SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 1674

MODELIRANJE PONAŠANJA NAPADAČA NA INTERNETU PRIJE I TIJEKOM PROVOĐENJA NAPADA

Igor Kramarić

Zagreb, lipanj 2018.

Sadržaj

Popis slika

Popis tablica

Popis ispisa

1. Uvod

Internet je od svog nastanka 1965. godine pa do danas postao globalni sustav međusobno povezanih računalnih mreža [1]. Kroz to vrijeme postao je i vrlo važna komponenta ljudskog života, tj. integralni dio za komercijalne i privatne svrhe, te za javne službe i organizacije koje upravljaju kritičnom infrastrukturom. Tako kompleksan sustav ovisi o različitim entitetima (hardver, programski proizvodi, procedure, politike, ljudi, itd.) na različitim razinama apstrakcije. Proporcionalno toj kompleksnosti raste i broj prijetnji, koje su kriminalcima dale novi način za krađu, a vojskama za ratovanje. Prema izvještaju *Online Thrust Alliance* (OTA) organizacije, 2017. godina je proglašena godinom s dosad najvećim brojem krađa osobnih podataka i sigurnosnih incidenata [2].

Postoji veliki broj razloga zašto je broj napada na Internetu u porastu, a neki se pri tome posebno izdvajaju. Prvi razlog je u samoj arhitekturi Interneta koji u samom početku nije građen sa sigurnošću na prvom mjestu [3]. Drugi razlog je to što Internet nije transparentan u smislu da je teško s velikom sigurnošću povezati napad sa stvarnom osobom ili skupinom [4]. Treći razlog je sve veća sofisticiranost napadača u tehničkom i organizacijskom smislu [5].

Povećanjem vještine i sofisticiranosti, kibernetički napadači predstavljaju veliku prijetnju organizacijama i državama te povjerljivosti, integritetu i dostupnosti podacima koje one posjeduju. Posljedica toga je da se branitelji više ne mogu oslanjati na metode obrane koje su se koristile u prošlosti. Za uspješno zaustavljanje današnjih napada više nisu dovoljne samo tehničke obrane, kao što su antivirusni programi ili vatrozidi, a razlog tome je da se niti napadači više ne oslanjaju na čisto tehničke aspekte za eksploataciju računalnih sustava, nego sve češće iskorištavaju ljudsku nepažnju i nedostatak obrazovanja kao inicijalni vektor napada.

U svrhu čim efikasnije obrane od kibernetičkih prijetnji, branitelji moraju stalno primjenjivati i unaprjeđivati nove metode i tehnike koje će se na odgovarajući način moći oduprijeti stalnom razvoju novih metoda napada. Zbog toga je potrebno promatrati širu sliku, te uz digitalne tragove koje napadači ostavljaju, treba pratiti i kako se oni ponašaju. Preciznije treba razumjeti njihove taktike, tehnike i procedure koje koriste tijekom cijelog životnog ciklusa napada.

U ovom radu bit će objašnjene metode modeliranja napadača, koje spadaju u proaktivne metode i bave se proučavanjem cijelog životnog ciklusa napada te braniteljima mogu omogućiti veću sigurnost kritičnih resursa koje brane. Fokus će biti na naprednim ustrajnim prijetnjama (engl. *Advance persistent threats*, APT) koje su u proteklih nekoliko godina zbog svojih mogućnosti i organiziranosti postale najveća sigurnosna prijetnja organizacijama i državama.

Svrha uključivanja znanja o napadačima te njihovo modeliranje je da se braniteljima omogući drugačija perspektiva, te da se dobije dublje razumijevanje iza samih napada i omogući proaktivno planiranje obrane, te bolju reakciju na napad koji je u tijeku. Modeliranje napadača može dati odgovor na pitanja kao što su: što zapravo napadač radi, gdje i kako, te kakve su mogućnosti da ih se spriječi u tome. Također, modeliranje napadača omogućuje braniteljima da bolje rasporede svoje ograničene resurse (novčane i ljudske) u svrhu bolje sigurnosti kritičnih resursa koje brane.

Ovaj rad organiziran je na sljedeći način: U 2. poglavlju bit će objašnjena šira slika kibernetičkih napada i napadača s ciljem da se bolje razumiju poglavlja koja slijede. U sljedećem, 3. poglavlju,

bit će objašnjeni razni modeli napadača koji se danas koriste. Neki od najpoznatijih kibernetičkih napada bit će modelirani u 4. poglavlju. U svrhu pokazivanja fleksibilnosti modela, izabrana su 2 vrlo različita scenarija. Pregled postojećih alata koji mogu pomoći braniteljima testirati njihove obrane, te njihove prednosti i nedostatke bit će opisani u 5. poglavlju. U 6. poglavlju dan je zaključak i smjernice za daljnji rad.

2. Ekosustav kibernetičkih napada

Modeliranjem napadačevih radnji organizacije mogu imati velike koristi za detekciju napada koji je u tijeku ili za bolju i efikasniju uspostavu obrambenih mehanizama. Da bi se ispravno pristupilo toj radnji, potrebno je imati detaljan uvid u razne aspekte koji okružuju kibernetičke napade. Prvi potencijalni problem na koji bi organizacije mogle naletjeti je kako odabrati koje napade i napadače modelirati. Zbog velike raznolikosti organizacija po infrastrukturi, djelatnosti i geografskoj lokaciji, te velikog broj napadača i njihovih metoda to nije jednostavno pitanje.

Primjer kompleksnosti kibernetičkog kriminala moguće je pronaći u EUROPOL-ovom IOCTA izvješću za 2017. godinu u kojem se može naći geografska distribucija kibernetičkog kriminala po kontinentima [13]. U izvješću je detaljnije razrađeno koji kontinenti i države u njima su izvorišta i odredišta kibernetičkih napada. Navedeno izvješće može se sažeti u sljedeće zaključke:

- Afrika - Polovica država članica Europske unije je karakteriziralo Afriku kao izvor specifičnih kibernetičkih prijetnji. Najčešće prijetnje iz Afrike su društveni inženjering i kibernetičke prijevare. Također nekoliko država je prijavilo Afriku kao izvor napada na kritičnu infrastrukturu.
- Amerika - Sjeverna Amerika česta je žrtva kada je u pitanju financijski motivirani kibernetički kriminal, s 37% malicioznih elektroničkih poruka od ukupnog prometa. Također Sjeverna Amerika vodi listu po krađi podataka (49%) i po cijeni po krađi podataka. Sjeverna Amerika predvodi i po broju napada prouzročenih ucjenjivačkim zloćudnim kodom (engl. *Ransomware*) s 34% od ukupnog broja takvih napada u cijelom svijetu, te po malicioznim programima koji napadaju bankarsku industriju. Također, Sjeverna Amerika sadržava veliku količinu ukupnog broja Web poslužitelja u svijetu te se na tim poslužiteljima nalazi oko 50% svih lažnih Web stranica. Za razliku od Sjeverne Amerike, Južna Amerika je okarakterizirana kao izvor širenja malicioznih programa za bankomate.
- Azija - Iako se u Aziji nalazi najveći broj korisnika Interneta, sadrži nerazmjerno mali broj kibernetičkih prijetnji. Japan, Kina i Južna Koreja su države koje u svojem posjedu imaju oko 11% poslužitelja koji služe za upravljanje raznim mrežama kompromitiranih računala (engl. *Botnets*). Za Kinu i Sjeverna Koreju se pretpostavlja da upravljaju s nekoliko državno sponzoriranih grupa. Azija je česta žrtva mobilnih napada, tj. napada pomoću malicioznih mobilnih programa. Uzrok tome je vrlo vjerojatno velika količina piratiziranog softvera.
- Europa - Najveći broj prijetnji u Europi dolazi iz same Europe. Najčešće vrste su društveni inženjering, maliciozni programi i napadi na kritičnu infrastrukturu. Istočna Europa je okarakterizirana kao izvor velikog broj malicioznih programa za bankomate, a Rusija kao dom za veliki broj državno sponzoriranih napadača i profesionalnih kibernetičkih kriminalaca. Europa se nalazi na 2. mjestu po broju financijski motiviranih napada. Kroz zadnjih nekoliko godina, poboljšanja u Internetskoj infrastrukturi na području Europe počela su privlačiti kriminalce koji svoju maliciozni infrastrukturu grade upravo na području Europe.

- Oceanija - Prema izvješću Australskih agencija za provedbu zakona najčešće prijetnje za Oceaniju su maliciozni programi za krađu podataka, ucjenjivački zlćudni kodovi i prijevare vezane uz društveni inženjering.

Cilj ovog poglavlja je dati pregled pojmova čije razumijevanje će olakšavati daljnje praćenje rada i pomoći braniteljima u razrješavanju osnovnih koncepata vezanih uz napade i napadače. Prvo se detaljnije opisuje interakcija između napadača i branitelja te pojmovi koji su vezani uz sigurnost. Nakon toga, opisane su vrste napadača prema raznim karakteristikama koje ih razdvajaju, a neke od posebno važnih su motivi, vještine i ciljevi.

2.1. Interakcija napadača i branitelja

Kako bi se bolje razumio koncept kibernetičkog napada, potrebno je detaljnije razumjeti interakciju napadača i branitelja te jasno definirati komponente od kojih se ta interakcija sastoji. Potrebno je znati na koji način branitelj štiti svoju imovinu i na koji način napadač eksploatira ranjivosti u braniteljevoj infrastrukturi kako bi ostvario svoj cilj. U nastavku su objašnjeni pojmovi vezani uz njihovu interakciju.

Imovina je resurs s ekonomskom vrijednošću koju pojedinac, organizacija ili država posjeduje ili nad kojim ima kontrolu, s očekivanjem da će mu u budućnosti donijeti korist. Imovina se može klasificirati u 4 vrste: (i) trenutna, (ii) fiksirana, (iii) financijska i (iv) nematerijalna [7].

Prijetnja je bilo kakva okolnost ili događaj s potencijalom da negativno utječe na djelovanje organizacije (uključujući njezinu misiju, funkcionalnost, imidž ili reputaciju), imovinu organizacije, ili pojedinca kroz informacijski sustav [8]. Neke od najvećih prijetnji u 2017. godini prema ENISA Threat Landscape izvješću su: maliciozni program, Web napadi, nedostupnost servisa, kriptoviruts (engl. *Ransomware*), krađa identiteta, krađa osjetljivih korisničkih podataka i kibernetička špijunaža [6].

Ranjivost je propust ili slabost u dizajnu sustava, implementaciji ili u operaciji i upravljanju koja se može eksploatirati s ciljem narušavanja sigurnosne politike sustava [9]. Ranjivosti mogu nastati zbog neispravnog validiranja korisničkog unosa, pogrešne konfiguracije sustava, grešaka u dizajnu sustava, itd. Postoji veliki broj različitih vrsta ranjivosti, a primjeri najopasnijih napada na Web aplikacije prema OWASP organizaciji su: neautorizirano ubacivanje koda, neispravna autentifikacija korisnika, izlaganje osjetljivih podataka, neispravna kontrola pristupa, pogrešna sigurnosna konfiguracija, korištenje dostupnih biblioteka koje sadrže poznate ranjivosti i nedovoljno logiranje i nadziranje [60].

Protumjera je akcija, uređaj, procedura ili tehnika koja smanjuje prijetnju, ranjivost ili napad s ciljem eliminiranja ili prevencije istog, minimiziranjem štete koju može prouzročiti ili otkrivanjem i prijavom tako da se kasnije može napraviti korektivna akcija [10]. Primjer protumjera je vatrozid, antivirusni program, razni autentifikacijski sustavi, itd.

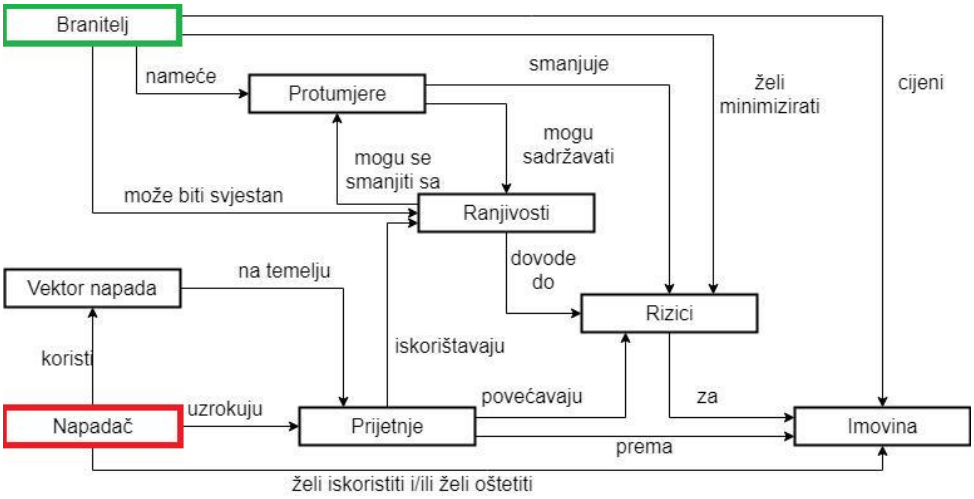
Rizik je razina utjecaja na organizacijsko djelovanje, organizacijsku imovinu ili individualca koja bi mogla nastati djelovanjem prijetnje na informacijski sustav i izglednosti da se ta prijetnja ostvari [10].

Vektor napada je put koji napadač koristi kako bi dobio pristup braniteljevoj imovini [11]. Česti vektori napada uključuju spam poruke, mrežnu krađu identiteta (engl. *Phishing*), maliciozno oglašavanje ili napad *Watering hole* [12].

Kibernetički napad je pokušaj dobivanja ilegalnog pristupa računalu ili računalnom sustavu s ciljem da se prouzrokuje šteta narušavanjem povjerljivosti, integriteta i dostupnosti imovine branitelja.

Napadač je pojedinac, grupa, organizacija ili vlada koja izvodi napad. Aktor kojemu je cilj pomoću malicioznog djelovanja kompromitirati informacijski sustav [10]. Više o vrstama napadača bit će rečeno u odjeljku 2.2.

Na slici 2.1 prikazana je interakcija napadača i branitelja, odnosno ranije objašnjeni pojmovi povezani su relacijama u smislenu cjelinu. Cilj branitelja je zaštititi imovinu koja mu je od interesa i koju on cijeni [61]. Branitelj će napraviti analizu prijetnji koje se odnose na imovinu koju on štiti i određuje razinu rizika uz svaku prijetnju. Prioritiziranje prijetnji po riziku omogućuje branitelju lakši i efikasniji odabir protumjera sa svrhom smanjenja rizika. Protumjere postavlja branitelj s ciljem da ukloni ili smanji utjecaj ranjivost i time posljedično smanji rizik koje te ranjivosti prouzrokuju nad imovinom. Ranjivosti omogućavaju i povećavaju vjerojatnost da se prijetnje ostvare. Napadaču je cilj doći do imovine koja mu je od interesa i koju cijeni, te želi koristiti tu imovinu suprotno od interesa branitelja [61]. Napadač preko vektora napada realizira prijetnju tako da iskorištava ranjivosti koje zaobilaze protumjere te tako dolazi do imovine koju želi.



Slika 2.1 Interakcija napadača i branitelja [6]

Da bi se u potpunosti razumjeli termini koji su opisani, u nastavku je dan primjer organizacije koja sadrži veliki broj privatnih podataka svojih korisnika. Tvrtka prirodno želi zaštiti podatke svojih korisnika, a također i svoj ugled, te je zbog toga najveća prijetnja toj tvrtki krađa privatnih podataka korisnika. Cilj je minimizirati rizik krađe privatnih podataka i tvrtka primjenjuje razne protumjere da bi osigurala tu imovinu. Primjeri protumjera koje tvrtka koristi su vatrozidi, redovite zakrpe sustava, itd. Problem koji je tvrtka uočila je taj da je pristup svim podacima

zaštićen slabom lozinkom. Da bi napadač pogodio lozinku i realizirao prijetnju mora nekim putem doći do sučelja gdje se lozinka unosi. Put kojim će napadač doći do sučelja je vektor napada, a primjer vektora napada je krađa računala djelatnika tvrtke koji ima pristup tom sučelju.

Problem prikazanog na slici 2.1 je da ne daje puni uvid u djelovanje napadača. Kako bi napadač znao tko ima pristup sučelju on treba raditi izviđanje i proučiti infrastrukturu i organizaciju tvrtke. Te djelatnosti se mogu odvijati i bez direktnog kontakta napadača i branitelja. Da bi se te djelatnosti mogle uočiti, branitelj mora znati kako napadač izvodi te djelatnosti pa prema tome krojiti svoje protumjere da bi se mogao obraniti i prije nego napadač uopće krene u napad. Modeli koji su opisani u 3. poglavlju daju mogućnost braniteljima da na strukturiran način opisuju i klasificiraju djelatnosti napadača prije i tijekom napada, sa svrhom maksimalnog umanjenja rizika.

2.2. Vrste napadača

Cilj ovog potpoglavlja je dati pregled i klasifikaciju napadač. Primarne karakteristike prema kojima se napadači razlikuju su motivi, vještine, resursi i ciljevi. Vrste napadača preuzete su iz MACE (engl. *Military Activities and Cyber Effects*) klasifikacije [14].

Početnici (engl. *Script Kiddies*) su najmanje sofisticirani napadači sa slabim tehničkim mogućnostima, kojiza svoje ciljeve koriste tuđe alate bez razumijevanja njihova rada. Pretežno su to mlađi ljudi, motivirani dosadom, privlačenjem pažnje ili povećanjem svog statusa u nekoj računalnoj zajednici. Većinom djeluju pojedinačno i slabih su financijski mogućnosti.

