ima ogromne potencijalne posljedice. Ovo je još jedan primjer kako napadi postaju sve sofisticiraniji i inovativniji te se naslanjaju više na ljudski čimbenik jer su tehničke mjere sigurnosti sve bolje i naprednije. Ovo su zapravo primjeri procesno kraćih i „jednostavnijih“ napada koji su nakon inicijalnog pristupa prešli u fazu eksfiltracije podataka odnosno pristupa vjerodajnicama i time završili svoj životni ciklus.

Phishing poruke obično su najčešći oblik distribucije zlonamjernog softvera, pa je primjera mnoštvo. No, budući da se napadači često oslanjaju na ljudski čimbenik i aktualna

događanja kako bi sakrili maliciozne elemente, jedan od primjera su i kampanje koje su se koristile u vrijeme *Covid*-19 virusa. Prema ovom članku objavljenom na ScienceDirect-u [29], zabilježen je porast od 400% kibernetičkih napada u vrijeme koronavirusa. Također, najčešće vrste zlonamjernog softvera bile su vrste koje služe za krađu informacija, a od njih je najčešći bio Redline koji se distribuirao putem *phishing* mailova.

7.2.3. Eskalacija privilegija (eng. *Privilege Escalation*), Izbjegavanje obrane (eng. *Defense Evasion*)

Proces kibernetičkog napada najčešće ide prema eskalaciji privilegija što predstavlja osiguravanje viših privilegija na sustavu, mreži ili općenito infrastrukturi koristeći trenutno raspoloživa prava. Većinom se od običnih korisničkih računa nastoji doći do administratorskih računa, pogotovo domenskih administratora. Tijekom cijelog napada koriste se razne tehnike za izbjegavanje obrane da bi napadač što dulje ostao neotkriven i neometan u izvršavanju svojih operacija.

Zbog prirode napada, u ovim slučajevima gdje se koristio Redline zlonamjerni softver, nije bilo previše primjera eskalacija privilegija, a i one koje su bile zabilježene nisu bile tehnički napredne jer su većinom koristile već spomenute vremenski postavljene zadatke ili postojeće korisničke račune čije su podatke za prijavu dobili drugim tehnikama ili samim Redline softverom nakon faze izvršenja. Zbog toga se ta faza neće detaljnije analizirati u ovome radu.

Međutim, svaki zlonamjerni softver kao takav nastoji zaobići postojeće mjere zaštite čemu govori u prilog i činjenica da MITRE na svojoj matrici prepoznaje čak 43 različite tehnike za ovu fazu napada, daleko više od broja tehnika za druge faze napada. Napadi u kojima se koristi softver za krađu podataka često uključuju različite alate za eksploataciju ranjivosti (eng. *Exploit kits*) koji sadrže razne tehnike izbjegavanja obrane i većinom su tehnike kombinirane jer same po sebi nisu dovoljne za napredniju zaštitu koja je potencijalno postavljena u okruženju. Jedan je primjer i korištenje RIG alata za iskorištavanje ranjivosti kojeg je tvrtka Bitdefender analizirala i to objavila u svom izvještaju [30], a taj alat iskorištava specifičnu ranjivost programa Internet Explorer pod oznakom CVE-2021-26411 kako bi dostavio maliciozni sadržaj među kojim je zamijećen i Redline. U tom se izvještaju također objašnjava kako je sam Redline uzorak u ovom primjeru kriptiran u više slojeva kako bi izbjegao detekciju. Naime, sam kod sadrži blokove koda koji se mogu smatrati smećem jer sadrže nekorištene nasumične varijable i parametre, a pored toga, prva razina kopira dio koda na drugu lokaciju gdje ga dekriptira koristeći hardkodirani ključ za enkripciju nakon čega pokreće prvi dio koda. To bi bila prva razina, a na sljedećoj razini, pokrenuti dio koda uključuje nekoliko funkcija i dekompresira dio glavnog dijela koda i prelazi na tu memorijsku lokaciju gdje se dekompresirani kod nalazi. Uz taj proces, u drugoj fazi je uključen i sloj XOR operacija s

generiranim pseudo-slučajnim bajtovima. U trećoj fazi se odvija dekompresija preostalog koda u izvršnu datoteku koja se učitava koristeći refleksiju i dolazi na početnu točku. U četvrtoj fazi se u prethodno kreiranoj izvršnoj datoteci učitava DLL koji sadrži maliciozni kod.

Osim izbjegavanja zaštite, zlonamjerni softver gotovo uvijek nastoji izbjeći i okoline za statičku analizu koda, pa se tako i ovdje koriste varijable okruženja te se u ovisnosti o vrijednosti tih varijabli zlonamjerni softver ne pokreće ili završava s radom ako je već bio pokrenut.

Nakon toga, u petoj se fazi dodatno raspakirava zapakirani kod te je sve spremno za šestu fazu u kojoj je učitana datoteka zapravo Redline sa svojim funkcionalnostima, zamaskiran kao *.Net* izvršna datoteka. Međutim i sama izvršna datoteka ima metode koje su prazne i dekriptiraju se tijekom izvođenja (eng. *Runtime*). Prema izvještaju [30], taj uzorak statički, izvan statusa izvođenja izgleda ovako:

```
public static class Program {
 private static void Main(string[] args) {
 Program.Run();
 }
 public static void Run() {} // inicijalno prazna metoda
 static Program(){
 z2jc63fLkugS1X8Q9N.uWdOlFaAb(); // funkcija za dekripciju
 }
}
```

Kao što je već i spomenuto, sve metode su tijekom izvođenja dekriptirane pozivom funkcije za dekripciju, a taj je poziv u ovom slučaju predstavljen sljedećim nizom znakova: *z2jc63fLkugS1X8Q9N.uWdOlFaAb();*

Nakon dekripcije, tijelo metoda postaje vidljivo u alatima za statičku analizu koda i može se točnije vidjeti što sam zlonamjerni softver radi. Budući da je ovo poglavlje vezano za tehnike izbjegavanja obrane, više o samom funkcioniranju ovakvog softvera bit će objašnjeno u zasebnom poglavlju.

U drugim je primjerima za izbjegavanje obrane, kao što je već bilo navedeno u prethodnim poglavljima korišteno potpisivanje koda certifikatima kojima se vjeruje, maskiranje softvera kao legitimnog, korištenje standardnih aplikacijskih protokola za komunikaciju i ostalo.

7.2.4. Pristup vjerodajnicama (eng. *Credential Access*) i Otkrivanje (eng. *Discovery*) te Lateralno kretanje (eng. *Lateral Movement*)

Budući da se ovdje stavlja fokus na Redline, očekivano je da je ova faza u napadima koji su analizirani bila glavna ili među glavnima jer se upravo temelji na pristupu vjerodajnicama za koje je Redline i kreiran. Prema samoj MITRE matrici [20], navodi se 17 tehnika prepoznatih u ovoj fazi, međutim neke koje su najprimjećenije u napadima koji su korišteni za analizu u ovome radu imaju sljedeće nazive: Vjerodajnice iz skladišta lozinki (eng. *Credentials from Password Stores*) te Prikupljanje vjerodajnica iz operacijskog sustava (eng. *OS Credential Dumping*) te Nezaštićene vjerodajnice (eng. *Unsecured Credentials*).

Lozinke se obično spremaju na nekoliko mjesta u sustavu, ovisno o operacijskom sustavu ili aplikaciji koja ih sprema. Također postoje specifične aplikacije i servisi koji spremaju lozinke kako bi korisnicima bilo lakše upravljati i održavati lozinke, a zovu se upravitelji lozinkama (eng. *Password managers*) i sefovi u oblaku (eng. *Cloud secrets vaults*). Jednom kada se dođe do vjerodajnica, one mogu biti korištene kako bi se izvršavalo lateralno kretanje i pristup do osjetljivih informacija [31]. Ovakvi upravitelji lozinkama često su meta napadača kada su u pitanju velike organizacije jer njihovi zaposleni često prema politikama tvrtke trebaju koristiti specifične upravitelje lozinkama ili jednostavno imaju previše korisničkih računa koje moraju održavati što sebi olakšavaju korištenjem takvih alata.

Prema MITRE dokumentaciji za prikupljanje vjerodajnica iz operacijskog sustava [32], napadači dohvaćaju ove podatke kako bi dobili pristup korisničkim računima na nekom sustavu, najčešće u obliku sažetka (eng. *Hash*) ili čak u čitljivom obliku (eng. *Clear text*). Navodi se također da se vjerodajnice mogu dohvatiti iz *cache* memorije operacijskih sustava, memorije ili struktura, a kasnije se mogu koristiti za lateralno kretanje i pristup osjetljivim informacijama.