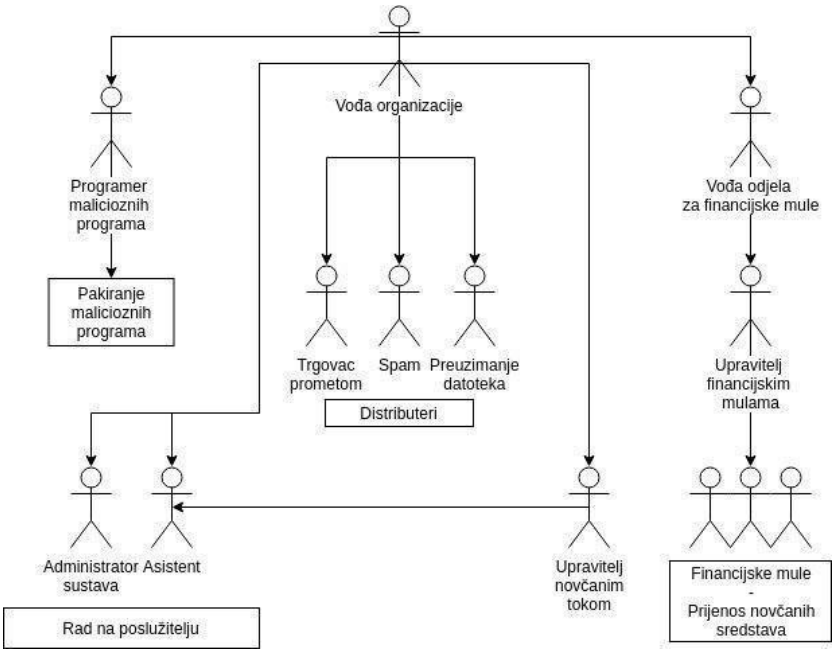
Politički aktivisti (engl. *Hacktivist*) su pojedinci ili grupe koje se malicioznim radnjama žele suprotstaviti nečemu za što misle da je pogrešno ili je protiv njihovog uvjerenja. Politički aktivisti su aktori koji su preslikali aktivizam u kibernetičku domenu [15], a njihova motivacija je političkog tipa. Meta napada političkih aktivista su različite te mogu biti od privatnih organizacija, preko javnih službi, pa sve do kritične infrastrukture [16]. Političkim aktivistima je cilj da se za njihov napad zna zašto su ga napravili i da se za taj napad pročuje kako bi se poruka proširila. Politički aktivisti u većini slučajeva nisu financijski potpomognuti, a zbog slabijih vještina i nestrpljenja najčešće napadaju Web stranice pomoću DDoS (engl. *Distributed Denail of Service*) napada [17]. Najpoznatiji politički aktivisti su Anonymous grupa.

Kibernetički vandali su napadači koji po motivaciji mogu biti slični početnicima, ali mogu biti umiješani i u ozbiljnije kriminalne radnje, kao što su krađe identiteta i financijske prijevare. Za razliku od početnika imaju veću razinu znanja. Mogu djelovati kao pojedinci ili u grupi te su slabih financijski mogućnosti.

Zaposelnici (engl. *Insiders*) su specifična vrsta napadača koji izvršavaju svoje napade na organizaciju u kojoj zaposleni. Oni mogu, ali i ne moraju posjedovati visoko tehničko znanje, ali posjeduju znanje o organizaciji i inicijalno imaju veće privilegije pristupa. Motivacija im je najčešće osveta zbog nekih postupaka njihovog poslovođe, a to manifestiraju kroz sabotažu sustava ili objavom privatnih podataka organizacije. Gotovo uvijek rade kao pojedinci i slabih su financijskih mogućnosti.

Sljedeće 3 vrste napadača su ujedno i fokus ovog rada. Ti napadači organizirani su kao skupine i funkcioniraju na sličan način kako funkcioniraju i legitimne organizacije. Također izvode ciljane i kompleksne napade. Ciljani napad znači da te organizacije nisu oportunističke. Razlika je u tome da oportunistički napadi napadaju veliki broj žrtava, te se nadaju da će nanijeti štetu čim većem broju žrtava, dok se ciljani napadi najčešće odnose na jednu ili malenu skupinu organizacija.

Profesionalne kibernetičke kriminalne skupine su vrsta napadača koja je primarno financijski motivirana. Te skupine funkcioniraju na sličan način kao i legitimne organizacije, a unutarnja struktura jedne takve skupine prikazana je na slici 2.2.



Slika 2.2 Struktura kibernetičke kriminalne skupine [70]

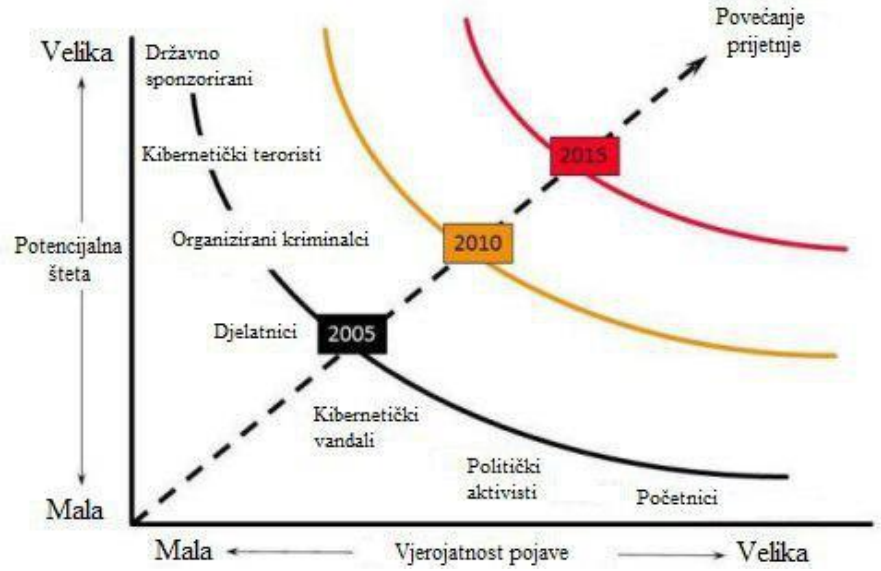
Kao i kod legalnih organizacija, postoji voditelj cijele skupine, koji pod svojom nadležnošću ima nekoliko odjela. Na slici 2.2 prikazani su odjeli za izradu malicioznih programa, za uspostavu i održavanje infrastrukture, odjel za distribuiranje malicioznog sadržaja i odjel za upravljanje protokom novaca. Meta napada takvih kriminalnih skupina su sve ustanove koje imaju podatke koji se daju monetizirati, kao primjerice kreditne kartice ili zdrastveni podaci. Ove skupine su dobro financirane i posjeduju relativno velike vještine. Iako koriste slične tehnike i alate kao i državno sponzorirani napadači, njihov princip rada je drugačiji jer im ustrajnost da ostanu neotkriveni nije toliko važna [19]. Također za razliku od ostale dvije skupine, ova vrsta napadača izvršava i oportunističke napade [20]. Primjer financijski motiviranog napada je napad na tvrtku Target.

Kibernetički teroristi (engl. *Cyber terrorist*) su napadači koji su najčešće umiješani u neku vrstu kibernetičkog ratovanja s protivničkom vladom ili nekim djelom vladine organizacije te države s ciljem destabilizacije ili uništavanja. Postoji više razina sofisticiranosti kibernetičkih terorista,

ali u ovom radu se promatra samo najopasnija vrsta koja pokazuje vrlo visoku sofisticiranost prilikom provođenja napada. Tipično su vrlo dobro financijski potpomognuti, vrlo velikih vještina i često tajnovita skupina. Motivi su im politički, religijski ili ideološki. Najčešće mete njihovih napada je kritična infrastruktura.

Državno sponzorirani napadači (engl. *Nation-state sponsored attackers*) ili češće nazivani *napredne ustrajne prijetnje* (engl. *Advanced persistant threat,* APT) su grupe koje rade direktno pod nadzorom vojne ili obavještajne službe neke države. Ustrajnost u imenu napadača odnosi se na njihovu upornost da ostvare svoj cilj. Motivirani su interesima službi čiji su sastavni djelovi, odnosno država za koje u konačnici rade. Financijski su jako dobro potpomognuti, posjeduju vrlo visoku razinu vještine, imaju pristup obavještajnim informacijama te su pod zaštitom država za koje obavljaju napade. Najčešći ciljevi su im kibernetička špijunaža, kompromitacija podataka ili sabotaža računalnih sustava [19]. Mete napada se protežu od privatnog sektora do kritične infrastrukture, ali najčešće u određenoj državi ili određenoj skupini država.

Na slici 2.3 je graf koji prikazuje kako se kroz godine povećava vjerojatnost napada i vjerojatnost da će taj napad uspjeti, tj. uzrokovati veliku štetu s obzirom na različite vrste napadača. Na crnoj liniji može se vidjeti da je 2005. godine vjerojatnost pojave napada od strane napadača Početnika bila velika, ali šteta prouzročena njihovim napadima mala, dok je pojava Državno sponoziranih napadača bila mala, ali prouzročena šteta velika. Crvena linija prikazuje stanje između vjerojatnosti napada i štete prouzročene napadom za 2015. godinu. Za razliku od crne linije, na crvenoj liniji može se vidjeti da broj napada od strane napadača Početnika nije znatno porastao, ali je šteta prouzročena tim napadima znatno porasla. Kod Državno sponzoriranih napadača situacija je upravo suprotna, tj. šteta koju oni prouzroče svojim napadom nije previše narasla u odnosu na 2005. godinu, što je i logično pošto su oni bili u stanju i tada napraviti jako veliku štetu, ali broj napada od strane Državno sponzoriranih napadača je znatno porasla.



Slika 2.3 Povećanje opasnosti od različitih napadača (modificirano iz [14])

3. Modeliranje napadača

Primarni cilj svakog branitelja je osigurati svoju imovinu, ali za postizanje visoke razine sigurnosti potrebno je posjedovati veliku količinu znanja i ljudskih resursa. Za efikasnu raspodjelu ljudskih i financijskih resursa u svrhu čim većeg poboljšanja sigurnosti organizacije potrebno je znati što organizacija posjeduje i koje su joj prijetnje. Da bi se to moglo ostvariti potrebno je znati kako napadači funkcioniraju, tj. kakve su im strategije, tehnike, alati i procedure (engl. *Techniques, tools and procedures,* TTP), te kako se onda tim znanjem može otežati tim istim napadačima ostvarivanje njihovih ciljeva. Ako je cijena napada veća od dobijene koristi, onda je ta organizacija loša meta iz perspektive napadača. Kako bismo razumjeti napadačke strategije i TTP-ove potrebni su nam modeli pomoću kojih možemo opisivati napade koje napadači provode.

Modeliranje napadača je apstraktan prikaz napadačevog ponašanja i njegovih karakteristika te služi za razvijanje i analiziranje hipoteza ili tvrdnji o efikasnosti braniteljevih tehnologija, arhitekturalnih odluka o sustavu i/ili braniteljskih akcija protiv napadača [21].

U daljnjem djelu ovog poglavlja bit će detaljno opisani najpoznatiji modeli ponašanja napadača. Također bit će objašnjeni neki pomoćni modeli i klasifikacije koje mogu pomoći u razumijevanju djelovanja napadača.

3.1. Prekidanje lanca

Model prekidanja lanca (engl. *Kill chain*) izvorno je nastao kao vojni koncept za opisivanje strukture napada, tj. za lakši prikaz kretanja napadač. Vojni model se sastoji od 4 dijela: identifikacija mete, slanje vojnih snaga prema meti, donošenje odluke o napadu i naredba za napad te uništavanje mete [22]. Cilj izrade modela prekidanja lanca za neki napad je dobiti slijedni tijek napada kako bi se olakšao prekid djelovanja protivnika. Što se bliže početku lanca napadač zaustavi, to je napadač manje štete uspio napraviti.

U ovom potpoglavlju bit će opisani modeli koji su izvedenica modela prekidanja lanca u svrhu korištenja istih u kibernetičkom svijetu. Prvo će detaljno biti objašnjena dva najpoznatija modela te će se poslije ukratko opisati ostali modeli koji postoje.

3.1.1. Prekidanje kibernetičkog lanca

Model prekidanja kibernetičkog lanca (engl. *Cyber Kill Chain*, CKC) razvila je tvrtka *Lockheed Martin*, a služi za modeliranje ofenzivnih aktivnosti napadača [23]. Korištenjem modela CKC moguće je bolje prioritizirati indikatore iz različitih izvora unutar organizacije, bolje

prioritizirati ulaganje u obrambene proizvode, procjenjivati efektivnosti obrambenih mjera i korelirati tehnike više različitih napada [24].

CKC pruža radni okvir za raščlanjivanje napada na 7 faza: izviđanje, naoružavanje, dostavljanje, eksploatiranje, instaliranje, naredbe i kontroliranje, djelovanje prema cilju. Na slici 3.1 je prikazan CKC model i njegove faze. U nastavku je detaljnije razrađena svaka od 7 faza te je objašnjeno što branitelj može učiniti koristeći znanje o pojedinoj fazi napada.

Slika 3.1 Model prekidanja kibernetičkog lanca

Izviđanje (engl. *Reconnaissance*) je faza u kojoj napadač prikuplja informacije o meti [23]. Mete mogu biti raznolike, od pojedinca do organizacija u privatnom sektoru ili kritične infrastrukture. Faza izviđanja se dodatno može podijeliti u identifikaciju meta koje mogu zadovoljiti ciljeve napadača, odabiranje meta i detaljno profiliranje. Način na koji se izvodi faza izviđanja može se podijeliti u dvije skupine: pasivno i aktivno izviđanje [23]. Pasivno izviđanje je prikupljanje informacija o meti, bez direktne interakcije napadača s metom. Primjer pasivnog izviđanja je pregled podataka o meti u otvorenim Internetskim bazama (npr. *Whois*) i identifikaciji zaposlenika organizacije putem društvenih mreža. Za razliku od pasivnog, aktivno izviđanje podrazumijeva direktan kontakt s metom, te u tim slučajevima postoji mogućnost izazivanja alarma obrambenih mehanizama. Primjer aktivnog izviđanja je profiliranje računalnih sustava mete (npr. skeniranje portova). Faza izviđanja je temelj za daljnje aktivnosti jer omogućuje napadaču da odredi koje će alate i tehnike koristiti, koje će metode dostave koristiti i na koji način će eksploatirati metu [23].

Iz perspektive branitelja detekcija izviđanja može biti vrlo teška, pogotovo detekcija pasivnog izviđanja. Detekcija izviđanja može dati uvid u namjere napadača. Primjer mogućih mjera

obrane je izgradnja obrambenih mehanizama za detekciju specifičnog načina pregledavanja Web stranica ili komunikaciju s računalnim sustavima [25].

Naoružavanje (engl. *Weaponization*) je faza u kojoj napadač dizajnira i kreira plan upada i stvara maliciozne programe specifične za metu [26]. Postoje dvije vrste malicioznih programa koji se koriste u ovoj fazi, maliciozni korisni teret (engl. *Malicious payload*) i eksploatacijski kod (engl. *exploit*) [23]. Maliciozni korisni teret može imati razne funkcionalnosti, ali najčešće služi u svrhe dobivanja udaljenog pristupa na računalnom sustavu žrtve. Eksploatacijski kod služi za dostavljanje malicioznog korisnog tereta, iskorištavanjem neke ranjivosti. Najčešći primjeri su eksploatacijski kodovi koji iskorištavaju ranjivosti u PDF čitačima i *MS Office* alatima. Primjeri alata koji su korišteni u razvijanju malicioznih programa su *Metasploit, Luckystrike* i *Veil* radni okviri [27]. Također, to je faza u kojoj napadač odlučuje hoće li sam izraditi te mogućnosti ili će ih nabaviti na crnom tržištu te testira svoje maliciozne programe da li rade dobro i koliko su uspješni u zaobilaženju obrambenih kontrola kao što su antivirusni programi.

Branitelj ne može detektirati izradu tih alata [25]. Mjere koje branitelj može poduzeti su detektiranje raznih vrsta artefakata u raznim malicioznim programima, sa svrhom ukomponiranja istih u svoje obrambene mehanizme. Također aktivno praćenje novosti vezanih uz maliciozne programe, te praćenje događanja na crnom tržištu može biti od velike pomoći branitelju.

Dostava (engl. *Delivery*) je faza u kojoj napadač šalje maliciozne programe prema meti [23]. Najčešće metode koje se danas koriste zahtijevaju interakciju korisnika. Primjer takvih metoda su elektroničke poruke s malicioznim prilozima, maliciozne Web stranice i maliciozni USB memorijski diskovi. Ova faza predstavlja veći rizik za napadača jer ostavlja tragove. Također, sve metode koje se oslanjaju na ljudsku interakciju moraju biti dobro oblikovane i privlačne za metu [23].

Dostava je prva faza u kojoj branitelj može detektirati i blokirati napad [25]. Neki od načina koje branitelj može iskoristiti u svoju korist analiziranjem CKC su: analiziranje medija preko kojeg je napadač dostavio svoje maliciozne programe, razumijevanje koji zaposlenici su bili ciljani, koje su njihove uloge i odgovornosti te analiza vremena u kojem je napadač krenuo s fazom dostave [25].

Eksploatacija (engl. *Exploitation*) je faza u kojoj se pokreće eksploatacijski kod [25]. Pošto se najčešće metode dostave temelje na slanju elektroničke pošte, ova faza se pokreće kada korisnik koji je primio takvu poštu otvori maliciozni privitak ili Web stranicu. Cilj ove faze je uspješno zaobilaženje obrambenih kontrola i omogućavanje instalacije malicioznog korisnog tereta na računalni sustav korisnika [23].

Branitelj može povećati mogućnost detekcije i obrane u ovoj fazi pravilnom edukacijom zaposlenika, boljim osvješćivanjem o sigurnosti i regularnim penetracijskim testiranjem.

Nakon što je faza eksploatacije završena, maliciozni program se instalira. *Instalacija* (engl. *Installation*) je faza u kojoj se instalira korsni maliciozni teret koji napadaču pruža mogućnosti koje su mu potrebne za daljnje provođenje napada. Zbog velike kompleksnosti današnjih

malicioznih programa, njihova instalacija se odvija u više koraka [23]. Početni maliciozni kod instalira dodatne komponente koje napadaču omogućavaju udaljeni pristup, te osiguravaju trajni pristup u slučaju ponovnog pokretanja računala i sličnih događaja.