Čest oblik spremanja lozinki, ali nikako dobar je spremanje lozinki i vjerodajnica općenito u bilješkama, na radnoj površini računala ili bilo gdje unutar sustava u tekstualnim datotekama. Te su datoteke u čitljivom obliku i lako ih je zloupotrijebiti jednom kada napadač ima pristup sustavu. Ono što MITRE navodi u svojoj dokumentaciji [33] specifično za ovu tehniku jest to da ove vjerodajnice mogu biti (slučajno) nesigurno pohranjene na različite lokacije u sustavu kao što su datoteke u čitljivom obliku, repozitoriji operacijskog sustava ili specifičnih aplikacija kao što su vjerodajnice u registrima ili čak drugim specifičnim datotekama poput datoteka privatnih ključeva.

Redline koristi sve ove tehnike kako bi dobio što više vjerodajnica za što više različitih platformi. Neki se napadi tu završavaju i napadači iskorištavaju te vjerodajnice za pristup aplikacijama, krađu sredstava i sl. dok neki napadi idu dalje u lateralno kretanje s pomoću tih vjerodajnica i ostvaruju pristup drugim sustavima unutar infrastrukture.

Spomenuti alati za forenzičku analizu također imaju slične mogućnosti prikaza korisničkih vjerodajnica iz sustava. Samim time, jasno je da maliciozni softver koji ima razinu pristupa sustavu na takvoj razini, vrlo lako može doći do istih. Zato je važno koristiti kvalitetne upravitelje lozinkama, kako bi se osigurao dodatni sloj zaštite. Neki od znakova kompromitiranih vjerodajnica su neobične prijave s neočekivanih lokacija, povećan broj neuspjelih prijava ili postojanje nepoznatih korisnika, posebno s administratorskim privilegijama. O svim aktivnostima ovih faza se dokazi i pokazatelji mogu pronaći na već spomenutim lokacijama, tj. uređajima. Međutim u fazama otkrivanja i lateralnog kretanja, nešto veću važnost imaju mrežni uređaji jer se naravno, kretanje izvršava preko mreže s jednog uređaja na drugi nakon što se isto tako preko mreže otkrivaju uređaji koji su spojeni na tu mrežu. Zbog ovoga je potrebno aktivno prikupljati i nadzirati logove te implementirati sigurnosna rješenja kako bi se pravovremeno detektiralo i reagiralo na potencijalne incidente.

7.2.5. Prikupljanje (eng. *Collection*) te Zapovijedanje i upravljanje (eng. *Command and Control*) te Eksfiltracija (eng. *Exfiltration*)

U složenijim napadima ove su faze važne za određivanje samog utjecaja cijelog napada jer se kroz fazu prikupljanja nastoji doći do svih relevantnih informacija koje bi mogle pomoći u daljim operacijama i poboljšati vjerojatnost uspjeha samog napada, a onda se kroz održavanje komunikacije s kontrolnim poslužiteljem izvodi zapovijedanje i upravljanje u kojemu se putem kontrolnog poslužitelja šalju naredbe zaraženim sustavima koje oni izvršavaju. Putem takve komunikacije događa se i eksfiltracija podataka o kojoj će biti riječi u sljedećem poglavlju.

U analiziranim napadima najviše su bile zamijećene tehnike snimanja zaslona (eng. *Screen Capture*), podaci iz međuspremnika (eng. *Clipboard Data*) te automatizirano prikupljanje (eng. *Automated Collection*) na kojoj se sve i temelji jer se svi podaci prikupljaju automatizirano, bez potrebe ručnih manipulacija podacima nakon što se Redline pokrene.

Osim prikupljanja vjerodajnica koje su zasebna faza prema MITRE matrici, u ovu fazu spada prikupljanje drugih informacija koje se nalaze na sustavima. Kao što je u analizi Redline uzorka Bitdefender [30] napisao, postoje konkretne metode koje služe za snimanje snimki zaslona i slanje tih snimki prema poslužitelju, a u njihovom uzorku su te metode bile vidljive. Konkretno, u napadima usmjerenim prema igračima videoigara, a prema ovome izvještaju tvrtke McAfee [26], istražitelji su otkrili ponašanje u kojemu su snimke zaslona bile poslane na poslužitelj napadača. U drugim napadima, takvo ponašanje nije konkretno zabilježeno, ali je Redline kao takav u mogućnosti odraditi i te stvari kao što je pokazano u ovome slučaju.

Naravno, prikupljanje se može općenito vršiti automatizirano za što je definirana i posebna tehnika koja je već spomenuta, međutim može se vršiti i preko komunikacijskog

kanala što onda uključuje zapovijedanje i upravljanje zaraženim sustavima čime se točno određuje slijed radnji i odabir podataka za prijenos. Ponovno, u slučajevima napada na industriju videoigara, prema izvještaju McAfee-a [26] postoji detaljna komunikacija zaraženih sustava sa zapovjednim poslužiteljem u vlasništvu napadača u kojima se zaraženim sustavima šalju oznake zadataka koje bi trebale izvršiti, a oznake su naravno kriptirane.

U analizi jednog od uzoraka, Bitdefender [30] izvještava da Redline koristi *.Net SOAP API (eng. Simple Object Access Protocol Application Programming Interface*) preko TCP povezivanja za komunikaciju sa svojim zapovjednim poslužiteljem. Komunikacijski kanal je kriptiran, a zahtjev uključuje autorizaciju i ne provjerava validnost certifikata. Preko tog kanala šalju se zahtjevi u obliku postavki. Postoji cijelo sučelje postavki koje se sastoji od varijabli koje predstavljaju preklopnike, odnosno to su *boolean* varijable koje mogu imati vrijednost istina ili laž. Vrijednosti iz zahtjeva mapiraju se na te varijable te u ovisnosti o vrijednostima tih varijabli Redline zna što od podataka treba poslati prema poslužitelju, a što ne. Primjer te klase dan je i u samom izvještaju [30]:

```
public class ESettings {
 public bool ScanBrowsers { get; set; }
 public bool ScanFiles { get; set; }
 public bool ScanFTPs { get; set; }
 public bool ScanBrowserExtensions { get; set; }
 public bool GetScreenshot { get; set; }
 public bool ScanTelegram { get; set; }
 public bool ScanVPNs { get; set; }
 public bool ScanGames { get; set; }
 public bool ScanDiscord { get; set; }
 public List<string> Patterns { get; set; }
 public List<string> Profiles { get; set; }
 public List<string> Paths { get; set; }
 public List<EConfig> Config { get; set; }
[...]
}
```

Nakon primljenih i postavljenih vrijednosti ovih postavki, kreće se u eksfiltraciju podataka u kojoj se na temelju tih vrijednosti određene stvari šalju prema zapovjednom poslužitelju. Već je bilo riječi o načinu na koji ta eksfiltracija funkcionira u primjerima koji su analizirani, a tehnike koje su primijećene i mogu se mapirati na tehnike iz MITRE matrice [20] su: automatska eksfiltracija (eng. *Automated Exfiltration*) te eksfiltracija preko komunikacijskog kanala (eng. Exfiltration over *C2 (Command and Control) Channel*).

Ovakvu je komunikaciju također moguće detektirati najčešće logovima s mrežnih uređaja jer se konkretno zapovijedanje i upravljanje, ali i eksfiltracija odvija najčešće preko vanjske mreže. Što se tiče same eksfiltracije to ne mora uvijek biti slučaj jer se podaci mogu eksfiltrirati i s uređaja na prijenosne diskove. No, u svakom slučaju se artefakti o takvim aktivnostima mogu prikupiti spomenutim forenzičkim alatima, a proaktivno detektirati i zaštiti sigurnosnim rješenjima. U slučaju eksfiltracije npr. korisno je imati implementiran i pravilno konfiguriran sustav za sprječavanje curenja podataka, odnosno DLP (eng. *Data Loss Prevention*) sustav koji bi svaki pokušaj prijenosa definiranih podataka detektirao i prema konfiguraciji dozvolio ili zabranio čime bi se uvelike smanjio broj ovakvih slučajeva te omeo cijeli proces napada. Eksfiltracijom podataka napadač želi doći do svojih ciljeva. Ometanjem te faze ometena je u većini slučajeva cijela operacija jer to otežava bilo kakav nastavak napada ili stvaranja koristi zbog manjka potrebnih informacija.

7.2.6. Utjecaj (eng. *Impact*)

Kao što i samo ime predlaže, ovdje su svrstane tehnike kojima se postiže utjecaj napada, odnosno njegov glavni cilj. Prema definiciji [34], napadač pokušava manipulirati, ometati ili uništiti sustave i podatke. Ovdje su uključene tehnike koje napadači koriste kako bi ometali dostupnost ili kompromitirali integritet manipulirajući poslovnim i izvršnim procesima. Tehnike korištene u ovoj fazi mogu uključivati uništenje ili izmjenu podataka. U nekim slučajevima, poslovni procesi mogu izgledati u redu, ali su zapravo izmijenjeni da bi doprinosili napadačevim ciljevima. Također se navodi da se ove tehnike mogu koristiti da bi se ispunio krajnji cilj ili da se osigura prikrivenost za povredu povjerljivosti podataka.

U analiziranim napadima cilj je većinom bio ilegalno prikupljanje vjerodajnica putem kojih bi se došlo do financijskih dobara te se nije išlo na štetu samom sustavu u smislu ometanja dostupnosti sustava nego se što se tiče utjecaja većinom radilo o povredi integriteta podataka koji je narušen samim pristupom vjerodajnicama, pa i kasnije njihovom zlouporabom.

7.3. Zaključno o provedenoj analizi kibernetičkih napada

Kroz ovo se poglavlje koristeći MITRE ATT&CK okvir [20] i faze napada te tehnike za svaku od njih analiziralo nekoliko nedavnih kibernetičkih napada koji su zabilježeni. Budući da su kibernetički napadi širok pojam i uključuju isto tako širok spektar različitih tehnika i metoda koje bi bilo teško objediniti u kraćem formatu, osnovu o kojoj je ovisio odabir napada za analizu činio je Redline zlonamjerni softver jer je to jedan od najčešće korištenih softvera te vrste (koji prikuplja vjerodajnice sa sustava za različite platforme), a najviše zbog svoje fleksibilnosti i

sveobuhvatnosti. Prolazeći kroz te faze, objašnjene su tehnike koje su najčešće zamijećene u slučaju tog skupa napada s referencama na opće stanje u području kibernetičke sigurnosti kako bi se svaki napad mogao analizirati na dovoljno detaljnoj razini te kako bi se prikazao cijeli proces kibernetičkog napada kao i sve stavke koje on kao takav podrazumijeva. Time je prikazana evoluirajuća priroda kibernetičkih napada koja se temelji na inovativnosti napadača i njihovih taktika i tehnika.

Ukratko je proces napada sljedeći: na neki način se zlonamjerni softver dostavi na ciljani sustav, a kao što je već bilo spomenuto, najčešće su to *phishing* e-mail poruke. Sam dokument najčešće je skriven i zapakiran kako bi zavarao žrtvu da klikne i pokrene datoteku misleći da je legitimna. Pokretanjem se izvršava podmetnuti softver koji uspostavlja komunikaciju sa svojim zapovjednim centrom (eng. *Control Center*) nakon čega mu šalje definirane podatke s kompromitiranog sustava te istim komunikacijskim kanalom prima naredbe od centra za izvršenje drugih radnji. Sustavi ostaju zaraženi dok netko ne detektira kompromitaciju i poduzme odgovarajuće radnje kao odgovor na incident ili se zlonamjerni softver samouništi nakon izvršenih zadataka.

8. Analiza Redline uzorka

Kroz ovo će poglavlje biti analiziran uzorak već više puta spomenutoga zlonamjernog softvera Redline zbog njegovog utjecaja i velike prisutnosti u kibernetičkim napadima u korelaciji s važnosti zaštite osobnih podataka. Kao softver koji krade podatke, bio je ključan u većini kibernetičkih napada u kojima se koristio za osiguravanje velikog utjecaja samih napada.

Svrha ove analize je, na određenoj razini apstrakcije, prikazati konkretne funkcionalnosti i način rada softvera ovakve vrste.

8.1. Statička analiza

Tehnika statičke analize odnosi se na analiziranje izvršne datoteke bez da je ona zapravo pokrenuta [35]. U ovome će se poglavlju izvršiti statička analiza prikupljenog uzorka.

Prvenstveno je važno utvrditi vrstu datoteke koju imamo. U Linux okruženjima to se lako doznaje naredbom *file*.

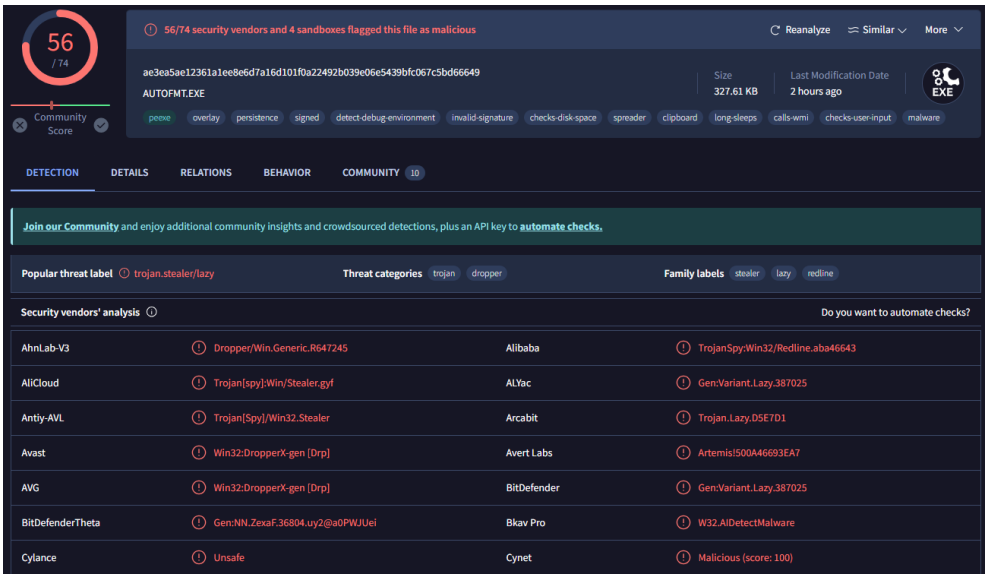
```
┌──(kali㉿kali)-[~/Desktop/Redline]
└─$ file redline.exe
redline.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

Prema rezultatu naredbe, ovo je izvršna datoteka s grafičkim sučeljem za Windows operacijski sustav.

Sljedeći je korak provjera sažetka na nekom od dostupnih javnih servisa. Sažetak datoteke unutar Linux okruženja također je lako dobiti putem naredbene ljuske, a rezultat je prikazan ispod.