U ovoj fazi napadač često ostavlja veliki broj tragova. Postoje razne metode za detekciju i zapisivanje instalacijskih aktivnosti i praćenje kreiranja novih datoteka [25].

Naredba i kontrola (engl. *Command and Control, C2*) je faza u kojoj se uspostavlja komunikacija između C2 poslužitelja kojim upravlja napadač i malicioznih programa koji se nalaze na kompromitiranim računalima [25]. Svrha ove faze je da napadač može konstantno unaprjeđivati maliciozne programe i zadavati im naredbe koje će izvršavati. Postoje 3 glavne strukture C2 poslužitelja: centralizirana, decentralizirana i struktura bazirana na društvenim mrežama [23].

Ovo je posljednja faza za branitelja u kojoj može proći bez ozbiljnih posljedica, jer napadač još nije učinio nikakvu ozbiljniju štetu [25]. Branitelj može detektirati C2 infrastrukturu kroz analizu malicioznog programa te detekcija specifičnih IP adresa ili imena domena [25].

Djelovanje prema cilju (engl. *Actions on objectives*) je faza u kojoj napadači izvode akcije koje vode prema određenom cilju zbog kojeg su i izveli napad na određenu žrtvu [25]. Primjer akcija koje napadač radi u ovoj fazi su: prikupljanje korisničkih vjerodajnica, eskalacija privilegija, prikupljanje i eksfiltracija osjetljivih podataka, uništavanje sustava i narušavanje integriteta podataka [25].

Branitelju je u interesu ovu fazu detektirati čim ranije pomoću forenzičkih alata [25]. Primjeri radnji koje branitelj može izvesti je detekcija eksfiltracije podataka i neautoriziranog korištenja vjerodajnica [25].

3.1.2. Životni ciklus ciljanih kibernetičkih napada

Životni ciklus ciljanih kibernetičkih napada (engl. *Cyber attack lifecycle*) je kao i CKC model izveden iz modela prekidanja lanca, a razvila ga je tvrtka Mandiant. Problem s CKC modelom je da sve radnje prikazuje sekvencijski te je zadnja faza zamišljena za opisivanje velikog broja akcija, tj. prvih 6 faza opisuje upad napadača u organizaciju, a posljednja faza opisuje sve ostale radnje napadača unutar organizacije. U ovom modelu to se rješava tako da se životni ciklus napada prikazuje kroz ciklički pogled, u smislu da se neki dijelovi životnog ciklusa napada mogu ponavljati na različitim metama unutar organizacije koja se napada [28]. Na slici 3.2 nalazi se Mandiant model, sastoji se od 8 faza, a u nastavku će biti detaljnije opisane one faze koje se razlikuju od faza u CKC modelu.

Inicijalno izviđanje (engl. *Initial reconnaissance*) je faza koja odgovara fazi Izviđanja u CKC modelu.

Slika 3.2 Životni ciklus ciljanih napada [29]

Inicijalna kompromitacija (engl. *Initial compromise*) je faza u kojoj napadač dostavlja i pokreće svoj maliciozni kod [30]. Ova faza sadrži dvije faze CKC modela: Dostavu i Eksploataciju.

Uspostava uporišta (engl. *Establish Foothold*) je faza u kojoj napadač uspostavlja trajan udaljeni pristup sustavu koji je kompromitirao [30]. Ova faza odgovara fazi Instalacije u CKC modelu.

Eskalacija privilegija (engl. *Escalate privileges*) je faza u kojoj napadač pokušava dobiti veći pristup sustavu koji je kompromitirao, te podacima koje taj sustav sadržava [30]. Primjer način na koji to može napraviti je pronalazak vjerodajnica na računalu koje je kompromitirao.

Unutarnje izviđanje (engl. *Internal reconnaissance*) je faza u kojoj napadač istražuje okolinu sustava koji je kompromitirao kako bi mogao detektirati lokaciju sustava ili podataka do kojih želi doći [30]. Ovaj korak sličan je i inicijalnom izviđanju, samo napadač mora biti puno oprezniji jer svaka njegova akcija može uzrokovati da obrambene kontrole detektiraju neovlašteno djelovanje i podignu alaram ili da čovjeka zadužen za održavanje kompromitiranog sustava uoči neobične aktivnosti.

Lateralno kretanje (engl. *Move laterally*) je faza u kojoj napadač koristi znanje dobiveno iz prethodne dvije faze kako bi se mogao kretati od sustava do sustava unutar kompromitirane okoline [30]. Česte metode lateralnog kretanja uključuju pristup mrežnim dijeljenim direktorijima (engl. *Network shares*) i korištenje protokola za udaljeni pristup [30].

Održavanje prisutnosti (engl. *Maintain presence*) je faza u kojoj napadač uspostavlja kontinuiran pristup sustavi organizacije koju je kompromitirao [30]. Za razliku od faze uspostave uporišta, u ovoj fazi napadač ne uspostavlja trajan pristup samo na inicijalno kompromitiranom sustavu nego više njih, na kojima su instalirani nepovezani mehanizmi trajnog pristupa, u slučaju ako je neki od tih mehanizama otkriven, drugi će mu omogućiti daljnji pristup.

Izvršavanje misije (engl. *Complete mission*) je faza u kojoj napadač izvršava svoj cilj, a to najčešće uključuje krađu intelektualnog vlasništva, financijskih podataka ili osjetljivih podataka o organizaciji. Nakon što napadač izvrši cilj, tipično zadržava trajan pristup kompromitiranoj organizaciji u slučaju ako će ponovno trebati izvršiti neki cilj koji mu ta organizacija može omogućiti [30].

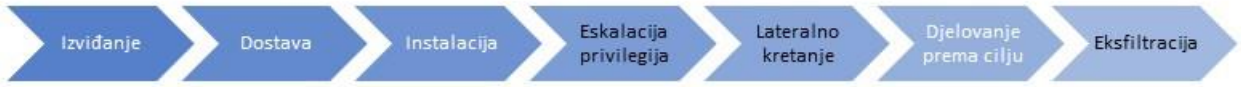
3.1.3. Ostali modeli prekidanja lanca

Postoji još nekoliko modela koji pokušavaju ispraviti nedostatke koje sadrži sam CKC model. U nastavku su ukratko opisani modeli koji na neki način prilagođavaju lanac kako bi se bolje opisalo napadačevo kretanje.

Laliberteov model prekidanja lanca razvio je Marc Laliberte, a sastoji se od 7 faza. Faze su prikazane na slici 3.3. U odnosu na CKC model izbačena je faza naoružavanja, a dodana je faza lateralnog kretanja. Razlog izbacivanja faze naoružavanja je zato što je to faza koju napadača interno provodi te je nešto što branitelj ne može vidjeti i protiv čega ne može djelovati [31]. Razlog za dodavanje faze lateralnog kretanja je ta da napadač u najviše slučajeva prvo kompromitira najranjivije računalo, a zatim lateralnim kretnjama stiže do svog cilja te je to faza koju branitelj može direktno detektirati i spriječiti [31].

Slika 3.3 Laliberteov model prekidanja lanca

Bryantov model prekidanja lanca sastoji se od 8 faza, a prikazan je na slici 3.4. Kao i Lalibertov model, uklanja fazu naoružavanja zato što je ta faza izvan dometa senzora branitelja [32]. Izbacuje fazu eksploatacije jer se to događa kroz faze dostave, instalacije i eskalacije privilegija [32]. Također izbacuje fazu naredbe i kontrole, zato što faze dostave, instalacije, lateralnog kretanja i eksfiltracije sadržavaju podatke o udaljenoj komunikaciji s napadačem [32]. Faza eskalacije privilegija opisuje prijelaz u kojem napadač dobiva pristup privilegiranim korisničkim računima. Faza lateralnog kretanja je uvedena kako bi se razdvojile akcije koje napadač provodi s eksterne mreže od onih koje provodi kada se nalazi unutar mreže organizacije. Faza eksfiltracije je dodana da naglasi mogućnost detekcije anomalnih prijenosa podataka iz interne prema eksternoj mreži [32].



Slika 3.4 Bryantov model prekidanja lanca

Maloneov model prekidanja lanca sastoji se od 3 zasebna lanca. Prvi lanac je nepromijenjeni CKC lanac koji se koristi za opisivanje inicijalnog upada napadača u organizaciju. Drugi lanac koji je prikazan na slici 3.5 naziva se Maloneov interni model i sastoji se od 5 faza, a opisuje kretanje napadača od inicijalne kompromitacije do ciljanog sustava [32]. Zadnji lanac prikazan je na slici 3.6 i naziva se Maloneov model manipulacije, sastoji se od 5 faza, a opisuje radnje koje napadači izvršava na ciljanom sustavu, sve do ostvarivanja svog cilja [32].

Slika 3.5 Maloneov interni model

Slika 3.6 Maloneov model manipulacije

Dodatno u [32] je predložen model koji objedinjuje ATT&CK model koji je opisan u sljedećem potpoglavlju i sve gore navedene modele, a sastoji se od 16 faza. Također postoji i model genomike prijetnji (engl. *Threat genomics*) koji pokušava pomoću tehnika iz sekvenciranja

genoma detektirati i predvidjeti napade. Model se sastoji od 10 faza, a više o modelu može se naći u [33].

3.2. ATT&CK

ATT&CK (*Adversarial Tactics, Techniques & Common Knowledge*) je baza znanja i klasifikacija napadačkih taktika i tehnika koje se baziraju na zapažanjima iz stvarnog svijeta. Bazu je izgradila MITRE organizacije 2013. godine, a u javnosti je dostupna od 2015 [34]. Glavna karakteristika ATT&CK modela je da se zasniva na promatranju ponašanja napadača (interakcije napadača sa sustavom) umjesto na pojedinim indikatorima kompromitacije koje napadač može jednostavno promijeniti. Cilj modela je bolja i jednostavnija karakterizacija napadačeva ponašanja te korištenje za potrebe emulacije ponašanja napadača.

ATT&CK se sastoji od tri modula: PRE-ATT&CK, ATT&CK za poduzeća i ATT&CK za mobilne platforme [34]. U ovoj cjelini biti će opisana prva dva modula jer se primarno fokusira na napredne ustrajne prijetnje, dok se ATT&CK za mobilne platforme fokusira na napadače raznih vještina i mogućnosti. Svaki od ta dva modula pokriva jedan dio CKC modela i detaljnije ga razrađuje te je opisan svojim taktikama i tehnikama. Taktike objašnjavaju taktičke ciljeve napadač tijekom napada, dok tehnike objašnjavaju akcije koje napadač izvodi kako bi izvršio svoj taktički cilj. Svaka tehnika je dodatno osim iz perspektive napadača, opisana i iz perspektive branitelja, tj. kako branitelj može detektirati ili braniti se protiv te tehnike. Pošto su tehnike uzimane iz primjera iz stvarnog svijeta, svaka tehnika sadržava i reference na materijale od kud je tehnika uzeta te koji su napadači koristili te tehnike. Dijelovi CKC koji pokrivaju PRE-ATT&CK i ATT&CK za poduzeća nalazi se na slici 3.7. Potrebno je napomenuti da opis taktika u ATT&CK modelu nije sekvencijski, npr. taktika naredbe i kontrole je opisana posljednja, iako je u većini slučajeva potrebna za izvršavanje ranijih taktika [32]. Da bi se uspješno mapirale taktike na CKC model potrebno je dodati vremensku komponentu [32].

Slika 3.7 Dijelovi CKC modela koje pokrivaju PRE-ATT&CK i ATT&CK

ATT&CK za poduzeća (engl. *ATT&CK for Enterprise*) je prvi modul koji je napravljen i na temelju kojeg je nastala cijela ideja ATT&CK modela. Fokus modula je na operacijske sustave Windows, Linux i macOS. Cilj tog modula je poboljšati razumijevanje napadačevog djelovanja nakon inicijalne kompromitacije sustava. ATT&CK za poduzeća se dijeli na 11 taktika [34]:

- *Inicijalni pristup* je taktika koja opisuje vektore napada koje napadač koristi kako bi dobio početni pristup na mreži koju napada.
- *Izvođenje* je skup tehnika koje služe za izvođenje napadačevog koda na lokalnom ili udaljenom sustavu.
- *Ustrajnost* je bilo koja akcija koja napadaču daje dugotrajan pristup sustavu koji napada.
- *Eskalacija privilegija* je tehnika koja omogućava napadača da dobije veće privilegije na sustavu ili mreži.
- *Zaobilaženje zaštitnih mjera* je skup tehnika koje služe napadaču kako bi mogao proći nedetektiran.
- *Dohvat vjerodajnica* je taktika koja rezultira pristupom ili potpunom kontrolom napadača nad sustavom, servisom ili domenom.
- *Otkrivanje* je taktika koja omogućuje napadaču stjecanje znanje o sustavu ili internoj mreži na kojoj se trenutno nalazi.
- *Lateralna kretnja* je skup tehnika koje služe napadaču da dobije pristup i kontrolu nad udaljenim sustavom u mreži.
- *Prikupljanje sadrži* tehnike koje govore kako napadač prikuplja informacije sa sustava na kojima se nalazi.
- *Eksfiltracija* je skup tehnika koje objašnjavaju kako napadač seli prikupljene informacije s braniteljske mreže, na lokaciju koju on želi.
- *Naredbe i kontrola* su skup tehnika koje objašnjavaju kako napadač komunicira sa sustavima koji su u njegovom vlasništvu.

PRE-ATT&CK modul se sastoji od taktika i tehnika koje opisuju napadačevo ponašanje prije kompromitacije, tj. kako napadač bira žrtvu, kako prikuplja informacije, gradi infrastrukturu i kako pokreće napad. Te aktivnosti su većinom izvan dometa organizacija koje se brane pa ih je teško detektirati i braniti se protiv njih. Cilj ovog modula je poboljšati obranu i detektirati maliciozne radnje i prije nego napadači uspiju dobiti pristup sustavu. PRE-ATT&CK može pomoći braniteljima s pitanjima kao što su: da li netko cilja moju organizaciju i koje tehnike napadači često koriste u svrhu napada na organizacije kao što je moja. Modul se sastoji od 15 taktika i 151 tehnike, koje branitelju mogu pomoći da donese bolje informirane odluke kako poboljšati tehničke i političke mjere prevencije. Taktike koje se nalaze u PRE-ATT&CK modulu su [34]:

- Definiranje prioriteta:
    - Planiranje
    - Smjer
- Biranje žrtve

- Prikupljanje informacija:
    - Tehničkih
    - O ljudima
    - O organizaciji
- Identifikacija slabosti:
    - Tehničkih
    - O ljudima
    - O organizaciji
- Napadačka operacijska sigurnost
- Uspostava i održavanje infrastrukture
- Izgradnja ličnosti
- Izgradnja mogućnosti
- Testiranje mogućnosti
- Pokretanje mogućnosti

Korisno je i spomenuti da oba gore navedena modula sadržavaju i informacije o poznatim naprednim ustrajnim prijetnjama. U tim opisima se nalaze pseudonimi koji opisuju kako su razne organizacije nazivale grupu, te koje tehnike koriste i pripadne alate.

3.3. Dijamantni model

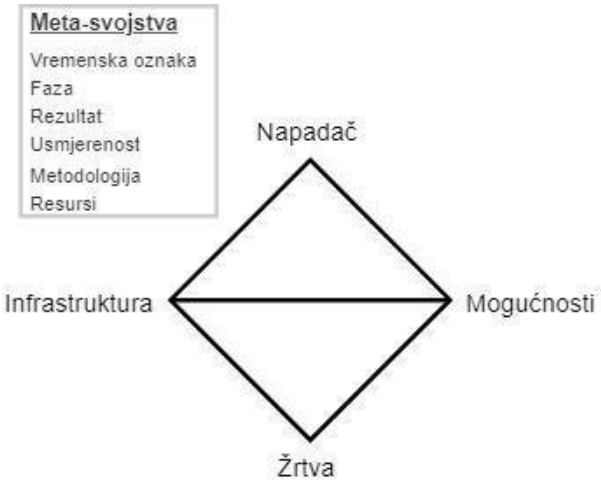
Dijamantni model (engl. *Diamond model*) je analitička metodologija za analizu napada razvijena 2006. godine [35]. Svrha modela je na sistematičan način pomoći u praćenju, detektiranju i grupiranju napadača i njihovih radnji te omogućiti lakši način za otkrivanje potrebnih protumjera u svrhu zaštite od tih napadača [35]. Model se razlikuje od prethodno opisanih modela koji su izvedenice modela prekidanja lanca. Pogodnosti koje model pruža su [35]:

- omogućava bolju kontekstualnu i relacijsku povezanost između indikatora kompromitacije u svrhu povećanja korisnosti tih indikatora,
- omogućuje bolju korelaciju između različitih napada pomoću grafova aktivnosti napada,
- Jednostavna integracija s drugim radnim okvirima za planiranje obrambenih strategija,
- omogućava jednostavnije detektiranje nedostataka u postojećim obavještajnim informacijama,
- karakterizaciju događaja u stvarnom vremenu pomoću korištenja klasifikacija i metoda za detekciju upada,
- uspostavlja podlogu za ontologije kibernetičkih aktivnosti, taksonomije, dijeljenje obavještajnih informacija o kibernetičkim prijetnjama i za bolje i efikasnije upravljanje znanjem.

3.3.1. Osnovni model

Najmanja opisna jedinica u Diamond modelu je *događaj* (engl. *Event*). Događaj se sastoji od 4 svojstva koji predstavljaju vrhove: napadač, mogućnosti (napadača), infrastruktura (napadača) i žrtva [36]. Vrhovi su povezani vezama koje opisuju njihov odnos u uzročno-posljedičnom smislu. Ideja modela je da opisuje napadača sa svojim mogućnostima koji preko infrastrukture napada žrtvu u svrhu postizanja svojih ciljeva [36].