```
┌──(kali㉿kali)-[~/Desktop/Redline]
└─$ sha256sum redline.exe
ae3ea5ae12361a1ee8e6d7a16d101f0a22492b039e06e5439bfc067c5bd66649
redline.exe
```

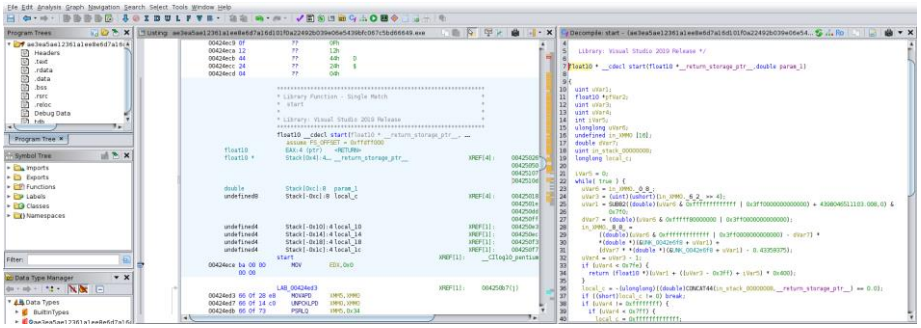
Ovaj je sažetak vezan za ovu datoteku i bilo kakva promjena sadržaja datoteke rezultirala bi potpuno različitim sažetkom. Zbog toga ovaj sažetak možemo postaviti u servis kao što je *VirusTotal* koji će na temelju tog sažetka reći je li ta datoteka maliciozna na osnovu prethodno skeniranih i učitanih datoteka i podataka u internu bazu. Rezultat se vidi na idućoj snimci zaslona s dijelom izvještaja sa spomenutog servisa.



Slika 5 - Izvještaj za sažetak na VirusTotal [www.virustotal.com]

Kao što je i očekivano, datoteka je označena kao maliciozna, a osim toga se na izvještaju može vidjeti i konkretna vrsta zlonamjernog softvera koja je detektirana.

Nadalje se može ići u analizu koda učitavanjem izvršne datoteke u neki od alata za dekompilaciju. Time se dobije kod u asemblerskom ili C-jezičnom formatu kojega je lakše čitati i razumjeti. Za potrebe ovoga rada, datoteka je učitana u besplatnu verziju *Ghidra* alata. Jednom kada je datoteka učitana, alat ju analizira, dekompilira i prikazuje razne pojedinosti o samoj datoteci.



Slika 6 - *Ghidra* sučelje s učitanom datotekom [Autorski rad]

Na prethodnoj se slici vidi da je alat uspio dekompilirati datoteku te je s desne strane prikazan kod u C programskom jeziku. Međutim, varijable i slične stvari su očekivano dobile generičke nazive pa je teže pronaći čemu koja od njih služi. Međutim, ovako je moguće vidjeti tok programa kroz programske konstrukte. Postoji puno čitanja vrijednosti s memorijskih lokacija što je očekivano za većinu programa, međutim u ovako dekompiliranoj verziji su te memorijske lokacije u prilično neiskoristivom formatu jer bez pokretanja ili detaljnog praćenja svake od njih nije moguće reći čemu svaka od njih točno služi.

Ovo je osnovni princip statičke analize koda i pristup istoj. U narednim bi se iteracijama nastojalo dešifrirati podatke dodatno kako bi se dobili čitljiviji podaci te bi se pratio sam tok programa kako je to napravljeno i u izvještaju Bitdefender-a [30]. U sljedećem će poglavlju biti više o samom ponašanju uzorka jer ovakav kod ne odaje previše važnih informacija.

8.2. Dinamička analiza

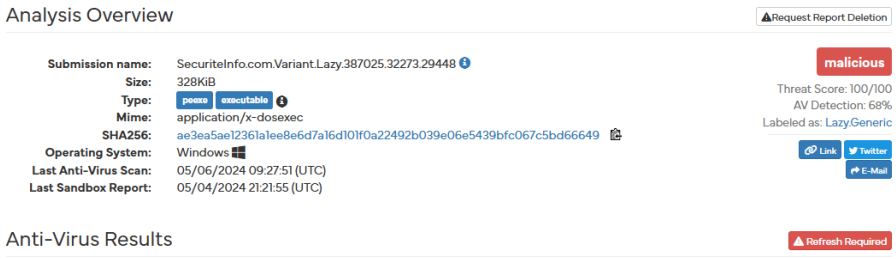
U Dinamičkoj analizi sumnjive datoteke se izvršavaju i nadziru u kontroliranom okruženju koje je najčešće virtualni stroj, emulator ili simulator. Kod ove je tehnike zanimljivo da okruženje treba biti „nevidljivo“ odnosno ne smije odavati da je virtualno jer su ozbiljniji zlonamjerni softveri napravljeni tako da imaju mogućnosti detekcije takvih okruženja prema kojima se prilagođavaju na način da ne izvršavaju nikakve maliciozne aktivnosti, ako detektiraju da su pokrenuti unutar njega. Ovime se dobiva uvid u ponašanje same datoteke koja se testira, ali treba napomenuti da je to vremenski zahtijevan pothvat, ali zahtijeva i puno ostalih resursa [35].

Iako postoje razni pristupi dinamičkoj analizi, u ovome su radu korišteni vanjski servisi u oblaku za analizu koja uključuje izvršavanje datoteke te za dobivanje izvještaja i datoteka poput snimke mrežnog prometa koja će biti analizirana ručno te će biti prikazani najvažniji dijelovi komunikacije zaraženog računala prema svom serveru.

8.2.1. Hybrid Analysis platforma

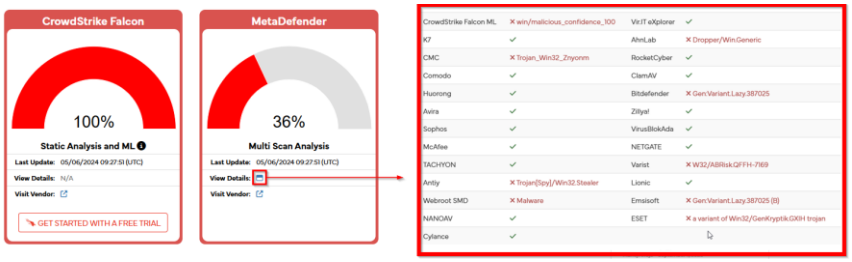
Ova platforma više služi za generičku analizu, tj. dobivanje općenitih informacija o analiziranom uzorku. Zbog toga će u nastavku biti prikazana i analiza na drugoj platformi koja daje više detalja o procesima i drugim indikatorima kompromitiranosti.

Početna stranica nakon izvršene analize uzorka prikazuje sve važne detalje koji su zabilježeni prilikom izvršavanja postavljene datoteke. Prvo su prikazane općenite informacije što je predstavljeno sljedećom slikom.



Slika 7 - Početna sekcija izvještaja Hybrid Analysis [www.hybrid-analysis.com]

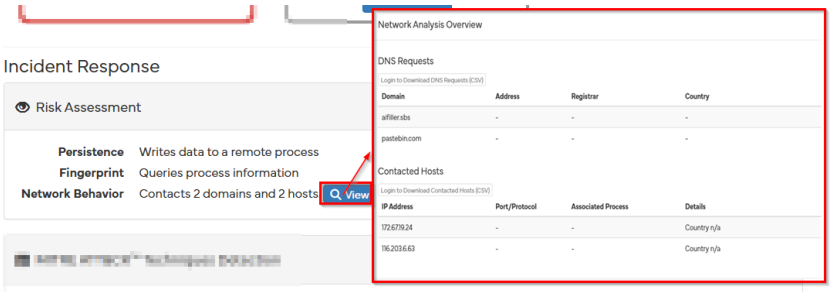
Dakle, na prethodnoj je slici prikazan pregled izvršene analize. Vide se podaci o veličini i vrsti datoteke kao i platforma odnosno operacijski sustav za kojeg je ona kreirana, a to je Windows. Također se vidi da je datoteka odmah označena kao maliciozna. Sljedeće su dvije sekcije izvještaja zapravo sumirani izvještaji antivirusnih alata i *sandbox* okruženja iz kojih se može pročitati koji su antivirusni alati označili datoteku kao malicioznu te postotak detekcije u tim slučajevima, kao i postotak vjerojatnosti da je datoteka maliciozna kombiniranjem analize strojnog učenja i statičke analize.