Osim primarnih svojstava postoje i dodatna meta-svojstva koja omogućavaju da se događaji povezuju u smislene aktivnosti nazvane *dretve aktivnosti* (engl. *Threat activity*) [36]. Događaji se mogu povezivati u različite dretve aktivnosti zavisno o potrebama branitelja. Meta-svojstva su: vremenska oznaka (početak i kraj), faza, rezultat, smjer, metodologija i resursi. Na slici 3.8 nalazi se dijamanti model s meta-svojstvima, a u nastavku je svako primarno svojstvo i meta svojstvo detaljnije opisano.



Slika 3.8 Dijamantni model [36]

Napadač je svojstvo koje opisuje pojedinca ili organizaciju koja koristi svoje mogućnosti u svrhu ostvarivanja cilja [36]. Svojstvo napadača je u većini slučajeva najteže ispuniti, pogotovo u vrijeme same detekcije napada. Svojstvo napadača sastoji se od dva podsvojstva [36]:

- *Operator napada* koji se upotrebljava kada se opisuju tehnički aspekti napadača. U to spada osoba koja direktno provodi napad.
- *Korisnik napada* opisuje entitet koji će na neki način profitirati iz napada. To može biti i sam operator napada ili neki drugi pojedinac/grupa koji je naredio operatoru napada da izvede taj napad. Pomoću ovog svojstva opisuju se strateški ciljevi napadača.

Svojstvo mogućnosti opisuje tehnike i alate koje napadač koristi prilikom izvođenja pojedinog događaja [36]. Svojstvo je korisno za katalogizaciju tehnika i alata napadača u svrhu lakše detekcije i prevencije istih.

Infrastruktura je sva fizička ili logička komunikacijska struktura koja služi za obavljanje i održavanje napadačevih mogućnosti [36]. Primjeri su IP adrese, imena domena, USB uređaji, itd. Postoje 3 vrste infrastrukture [36]:

- Tip 1 je infrastruktura u potpunosti pod kontrolom napadača.
- Tip 2 je infrastruktura koja je posrednik u napadu, a žrtva ju vidi kao napadača. To su računalni sustavi koji služe da prikriju pravi identitet napadača, a prikupljeni su tako da ih je napadač prethodno kompromitirao, primjeri su zombi računala, maliciozne domene i kompromitirani računi elektroničke pošte
- Pružatelj usluga je infrastruktura koja pruža usluge koji su neophodni kako bi Tip 1 i Tip 2 infrastruktura rade ispravno. Primjeri te infrastrukture su ISP-ovi, registratori domena te poslužitelji elektroničke pošte.

Žrtva je entitet koji napadač napada sa svojim mogućnostima preko infrastrukture. Iako žrtva može biti opisana na bilo koji način, postoji separacija na žrtvinu ličnost i žrtvinu imovinu [36].

- *Žrtvina ličnost* je organizacija ili pojedinci ili grupe unutar organizacije koju napadač napada preko imovine. Žrtvina ličnost se koristi u *cyber-victimology* ili društveno-političkim analizama.
- Žrtvina imovina je napadačka površina koju napadač eksploatira da bi izvršio svoje radnje. U tu skupinu spadaju računalne mreže i sustavi, elektronička pošta, IP adrese, računi društvenih mreža, itd.

U nastavku su opisana osnovna meta-svojstva preporučena za korištenje u dijamantnom modelu uz bitnu napomenu da se meta-svojstva mogu dodavati proizvoljno po potrebi branitelja.

Vremenska oznaka služi za precizno opisivanje nekog događaja, ili opisivanja intervala u kojem se taj događaj dogodio. Vremensko označavanje događaja može biti korisno za dobivanje jasnije slike o načinu rada napadača.

Svaka složenija maliciozna radnja sastoji se od više koraka (minimalno dvije faze: određivanje žrtve i izvođenja napada). Da bi se cijela maliciozna radnja mogla opisati pomoću dijamantnog modela, svaki događaj predstavlja jednu *fazu*, a događaji se ulančavaju da se dobije smislena priča o napadu. Za razliku od CKC, dijamantni model nije ograničen na broj faza te se one mogu proizvoljno dodavati, ovisno o potrebama branitelja.

Rezultat napadačevih akcija nam daje podatake o uspješnosti napadača i posljedicama njegovih radnji. To svojstvo je korisno kada se želi proučavati uspješnost napadača s pojedinim mogućnostima i protiv pojedinih vrsta obrana, te također može dati uvid u napadačevu namjeru.

Usmjerenost događaja je korisno svojstvo kada se proučavaju mogući mrežni i računalni načini obrane protiv napadača. Korištenjem tih informacija preko više događaja može se donijeti bolja odluka gdje postaviti preventivne i detekcijske mjere.

Metodologija je meta-svojstvo koje omogućava analitičaru kategoriziranje aktivnosti događaja bez ulaska u detalje, a također omogućuva da se događaj kategorizira u više skupina. Primjer metodologije je slanje poruka elektroničke pošte s malicioznim privitkom.

Resurs je meta-svojstvo koje opisuje koji su sve resursi potrebni da bi se događaj mogao uspješno izvršiti. Primjeri resursa su programski alati (npr. Metasploit) koje napadač treba da bi izvršavao napad, znanje koje napadač treba imati (kako raditi s Metasploitom), financije (npr. za kupnju malicioznih programa), itd.

Izuzev vizualnog prikaza, dijamantni model se može zapisati i kao više dimenzionalno polje koje je korisno za dijeljenje i obradu informacija na računalu [36]:

Događaj = {{Napadač, Pouzdanost},
{Mogućnosti, Pouzdanost},
{Infrastruktura, Pouzdanost},
{Žrtva, Pouzdanost},
{Vremenska oznaka početka, Pouzdanost},
{Vremenska oznaka kraja, Pouzdanost},
{Faza, Pouzdanost},
{Rezultat, Pouzdanost},
{Usmjerenost, Pouzdanost},
{Metodologija, Pouzdanost},
{Resursi, Pouzdanost}}

Za razliku od grafičkog modela u ovakvom zapisu dodan je i pojam pouzdanosti, koji opisuje sigurnost analitičara u tu tvrdnju. Ovakvim načinom lako se uočavaju nedostaci prilikom izrade modela i lako se mogu uočiti svojstva koja nedostaju. Model je zamišljen da bude proširiv te se svakom od osnovnih ili meta svojstava mogu dodati i podsvojstva [36]. Slijedi primjer kako dodati dodatna podsvojstva svojstvu žrtva [36]:

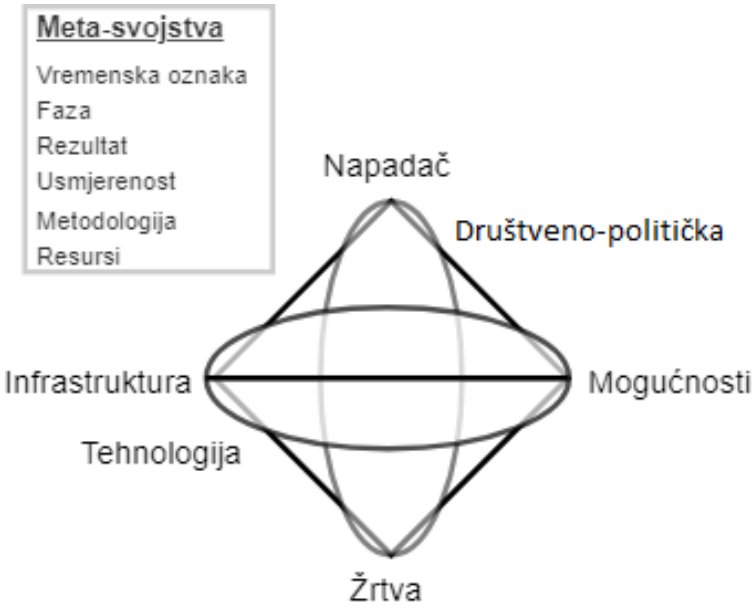
{Žrtva, Pouzdanost} = {{Organizacija, Pouzdanost},
{IP adresa računala, Pouzdanost},
{Ime računala, Pouzdanost},
{Aplikacija, Pouzdanost},
{TCP pristupna točka, Pouzdanost}}

3.3.2. Prošireni model

Prošireni dijamantni model uvodi dvije dodatne komponente u dijamanti model, društveno-političku komponentu koja povezuje napadača i branitelja, te tehnološku komponenta koja povezuje infrastrukturu i mogućnosti [36]. Na slici 3.9 je prikazan prošireni dijamantni model.

Društveno-politička komponenta opisuje vezu između napadača i branitelja, koja uvijek postoji bez obzira koliko bila indirektna ili nestalna. Društveno-politička komponenta je opisana pomoću odnosa proizvođača i potrošača, u kojem je napadač potrošač koji pokušava zadovoljiti svoje potrebe (financijski prihod, status u hakerskoj zajednici, itd.), a branitelj proizvođač koji nesvojevoljno pruža produkt (računalne resurse, financijske podatke, itd.) [36]. Veza između potreba napadača i mogućnosti žrtve da zadovolji te potrebe se naziva *napadačeva namjera*. Komponenta opisuje zašto je žrtva izabrana, koliku vrijednosti donosi napadaču, postoje li slične žrtve, koje bi mogle biti dodatne do sad nepoznate žrtve, otkrivanje namjera napadača, te kako se tom informacijom može upravljati da se omogući bolja obrana.

Tehnologija je komponenta dijamantnog modela koja objašnjava kako su mogućnosti i infrastruktura napadača međusobno povezane [36]. Primjer korištenja tehnološke komponente je maliciozni program koji komunicira preko HTTP protokola i koristi DNS protokol za razrješavanje imena upravljačkog poslužitelja (engl. *Command and control*, C2), tada su tehnologije koje se koriste protokoli IP, TCP, HTTP i DNS. Pregledom te komponente može se utvrditi koje tehnologije je napadač koristio bez obzira na pojedinu tehniku ili alat [36].



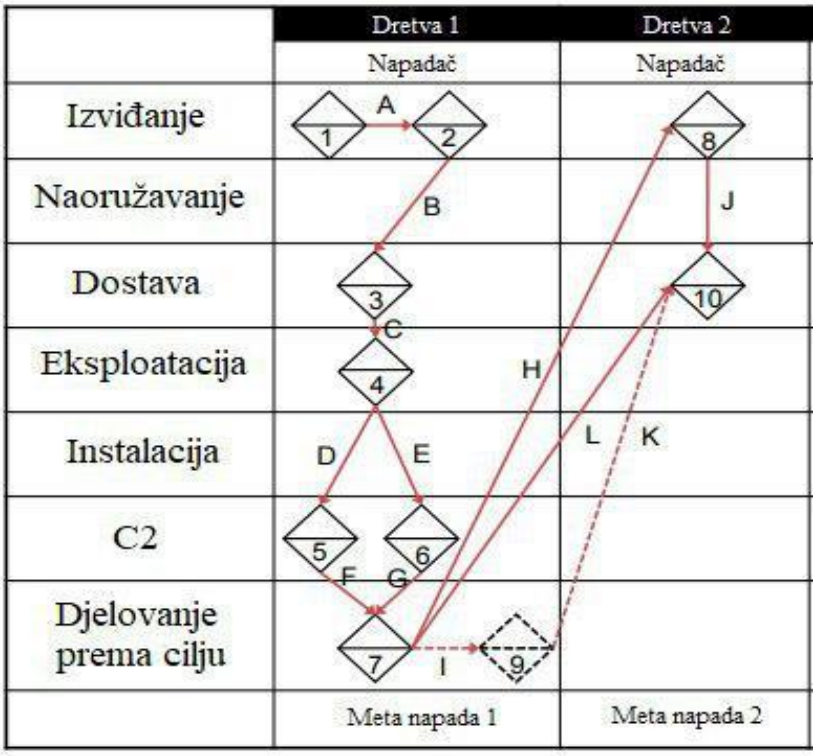
Slika 3.9 Prošireni dijamantni model [36]

3.3.3. Dretve aktivnosti

Kao što je već i ranije rečeno događaji opisuju samo jedan korak u interakciji napadača i branitelja, povezivanjem više događaja u niz dobiva se *dretva aktivnosti* (engl. *Activity thread*). *Dretva aktivnosti* je usmjereni graf u kojem svaki vrh predstavlja događaj, a veze predstavljaju relacije između pojedinih događaja [36]. Svaka veza je okrakterizirana s više svojstava:

pouzdanost analitičara, je li put nužan (AND) ili opcionalan (OR - postoji više mogućih puteva od događaja), je li događaj stvaran ili je samo hipoteza, te koje informacije i resurse prethodno izvedeni događaj pruža sljedećem događaju da bi se on uspješno izvršio [36]. Svaka dretva aktivnosti opisuje jedan par napadača i branitelja. Dretve aktivnosti su korisne zbog činjenice da jednom kada su završene mogu poslužiti za koreliranje različitih napada, sa svrhom da se otkriju maliciozne kampanje ili da se u skupini napada uoče sličnosti radi lakše obrane ili pripisivanja više napada jednoj grupi.

Na slici 3.10 prikazane su dvije dretve aktivnosti koje su međusobno povezane, a događaji su preslikani na pojedine faze CKC modela. Napadač prvo napada metu 1 (u nastavku MD1), te nakon uspješne kompromitacije koristi adresu elektroničke pošte kompromitiranog računala za slanje malicioznih poruka elektroničke pošte na metu 2 (u nastavku MD2). Može se vidjeti da se izuzev vertikalnog koreliranja, može raditi i horizontalno koreliranje u svrhu identifikacije istih ili sličnih radnji unutar više napada. Potrebno je naglasiti da su događaji i veze koji su prikazani isprekidanim linijama hipotetske, tj. pretpostavljene od strane analitičara. U tablici 3.1 dan je detaljniji opis događaja sa slike 15, a u tablici se nalaze podaci o broju događaja, da li je događaj stvaran ili hipoteza, te opis događaja. U tablici 3.2 dan je detaljniji opis veza između pojedinih događaja sa slike 15. Tablica se sastoji od identifikatora veze, pouzdanosti analitičara, da li je veza obavezna ili opcionalna, da li je veza stvarna ili hipoteza analitičara te koje informacije i resurse prethodni događaj pruža sljedećem da bi se on uspješno izvršio.



Slika 3.10 Dretve aktivnosti dijamantnog modela [36]

Tablica 3.1 Opis događaja u dretvi aktivnosti [36]

Događaj	Hipoteza/stvarno	Opis
1	Stvarno	Napadač provodi Internetsko pretraživanje podataka o MD1 te kao dio rezultata dobiva imena domena koja pripadaju MD1
2	Stvarno	Napadač koristi otkrivena imena domena za daljnje istraživanje i pronalazi podatke o mrežnim administratorima MD1
3	Stvarno	Napadač šalje malicioznu poruku elektične pošte mrežnim administratorima MD1
4	Stvarno	Jedan mrežni administrator otvara malicioznu poruku i omogućava izvršavanje malicioznog koda
5	Stvarno	Maliciozni kod pokrenut na računalu mrežnog administrator šalje HTTP zahtjev primarnom C2 poslužitelju i natrag dobiva HTTP odgovor
6	Stvarno	Analizom malicioznog koda utvrđeno je da maliciozni kod ima zabilježen i rezervni C2 poslužitelj, ukoliko je primarni C2 poslužitelj nedostupan
7	Stvarno	Nakon uspješno primljenog HTTP odgovora, maliciozni kod otvara napadaču TCP konekciju te mu daje pristup ljusci operacijskog sustava
8	Stvarno	Kroz ljusku napadač pretražuje na kompromitiranom računalo podatke o poslovnim partnerima i pronalazi podatke o MD2
9	Hipoteza	Napadač traži na kompromitiranom računalu adrese elektroničke pošte od MD2 i pronalazi adresu elektroničke pošte direktora MD2
10	Stvarno	Napadač šalje malicioznu poruku elektroničke pošte direktoru MD2 kroz adresu elektroničke pošte administratora čije je računalo kompromitirano

Tablica 3.2 Opis veza u dretvi aktivnosti [36]

Veza	Pouzdanost	I/ILI	Hipoteza/Stvarno	Pruža
A	Niska	I	Stvarno	Pruža imena domena od MD1
B	Visoka	I	Stvarno	Pruža mete za napad s malicioznom elektroničkom porukom
C	Visoka	I	Stvarno	Ništa
D	Visoka	ILI	Stvarno	Ništa
E	Visoka	ILI	Stvarno	Ništa
F	Visoka	I	Stvarno	Ništa
G	Visoka	I	Stvarno	Ništa
H	Srednja	I	Stvarno	Pruža pristup Interntskom pretraživaču kompromitiranog računala
I	Niska	I	Hipoteza	Pruža pristup adresama elektroničke poruke na kompromitiranom računalu
J	Visoka	I	Stvarno	Pruža identifikaciju MD2
K	Niska	I	Hipoteza	Pruža identifikaciju adresa elektroniče pošte od MD2
L	Visoka	I	Stvarno	Pruža mogućnost napada malicioznom porukom elektroničke pošte na MD2

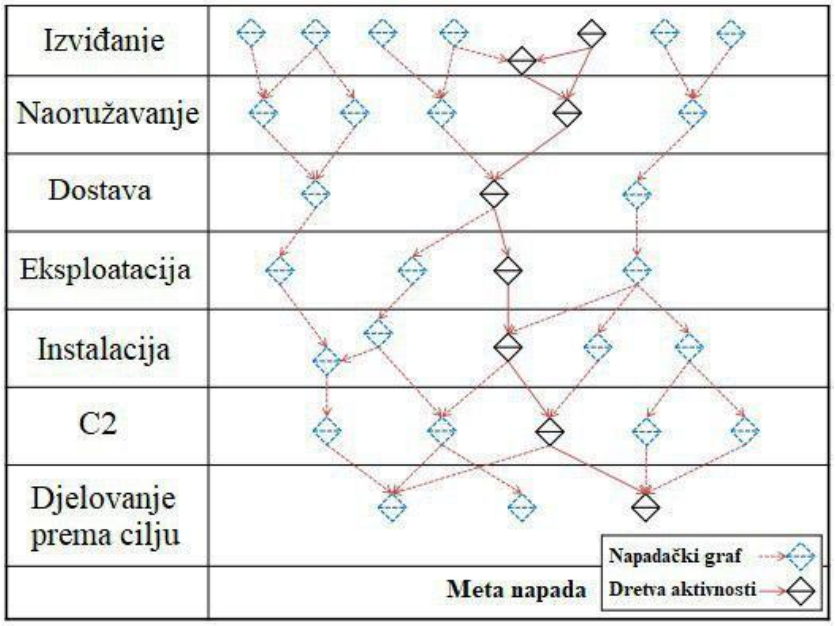
3.3.4. Grafovi aktivnosti napada

Kombinacijom napadačkih grafova i dretvi aktivnosti dobiju se *grafovi aktivnosti napada* (engl. *Activity-attack graph*). Grafovi napada bit će detaljnije objašnjeni u sljedećem potpoglavlju, ali

ukratko, oni opisuju sve potencijalne puteva koje napadač može iskoristiti za ostvarenje cilja, a dretva aktivnosti opisuje put koji je napadač zaista ostvario. Slika 3.11 prikazuje kako se dretva aktivnosti može kombinirati s napadačkim grafom.