Slika 8 - Izvještaj analize različitih AV alata [www.hybrid-analysis.com]

Dakle, na prethodnoj slici vidi se da je statičkom analizom i primjenom metoda strojnog učenja vjerojatnost da je datoteka maliciozna zapravo 100 %. Klikom na detalje otvara se prozor u kojemu je kao na slici prikazano koji od antivirusnih alata prepoznaju tu datoteku kao malicioznu s drugim detaljima.

Nadalje su prikazani detalji o komunikaciji te mapiranje na MITRE metode i tehnike. Mapirano je 73 indikatora na različite metode i tehnike, međutim broj je velik jer datoteka sadrži različite mogućnosti od kojih većina može biti iskorištena u mapiranim metodama i tehnikama, ali nije sigurno da se u konkretnom slučaju svaka funkcionalnost tako i koristi. Zbog toga su ti podaci više informativnog karaktera. U drugom dijelu su podaci za procjenu rizika koji na ovoj platformi uključuju podatke o ponašanju na mreži (kontaktiranim domenama i računalima) te podatke o digitalnom otisku i perzistentnosti.

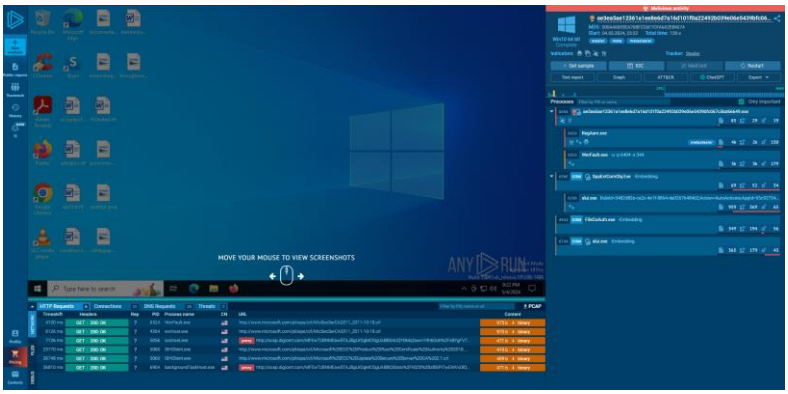


Slika 9 - Podaci za procjenu rizika [www.hybrid-analysis.com]

Kontaktirane su dvije domene koje bi mogle biti zanimljive, kao što se može vidjeti na prethodnoj slici, a to su pastebin[.]com te aifiller[.]sbs. Pastebin je popularan servis koji se koristi za bilješke i dijeljenje bilješki. Druga domena je nepoznata i u ovom slučaju bilo bi ju dobro analizirati, tj. pregledati promet koji ova datoteka kreira prema i s tom domenom. To će biti odrađeno u zasebnom poglavlju u kojemu će se koristiti Wireshark za analizu tog mrežnog prometa.

8.2.2. Any.Run platforma

Na ovoj je platformi puno više detalja o izvršenoj analizi, a uz to postoji i opcija preuzimanja datoteke snimljenog mrežnog prometa tijekom analize kojim se može dodatno kroz alate poput Wireshark-a analizirati konkretni paketi koji se šalju prema sumnjivom poslužitelju. Samo sučelje nakon izvršene analize prikazano je na sljedećoj slici.

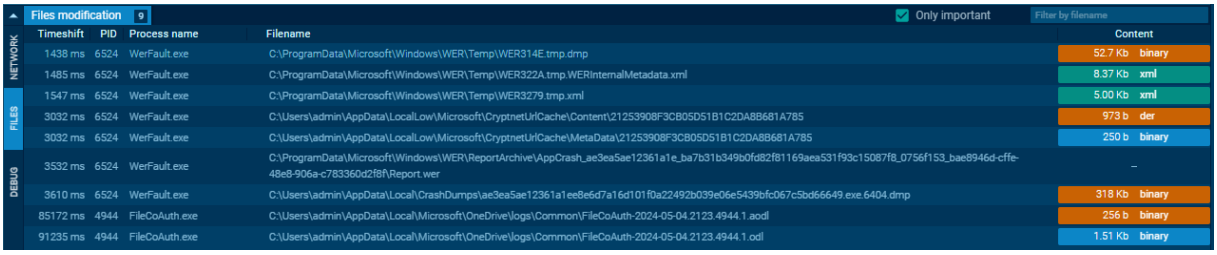


Slika 10 - Prikaz sučelja platforme Any.Run [app.any.run]

Velik dio zaslona zauzimaju snimke zaslona virtualnog stroja tijekom analize. Međutim, ovdje je samo jedna snimka zaslona koja je i prikazana na zaslonu jer se analiza izvršila automatski bez korisnika koji bi kliknuo pa pokrenuo datoteku i odabrao opciju za snimiti zaslon. Zbog toga se u ovome slučaju ne može vidjeti kako konkretno izgleda sučelje ove maliciozne datoteke, ali druge korisne stvari nalaze se ispod i s desne strane od maloprije spomenutog zaslona. Dakle, desno je postavljen grafički prikaz procesa u obliku hijerarhijskog stabla kako bi se lakše vidjeli pokrenuti procesi te njihov međusobni odnos. Klikom na bilo koji od procesa otvara se novi prozor ispod prikaza u kojemu se nalaze detalji o odabranom procesu. Crvenom trakom označeni su procesi koji imaju visoku ili najvišu vjerojatnost da su maliciozni. Jedan od tih je i proces pod nazivom *RegAsm.exe*. Ovo je inače legitimni proces unutar MS Windows okruženja, međutim, u ovom je slučaju zabilježena maliciozna uporaba. Zato se klikom na njega otvara prozor kako je prikazano na sljedećoj slici.

Slika 11 - Detalji procesa RegAsm.exe [app.any.run]

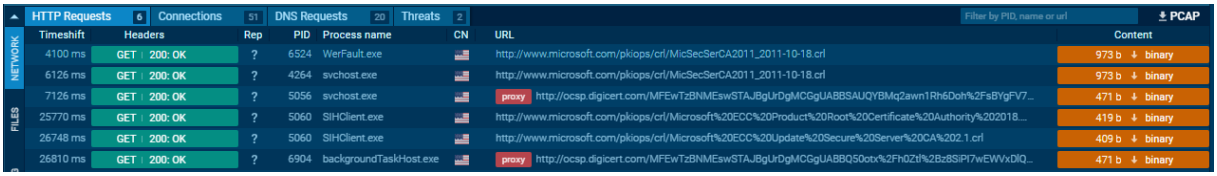
Prema podacima zabilježenim za ovaj proces u nastavku se može zaključiti da je to proces koji ima za svrhu analizirati okruženje na kojemu se nalazi te na temelju dobivenih informacija pokretati proces dalje. U popisu procesa također se vide i drugi legitimni Windows procesi kao što je *slui.exe* koji inače služi za aktivaciju Windows licenci. Ovaj popis trenutno nije dao konkretniji uvid u to što se točno događa na računalu u trenutku i vremenu nakon pokretanja ovoga uzorka maliciozne datoteke Redline softvera. Međutim, drugi dio zaslona koji sadrži podatke o mreži daje neke korisnije informacije. Osim mrežnog dijela, postoje i podaci o datotekama koji će također biti analizirani. Zabilježeno je 9 promjena nad datotekama, a popis tih 9 prikazan je na sljedećoj slici.



Slika 12 - Prikaz izmijenjenih datoteka [app.any.run]

Datoteke za koje su zabilježene izmjene izgledaju kao Windows datoteke te kao privremene datoteke. Međutim, napadači često koristeći takve metode nastoje zamaskirati svoje radnje jer se kreirajući legitimne datoteke stvara dojam uobičajenih aktivnosti dok se u pozadini odvija napad.

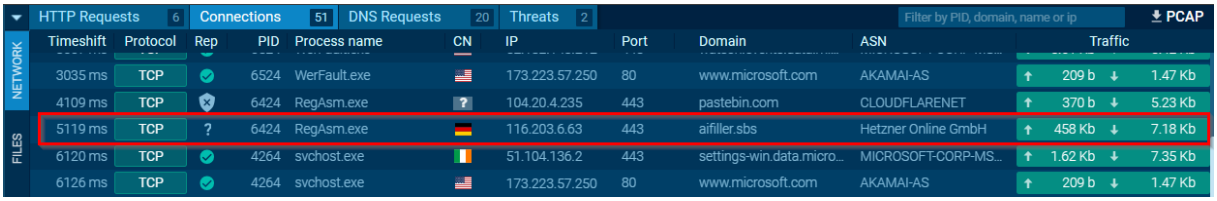
Za mrežnu aktivnost dostupni su podaci o HTTP zahtjevima, vezama, DNS zahtjevima te potencijalnim prijetnjama. HTTP Zahtjevi prikazani su na sljedećoj slici:



Slika 13 - Prikaz HTTP Zahtjeva [app.any.run]

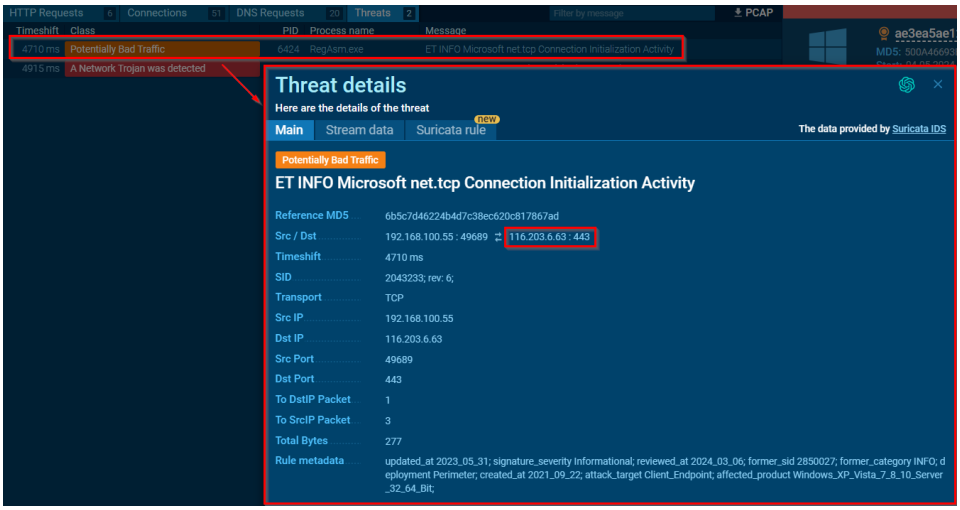
Vidljivo je da su se zahtjevi slali prema legitimnim stranicama, a među njima je i *digicert* što je očekivano jer se u prethodnom poglavlju moglo vidjeti da je zapravo ova datoteka potpisana neaktivnim, odnosno neispravnim *digicert* digitalnim certifikatom. Zbog toga se ta domena kontaktira prilikom pokretanja same datoteke.

Međutim, u odjeljku veza (eng. *Connections*) zabilježena je 51 uspostava veze, a na sljedećoj je slici prikaz manjeg broja tih veza među kojima je i od maloprije poznata domena koja bi mogla biti maliciozna:



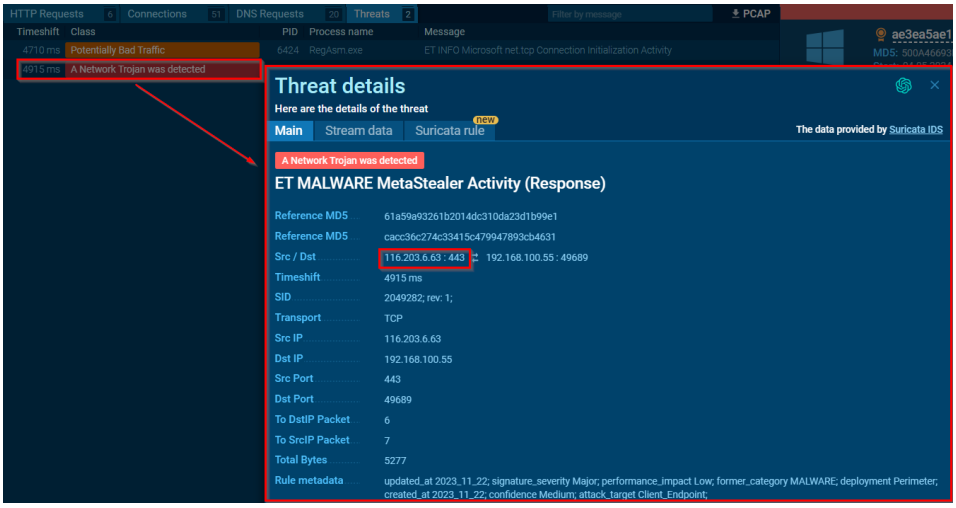
Slika 14 - Prikaz detalja o uspostavljenim vezama [app.any.run]

Naime, većina uspostavljenih veza je prema web stranicama na Microsoft domeni što je legitimni promet. Naime, Windows operacijski sustav šalje jako puno telemetrijskih podataka prema trećim stranama preko svojih poslužitelja pa je veliki promet prema njihovim adresama zapravo očekivan. Međutim, tu se ponovno pojavljuje domena aifiller[.]sbs kao i pastebin. Budući da je reputacija IP adrese „pod upitnikom“, potrebno ju je dodatno analizirati. Ove se domene pojavljuju naravno i pod DNS zahtjevima što je svakako očekivano zbog same arhitekture mreža kao takvih. Međutim, ono što je zanimljivo za nastavak analize je odjeljak prijetnji (eng. *Threats*) jer se u njemu pojavljuje IP adresa 116[.]203[.]6[.]63 povezana s ovom domenom. Dvije su klasifikacije bile ključne da se prepoznaju prijetnje pa su tako i generirana dva unosa pod odjeljkom prijetnji, a to su potencijalno zlonamjeran promet te detekcija mrežnog trojanca. Na sljedećoj su slici prikazani detalji prve od prijetnji, a kao što se može vidjeti, naslov je inicijalizacija veze (eng. *Connection Initialization Activity*). Međutim, ono što je uzrokovalo da se ta veza smatra prijetnjom je maloprije spomenuta IP adresa koja je također označena crvenim pravokutnikom na slici. U odjeljku podataka toka (eng. *Stream data*) može se vidjeti konkretan sadržaj paketa koji su razmijenjeni, međutim u ovome prikazu nije praktično vidjeti sadržaj jer je prelomljen svakih 30-ak znakova što ga čini teško čitljivim. Zbog toga će se kasnije taj tok analizirati kroz Wireshark.



Slika 15 - Prikaz prve prijetnje zlonamjernog prometa [app.any.run]

Slični detalji prikazani su i za drugu prijetnju čiji je naziv Odgovor na aktivnost *MetaStealer-a* (eng. *MetaStealer Activity (Response)*). Ona upućuje na to da je na prvu prijetnju dobiven odgovor od zapovjednog centra što se može vidjeti i po polju izvorišne i odredišne adrese u kojoj je sada maliciozna IP adresa postala izvorišna za razliku od prve prijetnje gdje je bila odredišna. Također je na slici označena crvenim pravokutnikom.



Slika 16 - Prikaz druge prijetnje mrežnog trojanca [app.any.run]

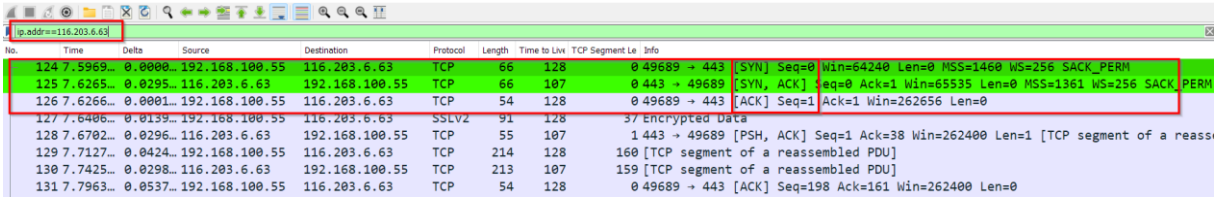
Ovime je završena analiza kroz ova dva *sandbox* okruženja u oblaku, a iz Any.Run je preuzeta snimka mrežnog prometa s pomoću koje će se u sljedećem poglavlju prikazati mrežni promet prema zabilježenoj IP adresi.

8.2.3. Wireshark analiza mrežnog prometa

Budući da su svi alati detektirali jednu specifičnu IP adresu kao malicioznu, potrebno je dodatno istražiti razmijenjene informacije između zaraženog računala i te domene. Snimka mrežnog prometa je preuzeta iz *Any.Run* platforme za analizirani uzorak Redline zlonamjernog softvera. Ovime se nastoji zaključiti što je točno napravljeno i koje informacije se šalju prema zapovjednom centru čime se cijela analiza zaključuje i određuje se njen utjecaj, a time i zaokružuje proces istrage napada i analize njegovog životnog ciklusa.

Nakon otvaranja datoteke, u traku za filtriranje se unosi filter kojim se filtrira mrežni promet s ili prema specificiranoj adresi kao što se može vidjeti na sljedećoj slici. Osim toga, vidi se uspostava TCP veze trosmjernim rukovanjem poznatijim pod engleskim terminom *3-way handshake* u kojemu računalo kontaktira zapovjedni poslužitelj s paketom u kojemu je podignuta SYN zastavica nakon čega poslužitelj odgovara paketom s podignutim SYN i ACK

zastavicama na temelju kojih računalo zna da je poslužitelj aktivan te želi i može uspostaviti traženu vezu i odgovara mu paketom s podignutom ACK zastavicom. Time je veza uspostavljena te započinje prijenos podataka. Uspostava veze, kao i filter označeni su crvenim pravokutnicima na sljedećoj slici, a ispod uspostave veze je konkretan mrežni promet.



Slika 17 - Uspostava veze prema poslužitelju [Autorski rad]