Prednosti kombiniranja napadačkih grafova i dretva aktivnosti su [36]:

- Dretva aktivnosti povećava količinu informacija dostupnih u napadačkom grafu, pošto svaki čvor u grafu predstavlja jedan događaj u dijamantnom modelu.
- Spajanjem dretva aktivnosti s napadačkim grafovima ne gubi se integritet grafova, te sve metode razvijene za analizu grafova mogu i mogu koristiti.
- Omogućuje preciznije određivanje težina pojedinih veza, pošto je poznato više informacija o izborima (alternativama) koje napadač ima na raspolaganju.
- Naglašavaju se napadačeve preference u odnosu na ostale alternativne puteve.
- Omogućava bolje nadopunjavanje znanja jer je omogućeno horizontalno koreliranje. Rezultat toga je preciznije i brže generiranje i testiranje hipoteza za napade koji su u tijeku.



Slika 3.11 Primjer kombiniranja dretve aktivnosti i grafa napada [36]

3.3.5. Grupe aktivnosti

Grupa aktivnosti je skup događaja i dretvi aktivnosti koje su povezane nekom mjerom sličnosti u njihovim svojstvima, ovisno o potrebama branitelja [36]. Svrha grupa aktivnosti je sažeti znanje o aktivnostima napadača i omogućiti bolje planiranje obrambenih strategija koje nisu vezane samo uz jednu dretvu aktivnosti. Grupe aktivnosti primarno se stvaraju radi uočavanja

sličnosti između različitih napada (najčešće između različitih dretva aktivnosti), obično povezivanjem sličnosti između infrastrukture i mogućnosti. Razlika između grupa i dretvi je da se grupe formiraju na temelju sličnosti, dok se dretve stvaraju kauzalnim vezama između događaja.

Grupe aktivnosti formiraju se upotrebom sljedećih 6 koraka [36]:

1. *Analitički problem* označava korak u kojem se definira specifičan problem koji se namjerava riješiti kreiranjem grupa aktivnosti.
2. *Odabir svojstava* je korak koji označava odabir svojstava i procesa napadača po kojem će se izvršavati grupiranje i klasifikacija.
3. *Kreiranje* je korak u kojem se kreiraju grupe aktivnosti iz skupa odabranih događaja i dretva aktivnosti.
4. *Rast* je korak u kojem se novi događaji i dretve aktivnosti dodaju u trenutno definirane grupe aktivnosti. Izrada grupa aktivnosti je kontinuirani proces.
5. *Analiza* je korak u kojem se kreirane grupe analiziraju u svrhu rješavanja problema koji je definiran u prvom koraku.
6. *Redefiniranje* je korak u kojem se grupe aktivnosti redefiniraju s vremenom da bi održale svoju točnost. Razlog redefiniranja može biti neka pogrešna pretpostavka u inicijalnom planiranju grupa aktivnosti.

3.4. Stabla napada

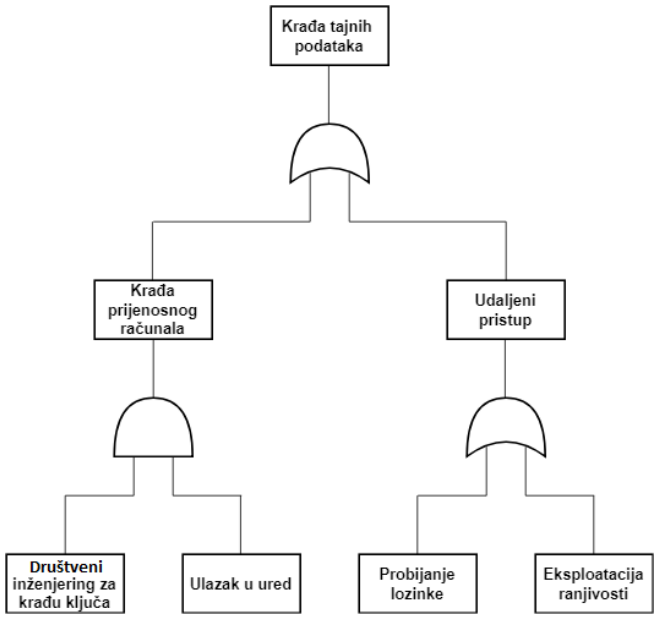
Stabla napada (engl. *Attack trees*) su grafički i matematički modeli koji pružaju formalni i metodički način za opisivanje sigurnosti sustava na temelju različitih napada [37]. Stabla napada prvi puta spominje 1994. godine Edward Amoroso, a popularizirao ih je Bruce Schneier objavom u radu iz 1999. godine [38]. Osnovna ideja napadačkih stabala je predstavljanje napada na sustav u obliku stabla, gdje je glavni cilj napadača predstavljen kao korijen stabla, a ostatak stabla opisuje različite načine na koje napadač može ostvariti cilj. Cilj stabla je na strukturirani i fleksibilan način predstaviti sve moguće napade koji se mogu dogoditi na korijenu stabla.

Stabla napada koriste se za [39]:

- Identifikaciju potencijalnih malicioznih radnji koje predstavljaju najveći rizik branitelju.
- Za određivanje efektivnih strategija za smanjenje rizika na zadovoljavajuću razinu.
- Opisivanje potencijalne interakcije napadača i branitelja.
- Pruža efikasan i efektivan alat za komunikaciju između sigurnosnih inženjera i analitičara.
- Omogućuje efikasno spremanje informacija o sustavu i napadačima, te omogućuje generiranje i testiranje hipoteza.

Zbog navedenih kvaliteta stabla napada primjenjiva su na sigurnosne probleme u širokom spektru područja, kao što su: telekomunikacije, kritična infrastruktura, financije, obavještajne i obrambene agencije [39].

Pojmove vezane uz stabla napada najlakše je objasniti na konkretnom primjeru. Na slici 3.12 prikazano je stablo napada koje opisuje krađu tajnih podataka. Svako stablo napada sastoji se od korijena stabla, čvorova i veza između njih. Korijen stabla je poseban čvor jer on opisuje krajnji cilj napadača, u ovom slučaju to je krađa tajnih podataka. Ostali čvorovi dijele su u dvije podskupine, listovi i srednji čvorovi. Listovi predstavljaju akcije koje napadač može izvesti, a srednji čvorovi prikazuju napadačeve podciljeve [40]. Listovi čvorova na slici 3.12 su društveni inženjering za dobivanje ključa, ulazak u ured, probijanje lozinke i eksploatacija ranjivosti. Srednji sloj koji je prikazan na slici su krađa prijenosnih računala i udaljeni pristup. Slično kao i kod modela prekidanja lanca cilj je zaustaviti napadača što ranije, tj. što bliže listovima.



Slika 3.12 Stablo napada za krađu tajnih podataka [41]

Veza između čvora i njegove djece može biti konjunktivna ili disjunktivna, to znači da neki čvorovi zahtijevaju da sva njegova djeca budu ostvarena, dok je za neke čvorove dovoljno da samo jedno dijete bude uspješno ostvareno. Potrebno je naglasiti da se to ne odnosi na listove, pošto oni nemaju djece. U primjeru sa slike 3.12 podcilj *krađa prijenosnog računala* ima konjunktivnu vezu sa svojom djecom, tj. oba djeteta moraju biti uspješno izvršena. To znači da napadač mora izvesti društveni inženjering da bi dobio ključ od ureda i ući u ured da bi uspješno ukrao prijenosno računalo. Podcilj *udaljeni pristup* ima disjunktivnu vezu sa svojom djecom, a to znači da napadač mora ili uspješno probiti lozinku ili eksploatirati ranjivost ili oboje da bi uspješno dobio udaljeni pristup. Krajnji cilj *krađa tajnih podataka* ima također disjunktivnu

vezu sa svojom djecom te prema tome napadač mora ili ukrasti prijenosno računalo ili dobiti udaljeni pristup da bi uspješno ukrao podatke.

Opisano stablo napada je najosnovniji primjer istog. Postoje razne mogućnosti proširenja stabla tako da se listovima pridijele binarne ili kontinuirane vrijednosti koje se dalje propagiraju kroz stablo [37]. Primjer toga je da se svakom listu pridijeli novčana ili vremenska vrijednost koja označava koliko će napadač morati resursa utrošiti da uspješno izvede taj napad. Naravno da bi tako nešto bilo moguće, prethodno je potrebno jasno definirati karakteristike napadača za kojeg se stablo promatra. Za primjer na slici 3.12, ako se promatra neki napadač početnik, onda su vrlo vjerojatno jedine prijetnje probijanje lozinke i u nešto manjoj mjeri eksploatacija ranjivosti. Međutim, ako se u obzir uzimaju organizirane kriminalne skupine, onda su opcije kao društveni inženjering i krađa prijenosnih računala lako moguće opcije uz probijanje lozinki i eksploataciju ranjivosti.

Također, dodatno poboljšanje modela stabla napada koji se može uzeti u obzir je i reakcija branitelja na određene akcije napadača. To može biti korisno za odlučivanje o određenim obrambenim mehanizmima koji se mogu postaviti na putu da se napadaču onemogući taj put ili da mu taj put postane pretežak ili preskup, ovisno o njegovim motivima, željama i karakteristikama.

Nakon definicije napadačkih stabala potrebno je naglasiti pozitivne strane zbog koji se koriste [42]:

- Fleksibilnost napadačkih stabala omogućava da se radi na bilo kojoj razini apstrakcije. Svaki čvor može prikazivati vrlo specifični tehnički aspekt sustava ili može predstavljati cijelu organizaciju.
- Vizualnost napadačkih stabala omogućuje lakšu prezentaciju netehničkom osoblju.
- Formalizam napadačkih stabala omogućava da se stabla jednostavno matematički opišu za korištenje u automatiziranim alatima. Također formalizam omogućava da se algoritmi korišteni u teoriji grafova mogu primjenjivati i na stablima napada.
- Omogućavaju lakše rasuđivanje o mehanizmima obrane.
- Stabla napada pogodna su kao podloga za razna istraživanja, te su kombinirana s raznim metodologijama kao što su Markovljevi lanci [43] i teorija igara [44].

Glavni problem napadačkih stabala je njihova skalabilnost na velike sustave, no postoji velika količina istraživanja koja pokušava riješiti navedeni problem [45].

3.5. Petrijeve mreže

Primjena *Petrijevih mreža* je alternativna stablima napada. Najvažnije karakteristike Petrijevih mreža su [46]:

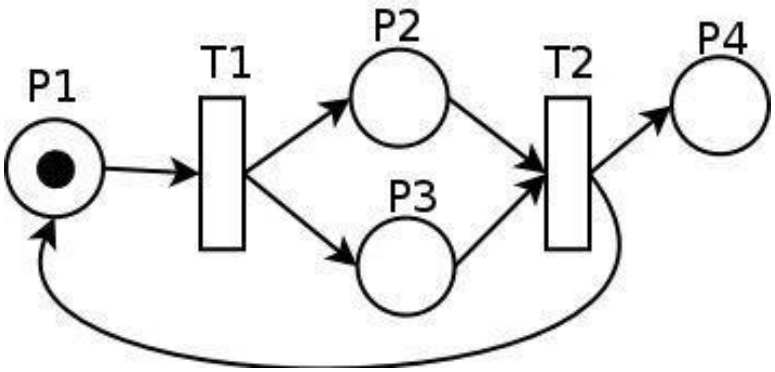
- omogućuju prikaz istodobnih i koordiniranih napada na sustav ili organizaciju,
- jednostavan prikaz međustanja napadača,
- modeliranje akcija napadača pomoću prijelaza,
- jednostavno i fleksibilno razmatranje različitih scenarija koji se mogu dogoditi.

Koordinirani napadi su napadi više malicioznih aktora koji svi zajedno djeluju prema zajedničkom cilju [47]. Važna značajka koordiniranih napada je da akcije jednog aktora mogu utjecati na akcije drugog. Problem napadačkih stabala je nedostatak prikaza više napadača na jednom grafu [47]. Da bi se taj problem mogao riješiti na stablima napada, potrebno je prikazati sve napadače kao jednog ili je potrebno modelirati za svakog napadača zasebno stablo napada. Petrijeve mreže inicijalno su razvijene kako bi se mogli opisitvati konkurentni asinkroni procesi [47].

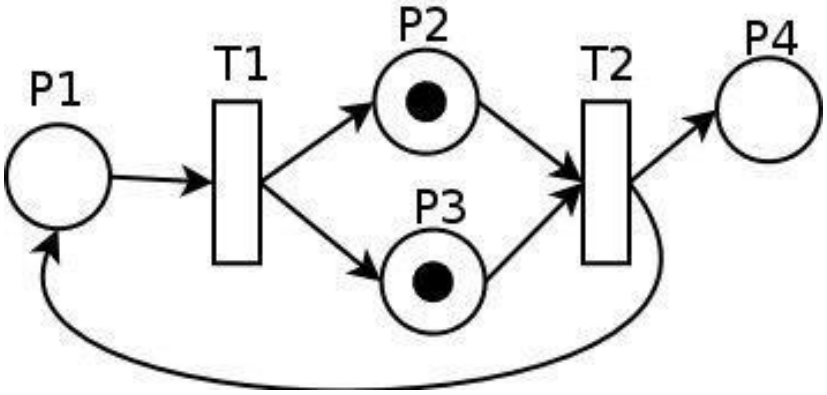
Petrijeve mreže najlakše je objasniti uz pomoć slike. Na slici 3.13 nalazi se primjer Petrijeve mreže. Petrijeva mreža je usmjereni graf koji se sastoji od stanja (kruzici), prijelaza (pravokunitici), usmjerenih veza između stanja i znački koje putuju kroz mrežu. Stanja na slici označena s P1, P2, P3 i P4 predstavljaju različita stanja sigurnosti sustava. Prijelazi označeni s T1 i T2 prikazuju moguće akcije napadača. Prijelazi se sastoje od ulaznih stanja i izlaznih stanja. Ulazna stanja mogu se promatrati kao preduvjeti koji moraju biti zadovoljeni da bi se prijelaz ostvari, a izlazna stanja kao posljedice prijelaza. Temeljni pojmovi vezani uz prijelaze su omogućavanje (engl. *enable*) i ispaljivanje (engl. *fire*). Značke koje su na slici prikazane crnim kružićima unutar stanja označavaju jesu li odgovarajući preduvjeti zadovoljeni i predstavljaju napadače, tj. jedna značka predstavlja jednog napadača. Prijelaz je omogućen ako svako ulazno stanje sadrži barem jednu značku. Nakon toga prijelaz je omogućen te može ispaliti značke u izlazna stanja. Na slici 3.13 T1 prijelaz je omogućen jer sva ulazna stanja, a to je u ovom slučaju samo P1, sadrži barem jednu značku i to znači da su za tu akciju svi preduvjeti ispunjeni. Potrebno je napomenuti da će nakon ispaljivanja prijelaza T1, značka nestati u P1, a nove značke će se pojaviti u P2 i P3 stanjima. Prijelaz T2 nije omogućen zato što stanje P2 i P3 ne sadrže niti jednu značku, a to znači da taj preduvjet nije ispunjen. U svrhu modeliranja napadača to znači da je napadač uspješno kompromitirao računalni sustav P1, ali ne P2 i P3. Da bi se uspješno modelirao veći broj napadača potrebno je svakog napadača predstaviti zasebnom značkom.

Primjer konkretnog modeliranja napada pomoću Petrijevih mreža može se objasniti pomoću slike 3.13. Stanje P1 sa značkom predstavlja računalo koje je napadač inicijalno kompromitirao u organizaciji koju je napadao. To računalo nije bio napadačev primarni cilj nego samo početak puta do računala na kojem se nalaze podaci koji su njemu interesantni (npr. brojevi kreditni kartica). Prijelaz T1 predstavlja unutarnje izviđanje mreže, a stanja P2 i P3 predstavljaju pronalazak ciljanog računala i pronalazak ranjivosti na ciljanom računalu. Uspješnim

izvođenjem prijelaza T1, značka će s P1 prijeći na P2 i P3 stanja. Stanje u kojem se nalazi Petrijeva mreža nakon uspješnog izvođenja prijelaza T1 prikazano je na slici 3.14.



Slika 3.13 Petrijeva mreža



Slika 3.14 Novi prijelaz

Korištenje Petrijevih mreža u svrhu modeliranja kibernetičkih napada sastoji se od dva dijela [47]:

1. Pobrojavanje svih mogućih sigurnosnih stanja kibernetičkih entiteta
2. Identifikacija svih mogućih napadačkih akcija koji utječu na promjene u sigurnosnim stanjima

Koraci za modeliranje napadača upotrebom Petrijevih mreža nisu previše detaljni, jer pojedina stanja i prijelazi unutar Petrijeve mreže mogu predstavljati različite razine apstrakcije, što daje dodatnu ekspresivnost i jednostavnost modeliranja.