Kao što se vidi i na prethodnoj slici, mrežni promet od računala prema poslužitelju kriptiran je što otežava njegovu analizu. Međutim, koristeći funkcionalnosti Wireshark alata, moguće je pratiti cijeli tok komunikacije između ova dva uređaja. Opcijom praćenja TCP toka (eng. *Follow TCP Stream*) dobiva se cijeli tok komunikacije u nešto čitljivijem obliku od onoga prikazanog na Any.Run platformi, međutim kriptirani sadržaj nije moguće dekriptirati bez odgovarajućeg ključa. Zato je velik dio prometa nečitljiv, međutim u dijelovima komunikacije mogu se vidjeti ključni dijelovi iz kojih se zaključuje o čemu se radi u ovom konkretnom uzorku. Na sljedećoj je slici prikazan taj komunikacijski tok na kojemu je vidljivo da nakon uspostave veze, poslužitelj šalje listu podataka koje računalo treba poslati prema „ugovoru“ (eng. *Contract*) što je vidljivo iz same poveznice. To je zapravo i očekivano ponašanje uzimajući u obzir analizirane informacije iz prethodnih izvještaja poput Bitdefender izvještaja o analizi Redline uzorka [30] u kojemu su istraživači u izvornom kodu vidjeli da postoje liste koje se preuzimaju i pretvaraju u postavke koje programu služe za dohvaćanje podataka koji su traženi u ovisnosti o dobivenim postavkama.

Slika 18 - Početak komunikacije - dobivanje uputa [Autorski rad]

Iz prethodne slike vidi se dio zahtjeva kojeg je poslužitelj uputio prema računalu (tekst s crvenom pozadinom je zahtjev klijenta prema poslužitelju, a tekst s plavom pozadinom

predstavlja zahtjev poslužitelja prema klijentu. Već u tom dijelu prikazano je da se traže datoteke različitih vrsta (prema ekstenzijama) koje mogu sadržavati osjetljive podatke za prijavu na račune različitih platformi. To su većinom tekstualne datoteke u kojima se čuvaju podaci o lozinkama za specifične račune, a neke od lokacija s kojih ih sam softver treba pokušati preuzeti su radna površina (eng. *Desktop*) korisničkog profila, pohranjeni podaci Internet pretraživača (na slici Google Chrome) itd.

Na sljedećoj je slici prikazan još jedan dio dobivenih postavki u kojima se vide nazivi popularnih platformi, poglavito u IT svijetu kao što su *GitLab, Docker, AWS, Azure*, ali i *Facebook* i *Google*. Prema ovome je također vidljivo što zlonamjerni softver pokušava dobiti od zaraženih računala, a potencijalni utjecaj u slučaju dobivanja točnih podataka bi mogao biti ogroman, ovisno o motivaciji i stručnosti napadača te postavljenim zaštitama na ciljanim platformama.

Slika 19 - Prikaz dijela traženih informacija [Autorski rad]

Odgovori računala prema poslužitelju većinom su kriptirani. Međutim, na kraju je moguće vidjeti neke od telemetrijskih podataka koji su poslani u čitljivom tekstu, a prikaz dijela tih podataka je na sljedećoj slici. Ukratko se šalju podaci o trenutnom korisniku, nazivu procesa softvera koji je pokrenut, drugim procesima koji su pokrenuti na računalu, aplikacijama instaliranim na računalu itd.

Slika 20 - Dio čitljivog odgovora računala prema poslužitelju [Autorski rad]

Ovime je dinamička analiza ovog uzorka završena jer se utvrdilo ponašanje uzorka kada je aktiviran te su se analizirale kontaktirane IP Adrese, vrsta komunikacije te sam sadržaj te komunikacije.

8.3. Detekcijska pravila

Budući da je sam kod kriptiran te većinom sadrži metode izbjegavanja skeniranja i detekcije antivirusnih alata, korisno je napraviti detekcijska pravila koja će detektirati određeni zlonamjerni softver na temelju ponašanja. Takav je oblik prepoznavanja prijetnji sve važniji i sve češće korišten pojačanom integracijom umjetne inteligencije u alate za sigurnost sustava jer umjetna inteligencija može vrlo dobro prepoznati uzorke ponašanja. Međutim, također se koriste detekcijska pravila kreirana u nekom od jezika za kreiranje takvih pravila. Najpoznatiji su jezici *YARA* i *Sigma*. Pravila se temelje na prepoznatim indikatorima kompromitiranosti koji uključuju vrijednosti sažetaka, kontaktirane domene, IP adrese i sl. Prema tome, u kreirano se pravilo upisuje logika kojom se može detektirati određeni zlonamjerni softver. Valja napomenuti da je potencijalan problem kod ovakvih pravila to što se može kreirati lažno pozitivni alarm za detekciju jer se često zlonamjerni softver ponaša vrlo slično legitimnom pa i legitimni proces može biti označen kao zlonamjeran. U smanjenju takvih slučajeva pomažu i vrijednosti sažetaka. Na temelju indikatora kompromitiranosti koji su zabilježeni za analizirani uzorak u ovome radu, kreirano je i u nastavku prikazano te objašnjeno *Sigma* pravilo za detekciju.

Na sljedećoj je slici prikazano samo pravilo nakon čega je i objašnjeno.