U [47] su predstavljene Petrijeve mreže za modeliranje kibernetičko-fizičkih napada na pametne mreže (engl. *Smart grids*), korištenjem hijerarhijskog pristupa. Hijerarhijski pristup rješava

problem skalabilnosti te omogućuje da dijelovi modela kreiraju zasebni stručnjaci. Detaljnije to znači da su obične Petrijeve mreže kompleksne za veće sustave, te za kreiranje takvih modela jedan stručnjak mora poznavati sve aspekte kibernetičkih i fizičkih prijetnji. Ideja je da se inicijalno kreira apstraktna Petrijeva mreža koja se kasnije može nadopunjavati podmodelima Petrijeve mreže koje će detaljnije opisivati pojedine dijelove apstraktnog modela. Na taj način svaki stručnjak može modelirati jedan dio sustava o kojem ima veliko znanje te se na jednostavan način omogućava integracija pojedinih podmodela. Također, time se izbjegava situacija da se Petrijeva mreža gradi u jednom koraku ili da pojedini dio mreže mora modelirati osoba koja nije stručna o tom dijelu sustava.

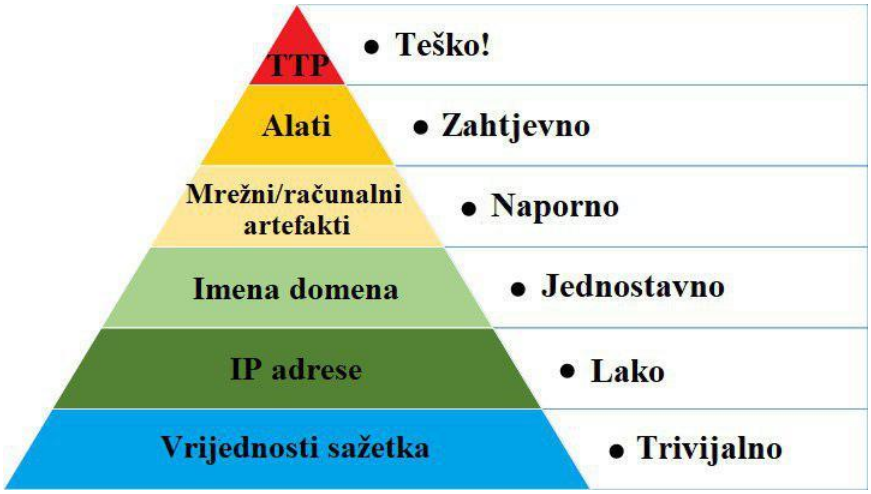
3.6. Pomoćni modeli i klasifikacije

U ovom potpoglavlju opisani su modeli koji mogu na neki način nadopuniti modele opisane u potpoglavlju 3.5 ili mogu poslužiti kao podloga za kreiranje novih modela. Piramida boli je model koji je nastao sa svrhom grupanja indikatora kompromitacije, zbog činjenice da modeli koji se zasnivaju na prekidanju lanca nisu imali dobar način za grupiranje istih. Klasifikacija vojnih aktivnosti i kibernetičkih posljedica nastala je sa svrhom da postane podloga za modeliranje, simulaciju i eksperimentiranje s kibernetičkim napadima, te je kao takva korištena za stvaranje raznih scenarija napada. CAPEC je katalog napadačkih uzoraka, koji služi kao podloga za tehnike u ATT&CK modelu.

3.6.1. Piramida boli

Piramida boli (engl. *Pyramid of Pain*) je model koji olakšava grupiranje i vizualizaciju indikatora kompromitacije (engl. *Indicator of compromise,* IOC) [48]. Model opisuje koliko je resursa potrebno napadaču da promijeni neki element svog napada ukoliko branitelj posjeduje znanje o tom elementu napada. Također služi kao dobar komplement modelima kao što je Cyber Kill chain ili dijamantni model.

Dijagram modela prikazan je na slici 3.15. Piramida je raspodijeljena u 6 slojeva, gdje svaki opisuje indikatore kompromitacije koje sadržava, a s desne strane se nalaze težine koje objašnjavaju koliko “boli” branitelj nanosi napadaču ako se uspješno reagira na te indikatore kompromitacije. U nastavku je detaljnije opisana pojedina razina piramide.



Slika 3.15 Piramida boli [48]

Vrijednosti funkcije sažetka (engl. *Hash value*) se najčešće koriste u kontekstu malicioznih datoteka. Svaki algoritam sažetka prima određeni ulaz i izračunava jedinstveni izlaz točno određene duljine. Danas su najkorišteniji primjeri takvih algoritama MD5 i SHA1. Pošto funkcije sažetka uzimaju u obzir svaki bit ulaza, promjena samo jednog bita rezultira potpuno drugačijim izlazom. Dobra strana toga je da su sažeci vrlo precizan indikator, ali loša strana je da napadač mora promijeniti samo jedan bit kako bi indikator kompromitiranja postao beskoristan.

IP adresa je temeljni indikator jer za bilo kakvu komunikaciju preko Interneta moraju postojati IP adrese računala koji komuniciraju. Dobra strana IP adresa je da se lako detektiraju i blokiraju, ali loša strana je da ih ima veliki broj pa je napadaču vrlo jednostavno promijeniti IP adresu i time zaobići daljnju detekciju koja se temelji na tim indikatorima kompromitacije.

Imena domena su indikatori koji se često pojavljuju, ali su malo teži za promijeniti napadaču u usporedbi s IP adresama. Uzrok teže promjene je to što treba platiti za registraciju te što poslužitelji domenskih imena imaju određeno kašnjenje u propagaciji promjena na Intarnetu.

Mrežni i računalni artefakti su indikatori koji za razliku od prethodnih stvaraju veće probleme napadaču ako su uspješno detektirani. Kada se ti indikatori uspješno detektiraju, napadač mora naći nove načine kako koristiti alate. Primjer je maliciozni program koji zapisuje podatke u Windows registrima. Ako se takvi zapisi mogu detektirati pomoću indikatora, tada napadač mora promjeniti način i mjesto zapisivanja informacija koje je do sad zapisivao u registrima. Primjeri mrežnih artefakata su određene vrijednosti koje su ubačene u HTTP ili SMTP poruke, a primjeri računalnih artefakata su zapisi u registrima, datoteke ili mape koje maliciozni program kreira.

Alati su indikatori koji opisuju alate koje napadači koriste za izvršavanje svojih ciljeva. Problem koji napadač ima kada mu se uspješno spriječi korištenje njegovih alata je što mora uložiti vrijeme u istraživanje alata s funkcionalnostima koje traži i učenje istog, ili razvijanje vlastitog

alata. Primjeri alata su alati za kreiranje malicioznih poruka elektroničke pošte, alati za probijanje lozinki ili alati koji koriste specifičnu mrežnu komunikaciju.

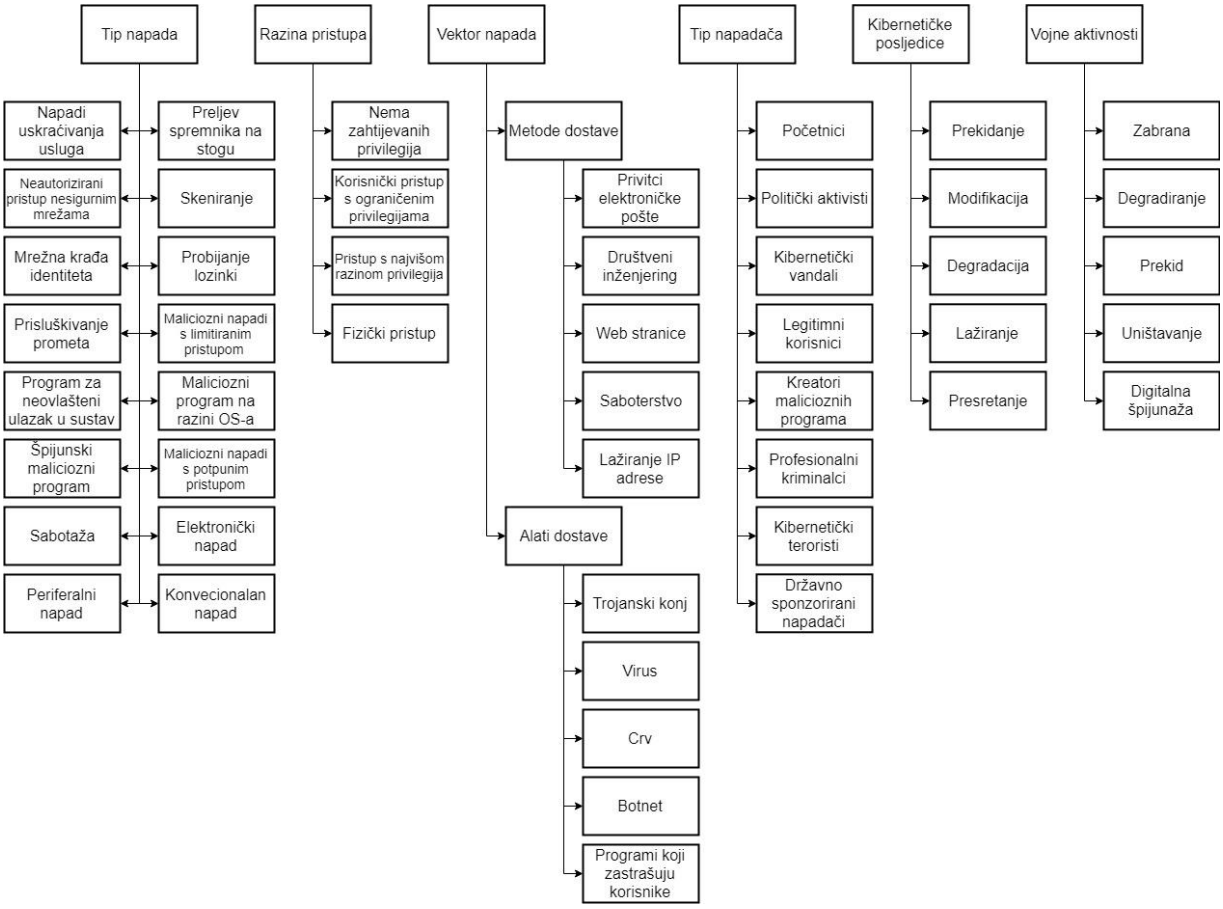
Taktike, tehnike i procedure su indikatori koji su daleko najkorisniji, ali i najteže dobavljivi. Takva vrsta indikatora nama govori kako napadači izvršavaju svoje akcije i baziraju se na promatranju napadačevog ponašanja, a ne samih alata koje koriste. Ti indikatori se protežu kroz cijeli životni ciklus napada, od izviđačke faze pa sve do eksfiltracijske faze. Primjeri takvih indikatora su mrežna krađa identiteta (engl. *Phishing*) ili vrsta žrtava koje napadač napada, kao što su financijske institucije ili kritična infrastruktura.

3.6.2. Vojne aktivnosti i kibernetičke posljedice

Vojne aktivnosti i kibernetički posljedice (engl. *Military Activities and Cyber Effects*, MACE) je klasifikacija koja je primarno izgrađena da služi kao podloga za modeliranje, simuliranje i eksperimentiranje s kibernetičkim napadima i posljedicama koje oni uzrokuju [14]. U kasnijoj fazi razvoja MACE, klasifikacija je proširena za vojne svrhe. Proširenje je omogućilo da se povežu vojne aktivnosti sa željenim efektima prilikom kibernetičkih napada. Klasifikacija je nastala kolaboracijom Defence Research and Development Canada (DRDC), Centre for Operational Research and Analysis (CORA) i Royal Military College of Canada (RMCC), unutar većeg projekta koji se bavi utjecajem posljedica kibernetičkih napada na odluke zapovjedništva i kako integrirati kibernetičke mogućnosti u process operacijskog planiranja [14].

Pošto je MACE klasifikacija izgrađena u svrhu praćenja kibernetičkih posljedica uzrokovanih kibernetičkim napadima korisna je za simuliranje tih efekata u svrhu treniranja i eksperimentiranja. Vježbe u kojima se koristila MACE klasifikacija za razvoj scenarija su: CAGE II, JOINTEX 2013 i DD13. Također može biti korisna i kao komponenta u modeliranju prijetnji, jer opisivanje prijetnje u okviru MACE klasifikacije je dobar početak za process modeliranja prijetnji i određivanje adekvatnih obrana [14].

Klasifikacija se sastoji od 6 glavnih kategorija, koje opisuju kibernetičke napade na temelju razine pristupa koje zahtijevaju da bi napad započeo, kibernetičke posljedice koje napad može proizvesti te vojne aktivnosti za koje se može koristiti. Glavne kategorije klasifikacije su: *Tip napada, Razina pristupa, Vektor napada, Tip napadača, Kibernetičke posljedice i Vojne aktivnosti*. Slika 3.16 prikazuje klasifikaciju, a u nastavku su detaljnije objašnjene glavne kategorije i njihove komponente.



Slika 3.16 MACE klasifikacija

Razina pristupa (engl. *Levels of Access*) je kategorija koja opisuje koju razinu pristupa računalnom sustavu organizacije koju napada napadač mora imati kako bi uopće mogao izvesti napad [14]. Razina pristupa opisuje restrikcije i privilegije koje napadača ograničavaju u onome što može učiniti. Prva kategorija *Tip napada* može se zasebno promatrati, ali ju je bolje promatrati u kontekstu ove kategorije jer svaki napad zahtjeva drugačiju razinu pristupa. Razina pristupa opisuje najmanju razinu pristupa koju napadač mora imati kako bi uspješno započeo napad. Potrebno je napomenuti da lista napada u prvoj kategoriji nije sveobuhvatna, u smislu da opisuje sve moguće napade, zato što se nove vrste napada pojavljuju svaki dan, već je cilj te kategorije dati apstraktniji pregled najvažnijih i najčešće viđenih napada [14].

Postoje 4 vrste razina pristupa [14]:

- *Razina 1: Nema zahtijevanih privilegija*. To su napadi koji ne zahtijevaju nikakav pristup računalu cilja napada. To su napadi koji služe za prikupljanje informacija o meti te napadi koji služe za dobivanje pristupa. Napadi iz prve kategorije koji spadaju u ovu razinu pristupa su:
    - Napadi uskraćivanja usluga (engl. *Denial of Service*, DoS) / Raspodijeljeni napadi uskraćivanja usluga (engl. *Distributed Denial of Service*, DDoS)

    - Preljev spremnika na stogu (engl. *Stack-based buffer overflow*)
    - Neautorizirani pristup nesigurnim mrežama (engl. *War driver*)
    - Skeniranje (engl. *Scanning*)
    - Mrežna krađa identiteta (engl. *Phishing*)
- *Razina 2: Korisnički pristup s ograničenim privilegijama*. Napadi koji zahtijevaju minimalno neku vrstu korisničkog pristupa računalnom sustavu koji se napada. Napadi iz prve kategorije koji spadaju u ovu razinu pristupa su:
    - Probijanje lozinki (engl. *Password Hacking/Cracking*)
    - Prisluškivanje prometa (engl. *Sniffers*)
    - Ostali maliciozni napadi koji zahtijevaju samo limitirani pristup računalnom sustavu
- *Razina 3: Pristup s najvišom razinom privilegije*. Napadi koji zahtijevaju da napadač posjeduje kompletnu kontrolu nad računalnim sustavom koji je kompromitirao. Napadi iz prve kategorije koji spadaju u ovu razinu pristupa su:
    - Program za neovlašteni ulazak u sustav (engl. *Backdoor*)
    - Maliciozni program na razini operacijskog sustava (engl. *Rootkit*)
    - Špijunski maliciozni program (engl. *Spyware/Keylogger*)
    - Ostali maliciozni napadi koji zahtijevaju potpuni pristup računalnom sustavu
- *Razina 4: Fizički pristup*. Napadi koji zahtijevaju fizički pristup računalnim sustavima ili mrežnoj infrastrukturi. Napadi iz prve kategorije koji spadaju ovu razinu su:
    - Sabotaža (engl. *Sabotage*)
    - Elektornički napad (engl. *Electronic attack*)
    - Periferalni napad (engl. *Peripheral attack*)
    - Konvencionalan napad (engl. *Conventional attack*)

Vektori napada (engl. *Attack vectors*) je kategorija koja opisuje metode i alate korištene za kompromitiranje računala i instaliranje malicioznih programa [14]. Preciznije, to su mehanizmi koji omogućuju napadaču da određenim putem dođu do računalnog sustava mete, sa svrhom kompromitiranja računala i instaliranja malicioznih programa.

- *Metode dostave* su mehanizmi pomoću kojih napadač dostavlja maliciozni kod. Mehanizmi u ovoj skupini zahtijevaju određenu razinu napora napadača da uspješno postavi i izvede napad. Mehanizmi dostave koji su navedeni u klasifikaciji su:
    - Privitci elektroničke pošte (engl. *Email Attachments*)
    - Društveni inženjering (engl. *Social Engineering*)
    - Web stranice (engl. *Websites*)
    - Sabotaža (engl. *Saboteur*)
    - Lažiranje IP adrese (engl. *IP Address Spoofing*)
- *Alati dostave* za razliku od metoda dostave često ne zahtijevaju kontrolu od strane napadača. Alati se mogu samostalno širiti ili mogu prevariti korisnika u svrhu da ih korisnik instalira na svoje računalo. Neki alati mogu biti dostavljeni pomoću mehanizama dostave. Alati dostave koji su navedeni u klasifikaciji su:
    - Trojanski konj (engl. *Trojan Horse*)
    - Virus

- Crv (engl. *Worm*)
- Botnet
- Programi za zastrašivanje korisnika (engl. *Scareware*)

Tipovi napadača (engl. *Adversary Types*) je kategorija koja opisuje različite vrste napadača. Napadači se mogu razlikovati po razini znanja ili resursa koje posjeduju, motivaciji ili metodi rada. Postoji 8 skupina napadača [14]:

- *Početnici* (engl. *Script Kiddies*) su najprimitivnija vrsta napadača. Posjeduju malu razinu znanja i loših su financijskih mogućnosti. Svoje radnje odvijaju pomoću alata koje su drugi izradili. Motivacija im je izgradnja statusa u sigurnosnoj zajednici ili privlačenje pažnje.
- *Politički aktivisti* (engl. *Hacktivists*) najčešće su slabijeg znanja, iako postoje slučajevi i naprednijih napada od strane političkih aktivista. Najčešće su loših financijskih mogućnosti, a motivacija im je političkog tipa.
- *Kibernetički vandali* (engl. *Cyber Punks*) su naprednija verzija Početnika. Motivacija im je i dalje ista, s tim da kibernetički vandali mogu biti umiješani i u maliciozne radnje, kao što su krađa identiteta. Razina znanja im je veća u odnosu na Početnika, ali su lošijih financijskih mogućnosti.
- *Legitimni korisnici* (engl. *Insiders*) su specifična vrsta napadača jer se su to većinom radnici organizacija koju napadaju. Mogu, ali i ne moraju biti dobrih tehničkih mogućnosti, ali imaju dobro znanje o unutarnjoj strukturi organizacije. Motivacija im je najčešće osveta.
- *Pisci malicioznih programa* (engl. *Coders*) iako mogu biti napadači, njihova primarna svrha je kreiranje alata i ostalih malicioznih programa koje će drugi napadači koristiti. Imaju dobru razinu znanja, a motivirani su financijski i s povećanjem statusa.
- *Profesionalni kriminalci* (engl. *Black Hat Hackers*) su napadači koji su posjeduju vrlo visoku razinu znanja. Primarna motivacija im je financijskog tipa. Iako mogu raditi sami, najčešće rade u sklopu kriminalnih organizacija.
- *Kibernetički teroristi* (engl. *Cyber Terrorists*) su napadači koji su umiješani u napade protiv drugih država ili vladinih organizacija. Posjeduju visoku razinu znanja i dobrih su financijskih mogućnosti. Motivirani su ideologijom.
- *Državno sponzorirani napadači* (engl. *Nation-States*) su napadači koji su pod kontrolom državnih organizacija, kao što su vojska ili obavještajne agencije. Posjeduju vrlo visoku razinu znanja i dobrih su financijskih mogućnosti. Motivacija im je određena interesima njihovih nadređenih organizacija.

Kibernetičke posljedice (engl. *Cyber Effects*) je kategorija koja opisuje koje posljedice u organizaciji mogu biti prouzročene različitim napadima. Posljedice mogu biti utjecati na same računalne sustave ili podatke koji se nalaze na njima. U nastavku je opisano 5 kategorija posljedica te vrste napada koje izazivaju te posljedice [14]:

- *Prekidanje* (engl. *Interruption*) je posljedica koja rezultirana nedostupnošću resursa koji se napada na neko određeno vrijeme. Napadi koji izazivaju posljedicu su:
  - DoS/DDoS

    - Preljevi spremnika na stogu
    - Maliciozni program na razini operacijskog sustava
    - Sabotaža
    - Elektronički napadi
    - Konvencionalni napadi
- *Modifikacija* (engl. *Modification*) je posljedica koja je rezultirana promjenama nad podacima. Napadi koji izazivaju posljedicu su:
    - Maliciozni napadi
    - Maliciozni program na razini operacijskog sustava
    - Sabotaža
    - Periferni napadi
- *Degradacija* (engl. *Degradation*) je posljedica koja je nastaje kada napadač uzrokuje smanjenje performansi računalnog sustava. Napadi koji izazivaju posljedicu su:
    - DoS/DDoS
    - Preljevi spremnika na stogu
    - Skeniranje
    - Maliciozni napadi
    - Maliciozni program na razini operacijskog sustava
    - Sabotaža
    - Elektronički napadi
    - Konvencionalni napadi
- *Lažiranje* (engl. *Fabrication*) je posljedica koja nastaje ubacivanjem lažnih informacija u sustav. Napadi koji izazivaju posljedicu su:
    - Preljevi spremnika na stogu
    - Mrežna krađa identiteta
    - Maliciozni napadi
    - Maliciozni program na razini operacijskog sustava
    - Sabotaža
- *Presretanje* (engl. *Interception*) je posljedica koja nastaje kada napadač iskoristi činjenicu da može snimati i prisluškivati protok informacija. Napadi koji izazivaju posljedicu su:
    - Skeniranje
    - Mrežna krađa identiteta
    - Prisluškivanje
    - Maliciozni napadi
    - Maliciozni program na razini operacijskog sustava
    - Špijunski maliciozni program
    - Sabotaža
    - Elektronički napadi
    - Periferni napadi

Vojne aktivnosti (engl. *Military Activities*) odnose se na vojne efekte koje napadačke vojne operacije mogu prouzročiti. Napadačke vojne operacije su operacije u kojima vojne snage

napadaju protivnika. Vojni efekti zapravo pokazuju kako kibernetički efekti mogu pomoći vojskama u izvršavanju njihovih željenih ciljeva. Postoji 5 vojnih efekata kojima je cilj nanijeti štetu protivničkoj infrastrukturi ili informaciji i programskoj potpori koja se nalazi na infrastrukturi. U nastavku je opisano svih 5 vojnih efekata te koji se kibernetički efekti mogu koristiti da bi se dobili željeni vojni efekti.

- *Zabrani* (engl. *Deny*): Sprječava napadača da pristupi svojoj infrastrukturi ili informacijama i programskoj potpori koja se tamo nalazi. Šteta na funkcionalnost sustav je samo privremena, ali sve su funkcionalnosti zahvaćene. Kibernetički efekti koji se mogu koristiti da se proizvede željeni vojni efekt zabrane su:
    - Prekidanje
    - Modifikacija
    - Lažiranje
- *Degradirati* (engl. *Degrade*): Nastoji smanjiti efektivnosti ili efikasnost napadačke infrastrukture, ili njegove mogućnosti da radi maliciozne radnje. Šteta na funkcionalnost sustav je trajna, ali samo neke funkcionalnosti su zahvaćene. Kibernetički efekti koji se mogu koristiti da se proizveden željeni vojni efekt degradacije su:
    - Modifikacija
    - Degradacija
    - Lažiranje
- *Prekinuti* (engl. *Disrupt*): Prekida protok informacija između dva odabrana sustava. Šteta na funkcionalnost sustava je privremena i samo neke funkcionalnosti su zahvaćene. Kibernetički efekti koji se mogu koristiti da se proizveden željeni vojni efekt prekidanja su:
    - Prekidanje
    - Modifikacija
    - Degradacija
- *Uništi* (engl. *Destroy*): Uništava infrastrukturu ili informacije i programsku potporu koja se tamo nalazi, tako da se ona ne može više popraviti. Šteta na funkcionalnost sustava je trajna i sve funkcionalnosti su zahvaćene. Kibernetički efekt koji se može koristiti da se proizveden željeni vojni efekt uništavanja je:
    - Modifikacija
- *Digitalna špijunaža* (engl. *Digital Espionage*): Pristup privatnim, komercijalnim ili vladinim informacijskim sustavima u svrhu krađe, uništavanja i pronevjere informacija za privatne i političke svrhe. Kibernetički efekti koji se mogu koristiti da se proizveden željeni vojni efekt digitalne špijunaže su:
    - Lažiranje
    - Presretanje

3.6.3. CAPEC

CAPEC (*Common Attack Pattern Enumeration and Classification*) je katalog napadačkih uzoraka koji je 2007. godine objavila MITRE organizacije [49]. Katalog je organiziran na intuitivan način te sadrži detaljan opis srodnih napada i za dijeljenja informacija o njima. Cilj CAPEC-a je pomoć prilikom razvijanja programske potpore. Također mnogi CAPEC obrasci su korišteni kroz razne tehnike koje su opisane u ATT&CK modelu.

Obrasci napada su opis čestih tehnika koje se koriste u svrhu eksploatacije programske potpore te se napadački uzorak može promatrati kao nacrt za specifičnu vrstu napada. Izvedeni su iz oblikovnih obrazaca i za razliku od oblikovnih obrazaca primijenjeni su u destruktivnom kontekstu [50]. Obrasci su generirani iz detaljne analize specifičnih eksploatacija iz stvarnog svijeta i koristan su alat za opisivanje i komuniciranje napadačke perspektiv [50].

CAPEC se sastoji od 508 napadačkih uzoraka koji su podijeljeni u 15 kategorija, koje su podjelijene u dvije meta-kategorije [49]:

- Mehanizmi napada
    - Prikupljanje i analiziranje informacija
    - Ubacivanje nepredviđenih podataka
    - Obmanjujuća interakcije
    - Manipuliranje vremenom i stanjem
    - Iskorištavanje postojećih funkcionalnosti
    - Zaobilaženje pristupnih kontrola
    - Manipuliranje strukturama podataka
    - Manipuliranje resursima sustava
- Domena napada
    - Društveni inženjering
    - Lanac opskrbe
    - Komunikacije
    - Programska podrška
    - Fizička sigurnost
    - Hardver

Svaki napadački uzorak opisan je osnovnim atributima, te proširenim atributima koji ovise o vrsti uzorka. U nastavku je dan popis osnovnih atributa i nekih od najčešćih proširenih atributa:

- Osnovni atributi
    - Sažetak napadačkog uzorka
    - Preduvjeti za izvođenje napada
    - Rješenje i ublažavanje napada
    - Povezani obrasci napada
- Prošireni atributi
    - Ozbiljnost napada
    - Vjerojatnost uspjeha napada

- Primjer
- Indikatori i upozorenja napada
- Zahtijevana vještina i znanje napadača
- Zahtijevani resursi napadača
- Motivi i posljedice napada
- Povezane slabosti
- Bitni sigurnosni zahtjevi
- Reference na izvore

4. Primjena modela na stvarnim napadima

U ovom poglavlju bit će opisana dva vrlo poznata napada koja su se dogodila u prošlosti pomoću modela koji su opisani u prošlom poglavlju. Napadi koji će biti opisani su napad na Tvrtku Target i napad na Ukrajinska postrojenja električne energije. Ukrajinski napad opisan je pomoću dijamantnog modela, preciznije napravljena je dretva aktivnosti. Target napad će biti opisani pomoću kibernetičkog lanca prekidanja. Cilj ovog poglavlja je dati osjećaj modeliranja dva vrlo kompleksna napada te time prikazati zašto su modeli za modeliranje napadača korisni u svrhu poboljšavanja razumijevanja djelovanja napadača te posljedično za uspješniju obranu.

4.1. Napad na tvrtku Target

Target je druga najveća maloprodajna tvrtka u Sjedinjenim Američkim državama [56]. U studenom i prosincu 2013. godine Target je bio žrtva kibernetičkog napada [57]. Napadači su uspješno upali u računalne sustave kroz partnersku tvrtku te pritom ukrali 70 milijuna osobnih podataka klijenata te 40 milijuna brojeva kreditnih kartica [57]. Kasnije je prijavljeno da su se ukradene kreditne kartice pojavile na crnom tržištu, a samu tvrtku Target je krađa podataka koštala oko 252 milijuna američkih dolara [58].

Postupak napada tekao je na sljedeći način. Napadači su prvo kompromitirali partnersku tvrtku. Napad je izveden pomoću poruke elektroničke pošte koja je sadržavala maliciozni privitak. Nakon što je privitak otvoren, maliciozni program je instaliran te je on počeo automatsku krađu vjerodajnica. Nakon određenog vremena napadači su uspješno ukrali vjerodajnice koje partnerska tvrtka koristi za prijavu na Web sučelje tvrtke Target. Web sučelje je služilo za prijavu partnerskih tvrtki u svrhu obavljanja poslovnih obveza s Targetom. Uspješnom prijavom na Web aplikaciju napadači su pronašli ranjivost u Web sučelju koja im je omogućavala da izvode proizvoljan kod na Web poslužitelju. Napadači su nakon toga radili unutarnje izviđanje u svrhu daljnje propagacije, a paralelno s tim su uspjeli ukrasti legitimnu sjednicu domenskog administratora. Pomoću ukradene sjednice uspješno su kreirali novog domenskog administratora. Nakon izviđanja i kreiranja domenskog administratorskog računa napadači su se propagirali do zanimljivih računala i nakon toga ukrali 70 milijuna privatnih informacija korisnika te instalirali maliciozni program na POS (engl. *Point of sale*) terminale koji je služio za krađu informacija o kreditnim karticama. Svi ukradeni podaci bili su prikupljani na poslužitelj unutar Target mreže, koji je nakon toga poslužio napadačima da uspješno eksfiltriraju podatke na svoje poslužitelje [57].

U nastavku je detaljnije objašnjen napad pomoću kibernetičkog lanca prekidanja, a analiza je bazirana na izvješćima [57] i [59].

4.1.1. Kibernetički lanac prekidanja

U fazi *izviđanja* napadači su tražili put u unutarnju mrežu tvrtke Target i odlučili da je optimalan put preko partnerske tvrtke Fazio Mechanical. Iako nije poznato kako su napadači saznali informacije o partnerski tvrtkama, u izvješćima je navedeno da se u trenutku napada moglo pristupiti popisu partnera tvrtke Target pomoću jednostavnih Internetskih pretraživanja. Također, vjeruje se da su napadači na sličan način kroz analizu metapodataka uspjeli saznati više informacija o nekim dijelovima interne mreže tvrtke Target i posljedično tako saznali za Web sučelja koja koriste partnerske tvrtke. Nakon odluke o napadu na Fazio Mechanical napadači su detaljnije istražili zaposlenike te tvrtke u svrhu slanja ciljanih i vjerodostojnih poruka elektroničke pošte.

U fazi *naoružavanja* napadači su, korištenjem informacija o zaposlenicima tvrtke Fazio Mechanical, napravili vjerodostojne maliciozne poruke elektroničke pošte. Poruke su u sebi sadržavale maliciozni privitak. Iako nikad nije potvrđeno koja vrsta privitka je bila u porukama, vjeruje se da je privitak bio PDF ili Microsoft Office dokument koji je u sebi sadržavao maliciozni program *Citadel*. Citadel je dobro poznat i analiziran maliciozni program s funkcionalnošću krađe vjerodajnica Web aplikacije.

U fazi *dostave* napadači su slali maliciozne poruke elektroničke pošte tvrtki Fazio Mechanical. Vjeruje se da je slanje poruka krenulo oko 2 mjeseca prije inicijalnog upada u sustave tvrtke Target. Informacije o akcijama napadača u tvrtki Fazio Mechanical nisu dostupne, ali je poznato da tvrtka nije bila u skladu s najboljim sigurnosnim praksama i koristila je besplatnu anti-virusnu zaštitu koja nije omogućavala zaštitu u stvarnom vremenu.

U roku od 2 mjeseca napadači su uspješno ukrali vjerodajnice za Web aplikaciju koja se nalazila na internoj mreži Targeta, a služila je za poslovanje s partnerskim tvrtkama. Iako nikad nije točno potvrđeno o kojoj se aplikaciji točno radi, prema izvještajima Fazio Mechanical je koristio interne Web aplikacije za naplaćivanje računa, dogovaranje ugovora i upravljanje projektima. Prema tome postoje 3 moguće Web aplikacije:

- *Ariba* Web aplikacija koja služi kao sustav za naplaćivanje računa. Upravo Ariba se najčešće spominje kao aplikacija za koju su napadači uspjeli prikupiti vjerodajnice.
- *Partners Online* Web aplikacija koja služi za dogovaranje ugovora i upravljanje projektima.
- *Target Property Development Zone* Web aplikacija koju je Fazio Mechanical tvrtka koristila za obavljanje svojih poslova.

Potrebno je napomenuti da Target nije postupao u skladu s najboljim preporučenim sigurnosnim praksama i nije zahtijevao 2-faktorsku autentifikaciju, što je uvelike olakšalo napadačima inicijalni pristup autentificiranom korisničkom sučelju.

U fazi *eksploatacije* napadači su iskoristili ukradene vjerodajnice za autentifikaciju na internoj Web aplikaciji nakon čega su pronašli ranjivost koja im je omogućila daljnje akcije. Iako je poznato da segmentacija internet mreže Targeta nije bila dobro, napadači svejedno nisu mogli

direktno pristupi ničemu osim samoj Web aplikaciji. Da bi pristupili Web poslužitelju na kojemu se aplikacija izvršavala, a potom i ostalim računalima na internoj mreži, napadači su morali pronaći ranjivost u Web aplikaciji koja će im to omogućiti. Napadači su uspješno pronašli i eksploatirali ranjivost u funkcionalnosti za učitavanje dokumenata koja nije radila ispravnu provjeru učitanih datoteka. Na taj način napadači su uspješno učitali PHP skriptu imena ”xmlrpc.php” koja je u sebi sadržavala Web ljusku te tako omogućila napadačima izvršavanje naredbi na operacijskom sustavu.

Zbog mogućnosti izvođenja naredbi na operacijskom sustavu Web poslužitelja napadači su krenuli u ostvarivanje perzistencije u internoj mreži i na unutarnje istraživanje s ciljem proširivanja svojeg znanja o internoj mreži i detekciji poslužitelja na kojima se nalaze podaci o kreditnim karticama i informacije o kupcima. Da bi uspješno prikupili informacije o unutarnjoj mreži napadači su ciljali Aktivni direktorij (engl. *Active Directory*) koji sadrži informacije o svim korisnicima, računalima i servisima na domeni. Da bi se pristupilo Aktivnom direktoriju nije potreban poseban alat ili veće privilegije, već suprotno, alati za pristupanje Aktivnom direktoriju dolaze u paketu s ostalim internim Windows alatima koji se baziraju na standardnom Lightweight Directory Access Protocol (LDAP) protokolu. To znači da bilo koji domenski korisnik može postavljati upite Aktivnom direktoriju, a tu mogućnost su napadači i iskoristili te tako saznali svoje ciljane mete, lokacije SQL poslužitelja i POS terminala. Slanjem upita na DNS poslužitelj koji je kolociran na poslužitelju Aktivnog direktorija napadači su saznali IP adrese SQL poslužitelja i POS terminala.