```
title: Detekcija Redline uzorka
id: b2ff85e0-1ef0-11e8-accf-0ed5f89f718b
description: Detektira Redline Malver na temelju DNS zahtjeva i kontaktiranih IP adresa
author: Antonio
date: 2024-05-28
logsource:
    category: network_connection
    product: windows
detection:
    dns_requests:
        dns|contains:
            - 'aifiller.sbs'
            - 'pastebin.com'
    ip_connections:
        destination_ip:
            - '52.111.227.13'
            - '52.165.165.26'
            - '20.74.47.205'
            - '20.223.35.26'
            - '52.165.164.15'
            - '20.190.159.68'
            - '173.223.57.250'
            - '104.107.21.60'
            - '2.19.193.96'
            - '116.203.6.63'
            - '104.20.4.235'
            - '52.182.143.212'
    condition: dns_requests or ip_connections
falsepositives:
    - Legitimni softver koji ima slično ponašanje
level: high
```

Slika 21 - Sigma detekcijsko pravilo [Autorski rad]

Sami metapodaci nisu pretjerano važni za analizu, a uključuju podatke o autoru, datum kreiranja te naziv i opis samog pravila, a na posljetku id polje koje je zapravo UUID broj, nasumično generiran i unikatan za svako pravilo.

Postavlja se uvjet da se nadgleda mrežni promet pod poljem *logsource*, a sama detekcija ovisi o DNS zahtjevima koji u ovome slučaju sadrže dvije domene kako je bilo i ranije analizirano, a to su aifiller[.]sbs te pastebin[.]com, a druge IP adrese su također zabilježene u dinamičkoj analizi. Iako je većina IP adresa koje su tu zapisane zapravo u vlasništvu Microsofta, stavljene su u indikatore kompromitiranosti jer su kontaktirane nakon pokretanja samog uzorka Redline softvera. Uvjet za detekciju je zabilježen bilo koji od tih DNS zahtjeva ili mrežnih veza što se vidi iz *condition* polja unutar pravila. Tekstualni opis pružen je i za moguće lažno pozitivne detekcije u kojima se opisuje što i zašto bi moglo biti pogrešno označeno kao maliciozno, a sama razina prijetnje je visoka.

Ovo se pravilo nadalje može učitati u sustav za upravljanje sigurnosnim informacijama i događajima (eng. SIEM – *Security Information and Event Management*) nakon čega će se za svako detektirano ponašanje koje odgovara ovome pravilu kreirati alarm za sigurnosne analitičare koji će na temelju njega moći poduzeti dalje korake u procesu odgovora na sigurnosni događaj.

9. Zaključak

Istraženi su kibernetički napadi i njihova evolucija, s naglaskom na digitalnu forenziku i strategije kibernetičke sigurnosti. Razmatrane su različite vrste kibernetičkih napada i detekcijskih mehanizama koji se koriste za prepoznavanje i odgovaranje na te prijetnje. Kibernetičke prijetnje postaju sve sofisticiranije, a s razvojem umjetne inteligencije i drugih tehnologija, napadači mogu brže i učinkovitije zaobilaziti tradicionalne sigurnosne mjere. Cilj rada je bio kroz konkretne primjere napada prikazati kako se kibernetičke prijetnje razvijaju te kako se identifikacijom uobičajenih obrazaca napada mogu kreirati i unapređivati strategije kibernetičke sigurnosti.

U prvom dijelu rada prikazani su opći principi okvira kibernetičke sigurnosti te vrste i primjeri kibernetičkih napada, a zatim analizirane faze napada prema MITRE ATT&CK okviru, pružajući detaljan pregled taktika, tehnika i procedura koje napadači koriste. Posebno su obrađene faze kao što su pristup vjerodajnicama, otkrivanje sustava i lateralno kretanje. Uz to, analizirani su mehanizmi za detekciju napada, uključujući one temeljene na potpisima, anomalijama, statističkim metodama, znanju, rudarenju podataka i strojnom učenju. Primjeri konkretnih napada dodatno su ilustrirali teorijske koncepte i omogućili dublje razumijevanje stvarnih prijetnji te su poslužili kao osnova za preporuke za unapređenje kibernetičke sigurnosti. Analizom uzorka Redline softvera u nastavku je prikazan detaljan proces forenzičke analize konkretno *malware* napada, ali principi se mogu primijeniti na sve vrste napada.

Ta je analiza provedena koristeći tehnike statičke i dinamičke analize. Obuhvaćeno je sljedeće: pregled izvršne datoteke, identifikacija vrste datoteke, generiranje sažetaka te dekompilacija uzorka s pomoću alata kao što su *Ghidra* i *IDA Pro*. Dinamička analiza uključivala je izvođenje uzorka u kontroliranom okruženju te promatranje njegovog ponašanja, uključujući mrežni promet analiziran s pomoću Wiresharka. Korištenjem online servisa kao što je *Any.Run*, dobiveni su dodatni podaci o ponašanju zlonamjernog softvera, uključujući DNS zahtjeve i uspostavljene veze.

Jedan od rezultata ove analize bio je kreiranje Sigma pravila za detekciju Redline softvera. Ovo pravilo omogućuje pravovremenu detekciju i odgovaranje na prijetnje, što je ključno za zaštitu organizacija od kibernetičkih napada. Osim toga, identificirani indikatori kompromitiranosti pružaju konkretne smjernice za unapređenje sigurnosnih mjera.

Razumijevanje taktika i tehnika napadača ključno je za razvoj učinkovitih strategija zaštite i obrane. Time se doprinosi boljem razumijevanju suvremenih prijetnji informacijskoj sigurnosti te razumijevanju sposobnosti napadača da se prilagode i izbjegnu postojeće mjere zaštite, a sve u svrhu jačanja sveukupne otpornosti organizacija i pojedinaca na kibernetičke prijetnje kroz razvoj kvalitetnih strategija kibernetičke sigurnosti.

Popis literature

[1] S. Raghavan, “Digital forensic research: current state of the art,” *CSIT*, vol. 1, no. 1, pp. 91–114, Mar. 2013, doi: 10.1007/s40012-012-0008-7.

[2] D. Paul Joseph and J. Norman, “An Analysis of Digital Forensics in Cyber Security,” in *First International Conference on Artificial Intelligence and Cognitive Computing*, R. S. Bapi, K. S. Rao, and M. V. N. K. Prasad, Eds., Singapore: Springer, 2019, pp. 701–708. doi: 10.1007/978-981-13-1580-0_67.

[3] “What is the Diamond Model of Intrusion Analysis?,” SOCRadar® Cyber Intelligence Inc. Accessed: Apr. 23, 2024. [Online]. Available: https://socradar.io/what-is-the-diamond-model-of-intrusion-analysis/

[4] C. T. Corp, “CyCraft Classroom: MITRE ATT&CK vs. Cyber Kill Chain vs. Diamond Model,” CyCraft. Accessed: Apr. 23, 2024. [Online]. Available: https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f

[5] N. Naik, P. Jenkins, P. Grace, and J. Song, “Comparing Attack Models for IT Systems: Lockheed Martin’s Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model,” in *2022 IEEE International Symposium on Systems Engineering (ISSE)*, Oct. 2022, pp. 1–7. doi: 10.1109/ISSE54508.2022.10005490.

[6] “The CSF 1.1 Five Functions,” *NIST*, Apr. 2018, Accessed: Jun. 21, 2024. [Online]. Available: https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

[7] K. M. Sudar, P. Deepalakshmi, P. Nagaraj, and V. Muneeswaran, “Analysis of Cyberattacks and its Detection Mechanisms,” in *2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Nov. 2020, pp. 12–16. doi: 10.1109/ICRCICN50933.2020.9296178.

[8] “What Is a Cyberattack? | Microsoft Security.” Accessed: Jun. 21, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cyberattack

[9] laurama, “June 2023’s Most Wanted Malware: Qbot Most Prevalent Malware in First Half of 2023 and Mobile Trojan SpinOk Makes its Debut,” Check Point Blog. Accessed: Jun. 21, 2024. [Online]. Available: https://blog.checkpoint.com/security/june-2023s-most-wanted-malware-qbot-most-prevalent-malware-in-first-half-of-2023-and-mobile-trojan-spinok-makes-its-debut/

[10] “Latest SQL Injection news,” BleepingComputer. Accessed: Jun. 22, 2024. [Online]. Available: https://www.bleepingcomputer.com/tag/sql-injection/

[11] “Latest Phishing news,” BleepingComputer. Accessed: Jun. 22, 2024. [Online]. Available: https://www.bleepingcomputer.com/tag/phishing/

[12] “ONNX phishing service targets Microsoft 365 accounts at financial firms,” BleepingComputer. Accessed: Jun. 22, 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/onnx-phishing-service-targets-microsoft-365-accounts-at-financial-firms/

[13] “New phishing toolkit uses PWAs to steal login credentials,” BleepingComputer. Accessed: Jun. 22, 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-phishing-toolkit-uses-pwas-to-steal-login-credentials/

[14] “Warmcookie Windows backdoor pushed via fake job offers,” BleepingComputer. Accessed: Jun. 22, 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/warmcookie-windows-backdoor-pushed-via-fake-job-offers/

[15] “Latest Botnet news,” BleepingComputer. Accessed: Jun. 22, 2024. [Online]. Available: https://www.bleepingcomputer.com/tag/botnet/

[16] “Latest XSS news,” BleepingComputer. Accessed: Jun. 22, 2024. [Online]. Available: https://www.bleepingcomputer.com/tag/xss/
[17] “Famous DDoS attacks | Biggest DDoS attacks.” Accessed: Jun. 22, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/
[18] “Do Not Cross The ‘RedLine’ Stealer: Detections and Analysis,” Splunk. Accessed: Apr. 26, 2024. [Online]. Available: https://www.splunk.com/en_us/blog/security/do-not-cross-the-redline-stealer-detections-and-analysis.html
[19] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington, and C. Thomas, “MITRE ATT&CK: Design and Philosophy,” Mar. 2020, Accessed: Apr. 30, 2024. [Online]. Available: https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy
[20] “Tactics - Enterprise | MITRE ATT&CK®.” Accessed: Apr. 30, 2024. [Online]. Available: https://attack.mitre.org/tactics/enterprise/
[21] “LAPSUS$, DEV-0537, Strawberry Tempest, Group G1004 | MITRE ATT&CK®.” Accessed: Apr. 30, 2024. [Online]. Available: https://attack.mitre.org/groups/G1004/
[22] “Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®.” Accessed: Apr. 30, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1566/
[23] “Drive-by Compromise, Technique T1189 - Enterprise | MITRE ATT&CK®.” Accessed: Apr. 30, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1189/
[24] “Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®.” Accessed: Apr. 30, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1053/
[25] “What Is Svchost.exe (Service Host)?,” Lifewire. Accessed: Jun. 20, 2024. [Online]. Available: https://www.lifewire.com/scvhost-exe-4174462
[26] M. Labs, “Redline Stealer: A Novel Approach,” McAfee Blog. Accessed: Apr. 28, 2024. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/
[27] “RedLine/Vidar Abuses EV Certificates, Shifts to Ransomware,” Trend Micro. Accessed: Apr. 30, 2024. [Online]. Available: https://www.trendmicro.com/en_us/research/23/i/redline-vidar-first-abuses-ev-certificates.html
[28] “Attackers Hide RedLine Stealer Behind ChatGPT, Google Bard Facebook Ads.” Accessed: Mar. 15, 2024. [Online]. Available: https://www.darkreading.com/cyberattacks-data-breaches/attackers-hide-redline-stealer-behind-chatgpt-google-bard-facebook-ads
[29] H. Saleous *et al.*, “COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities,” *Digital Communications and Networks*, vol. 9, no. 1, pp. 211–222, Feb. 2023, doi: 10.1016/j.dcan.2022.06.005.
[30] “Bitdefender-PR-Whitepaper-RedLine-creat6109-en-EN.pdf.” Accessed: Mar. 10, 2024. [Online]. Available: https://www.bitdefender.com/files/News/CaseStudies/study/415/Bitdefender-PR-Whitepaper-RedLine-creat6109-en-EN.pdf
[31] “Credentials from Password Stores, Technique T1555 - Enterprise | MITRE ATT&CK®.” Accessed: May 03, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1555/
[32] “OS Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK®.” Accessed: Apr. 26, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1003/
[33] “Unsecured Credentials, Technique T1552 - Enterprise | MITRE ATT&CK®.” Accessed: May 03, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1552/
[34] “Impact, Tactic TA0040 - Enterprise | MITRE ATT&CK®.” Accessed: May 03, 2024. [Online]. Available: https://attack.mitre.org/tactics/TA0040/
[35] R. Sihwail, K. Omar, and K. A. Zainol Ariffin, “A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis,” *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 4–2, p. 1662, Sep. 2018, doi: 10.18517/ijaseit.8.4-2.6827.

Popis slika

Popis tablica