U fazi *instaliranja* napadači su uspješno osigurali perzistenciju na internoj mreži tvrtke Target kreiranjem novog domenskog administratora. Također, time su osigurali jednostavniji pristup interesantnim poslužiteljima i POS terminalima, a koji zahtijevaju veću razinu prava pristupa koju do tog trenutku nisu posjedovali. U nastavku je objašnjeno kako su to postigli.

Najbolji način za ostvarivanje perzistencije i prava pristupa svim željenim sustavima je korištenjem korisničkog računa domenskog administratora. Zbog loše sigurnosne prakse u internoj mreži tvrtke Target većina internih aplikacija je koristila vjerodajnice Aktivnog direktorija. Na sreću napadača, jedna od tih aplikacija je bila i administrativno sučelje na Web poslužitelju koji je bio kompromitiran. Iako napadači nisu bili u mogućnosti direktno ukrasti vjerodajnice domenskog administratora, tehnikom *Pass-the-hash* uspjeli su ukrasti sjedničku značku koja se nalazila u memoriji Web poslužitelj. Zbog načina rada autentifikacijskog poslužitelja i Windows mreže sjednička značka može ostati u memoriji sve do gašenja sustava, a pošto se radilo o poslužitelju koji se rijetko gasi, napadači su imali veliku vjerojatnost uspjeha. Iako nije točno potvrđeno, vjeruje se da su napadači tehniku Pass-the-hash izveli jednim od sljedećih alata:

- *Windows Credential Editor* (WCE)
- *QuarksPwDump*
- *Elcomsoft Proactive Password Auditor*

Kada su napadači došli u posjed sjedničke značke korisničkog računa domenskog administratora, kreirali su novog domenskog administratora imena "best1_user". Korištenje novog korisničkog računa omogućilo je napadačima veću fleksibilnost u odnosu na korištenje sjedničke značke i to zbog dva razloga:

- U slučaju da je postojeći domenski administrator promijenio lozinku, ukradena sjednička značka više ne bi bila valjana pa su tako osigurali bolju perzistenciju.
- Remote desktop (RDP) i slični servisi za udaljeni pristup nekom računalu eksplicitno zahtijevaju lozinku i napadačima u tom slučaju sjednička značka ne bi bila od koristi. Tako su osigurali mogućnost udaljenog pristupa i propagacije do željenih sustava.

Kasnije, maliciozni program je koristio "best1_user" korisnički račun za kopiranje podataka o kreditnim karticama s POS terminala na centralnu točku koja se nalazila na internoj mreži.

Faza *naredbe i kontrole* je najmanje poznata faza u cijelom napadu. Inicijalno kao C2 poslužitelj napadači su koristili računala tvrtke Fazio Mechanical, a jednom kada su uspjeli zadobiti veći pristup internoj mreži Target-a izradom novog domenskog administratora nije poznato kako su uspostavljali komunikaciju. Kasnije tijekom eksfiltracije podataka korišteni su FTP poslužitelji u Rusiji.

U fazi *djelovanja prema cilju* napadači su nakon uspješnog unutarnjeg izviđanja i kreiranja novog administratorskog računa krenuli u propagaciju do ciljanih meta, inicijalno bili SQL poslužitelji. Na putu do poslužitelja napadači su trebali riješiti dva problema:

- Zaobilaženje vatrozida i ostalih mrežnih sigurnosnih rješenja koja su ograničavala direktan pristup poslužiteljima.
- Kako doći do ciljanog poslužitelja kreiranjem lanca komprimitiranih računala.

Za uspješno zaobilaženje vatrozida i ostalih mrežnih sigurnosnih rješenja, napadači su koristili alat *Angry IP Scanner* [71] koji omogućava napadačima otrkivanje direktno dostupnih računala s računala na kojemu se oni trenutno nalaze. Pošto s trenutno kompromitiranog računala nisu mogli stići do ciljanih poslužitelja, napadači su morali propagirati kroz niz različitih računala i poslužitelja kako bi došli do svog cilja. Za pokretanje procesa na udaljenim poslužiteljima napadači su u kombinaciji s vjerodajnicama domenskog administratora koristili dva alata:

- *Microsoft PsExec* je alat koji omogućava izvršavanje programa na udaljenom računalu pomoću naredbenog retka.
- *RDP klijent* je alat koji također omogućava izvršavanje programa na udaljenom računalu, ali za razliku od PsExec alata on omogućuje korisniku da to sve izvodi pomoću grafičkog sučelja.

Nakon što su se uspješno propagirali do SQL poslužitelja napadači su prvo koristili *osql.exe* i *isql.exe* alate za ispitivanje da li baza podataka sadrži podatke koji su njima od interesa. Nakon što su utvrdili da su podaci u bazi podataka relevantni, koristili su alat *bcp.exe* za prikupljanje svih unosa u bazi podataka.

Pretpostavlja se da je inicijalna meta napada bila samo baza podataka, ali problem je nastao kada su napadači uočili da je baza podataka u skladu s preporučenim sigurnosnim praksama te ne sadrži podatke kreditnih kartica. To je uzrokovalo da promjene način rada i da se okrenu POS terminalima koje su prethodno detektirali u fazi unutarnjeg izviđanja. Napadači su propagirali do POS terminala na jednak način kako su i inicijalno došli do SQL poslužitelja te su na terminale instalirali maliciozni program *Kaptoxa*. Maliciozni program Kaptoxa radi na način da skenira memoriju POS terminala i ako identificira podatke o kreditnoj kartici onda ih pohrani u lokalnu datoteku. Druga funkcionalnost Kaptoxa malicioznog programa je kreiranje datoteke (engl. *Remote file share*) na udaljenom FTP računalu unutar Target mreže pomoću vjerodajnica domenskog administratora i Windows ugrađene naredbe `net use`. Maliciozni program je periodički kopirao lokalne datoteke koje su sadržavale informacije o kreditnim karticama s POS terminala u udaljenu dijeljenu datoteku.

Nakon što su podaci prikupljeni iz baze podataka ili POS terminala stigli na FTP računalo, maliciozna skripta koja je instalirana na jednak način kao i Kaptoxa maliciozni program slala je uz pomoć Windows FTP klijenta podatke na udaljeni FTP poslužitelj izvan Target mreže koji je bio u posjedu napadača. Poznato je da se jedan od FTP poslužitelja nalazio u Rusiji, iako se vjeruje da ih je bilo više diljem svijeta.

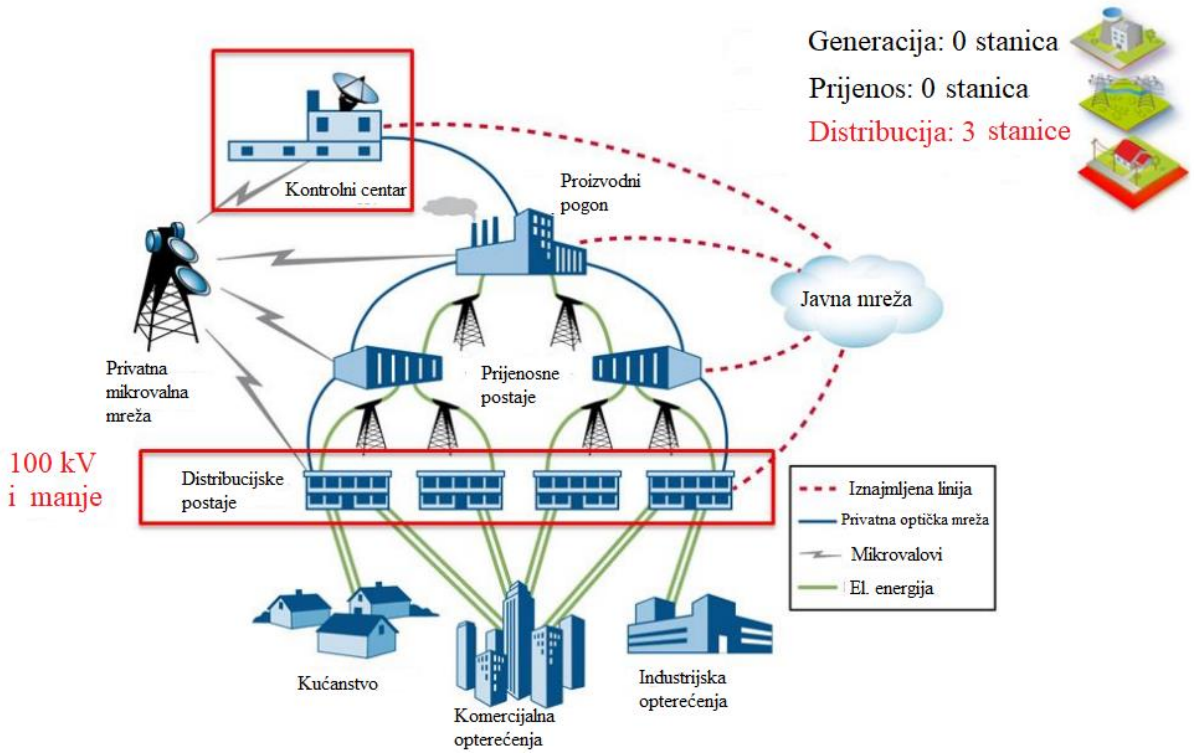
Nakon opisa napada pomoću kibernetičkog lanca prekidanja lakše se mogu vidjeti radnje koje su tvrtke Fazio Mechanical i Target mogle napraviti da bi spriječilo napad. Obrambene akcije koje su mogle zaustaviti napad su:

- Korištenje komercijalnog anti-virusnog programa sa zaštitom u stvarnom vremenu.
- Korištenje 2-faktorskog mehanizma za prijavu partnerskih tvrtki na Web sučelja.
- Ispravna segmentacija interne mreže pomoću strožih pravila vatrozida.
- Onemogućavanje korištenja vjerodajnica s Aktivnog direktorija za prijavu na većinu internih aplikacija.
- Povećanje sigurnosnih kontrola sa svrhom otkrivanja unutarnjeg istraživanja, pogotovo radnji koje se odvijaju pomoću LDAP protokola.
- Povećanje sigurnosnih mjera oko Aktivnog direktorija, pošto je on bio centralna točka oko koje se većina akcija napadača odvijala.
- Ograničavanje administratorski prava za pojedine korisnike i aplikacije.
- Periodičko provjeravanje Aktivnog direktorija u svrhu uočavanja nepoznatih i skrivenih korisnika.
- Korištenje liste dobroćudnih programa koji mogu biti instalirani na poslužiteljima i POS terminalima.

4.2. Napad na Ukrajinska električna postrojenja

Napad na Ukrajinska električna postrojenja dogodio se 23.12.2015. godine u 15:35 te je prvi ikad zabilježeni kibernetički napad na električna postrojenja [51], [52]. To je ujedno i jedan od prvih napada koji je pokazao koliku štetu kibernetički napadi mogu imati na kritičnu infrastrukturu, tj. kako kibernetički napadi mogu drastično utjecati na fizički svijet. Napadači su uspješno kompromitirali računalne i SCADA (engl. *Supervisory control and data acquisition*) sustave 3 različite tvrtke za distribuciju električne energije i time uzrokovali prekid dovoda električne energije za 225.000 ljudi na nekoliko sati [52]. Ukrajinski distribucijski centri, iako imaju automatizirani način gašenja i paljenja distribucije, također imaju i mogućnost ručnog paljenja pa se time uspješno uspostavila opskrba električnom energijom. Važno je napomenuti da postoje države koje nemaju mogućnost ručnog obnavljanja distribucije električnom energijom i kod tih bi država takav napad prouzročio puno veću štetu.

Na slici 4.1 nalazi se prikaz strukture Ukrajinskog energetskog sustava. Crvenim su okvirima označeni entiteti koji su napadnuti. Preciznije, napadnuti su kontrolni centri distribucijskih tvrtki koji upravljaju stanicama za distribuciju električne energije prema krajnjim korisnicima.



Slika 4.1 Prikaz strukture Ukrajinskog električnog sustava [52]

Nije poznato zašto su baš 3 specifična distribucijska centra napadnuta, ali neke mogućnosti su [52]:

- Mete sa sličnim sustavima i konfiguracijom.
- Sustavi sa zajedničkom centraliziranom točkom koja ih kontrolira.
- Napadač je imao mogućnosti koje su mu jednostavno omogućile upad u te sustave.
- Napadačeva procjena da je rizik od otkrivanja na tim metama manji.
- Napadačeva procjena da će na njima uspješno uspjeti doći do cilja u određenom vremenskom periodu.

Napadi na 3 distribucijske tvrtke bili su koordinirani i dogodili se u razmaku od 30-tak minuta. Napad nikad nije javno atribuiran niti jednoj grupi ili državi, ali često se spominje Rusija zbog stanja između dviju država u to vrijeme [53]. Također, spominje se i da je napad djelo više koordiniranih skupina [53]. Sigurno je da se radi o napadačima vrlo visokog tehničkog znanja, koji su dobro financijski podržani te su jako dobro koordinirani, ali atribucija niti nije važna ukoliko je jedino važno razmotriti kako se uspješno obraniti od takvih napadača u budućnosti.

Napadači su uspješno demonstrirali razne taktike i tehnike kako bi zaobišli zaštite. Mogućnosti koje su napadači pokazali su [52]:

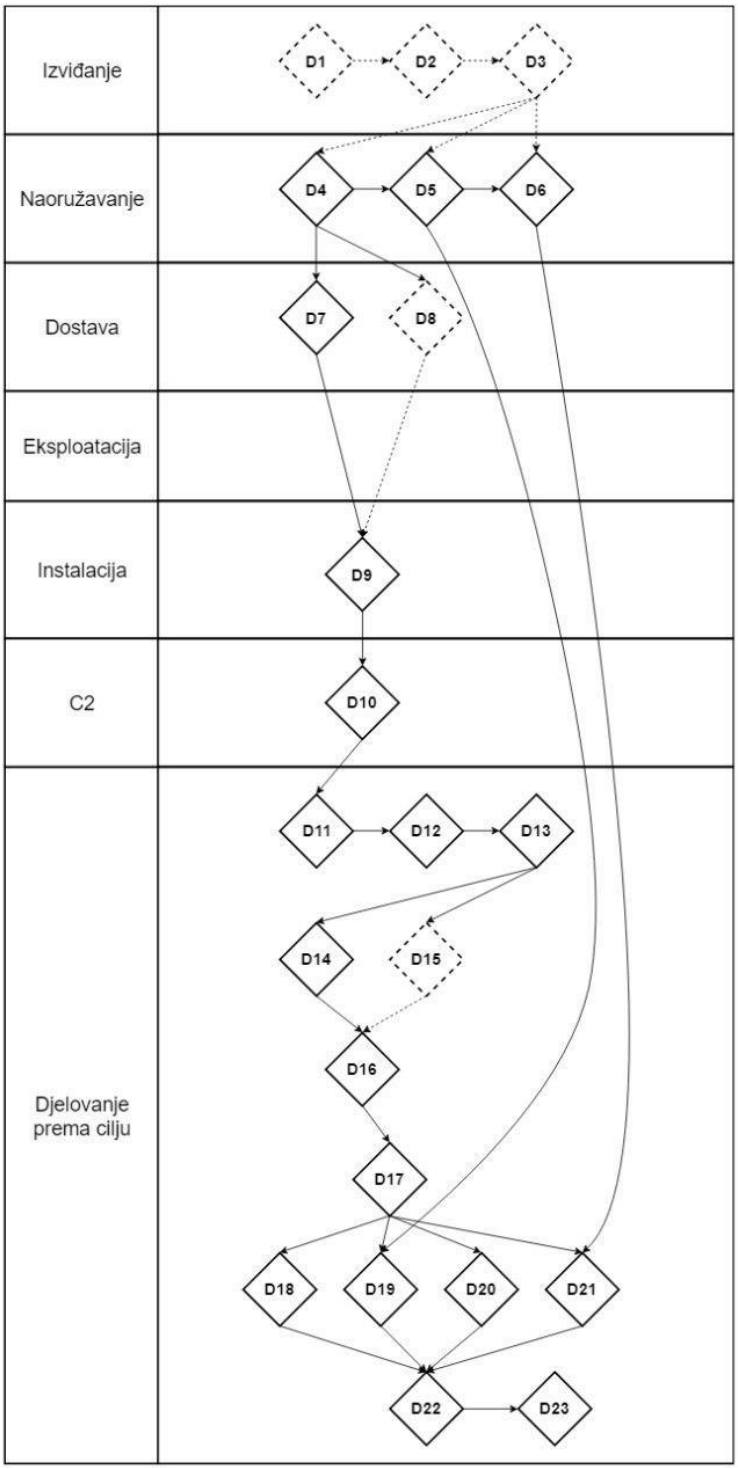
- Ciljane i pomno smišljene maliciozne poruke elektroničke pošte.
- Korištenje malicioznog programa Black Energy 3.
- Naoružavanje Microsoft Office dokumenata sa svrhom dobivanja inicijalnog pristupa.
- Krađa vjerodajnica i ostalih informacija potrebnih za uspješnu propagaciju do SCADA sustava.
- Korištenje virtualne private mreže za ulazak u SCADA sustave.
- Vrlo visoka razina poznavanja korištenja SCADA sustava.
- Izgradnja prilagođenog malicioznog firmware programa za komunikacijske uređaje.
- Korištenje modificiranog malicioznog programa KillDisk za brisanje Master Boot Record sekcije i ciljano brisanje nekih sistemskih zapisa.
- Uzrokovanje nedostupnosti telefonskih linija u pozivnim centrima pomoću velikog broja poziva koji su im bili upućeni.

Potrebno je napomenuti da suprotno početnom mišljenju maliciozni programi Black Energy 3 i KillDisk nisu sami imali mogućnost prouzročiti nestanak distribucije električne energije. Oni su samo omogućili napadaču da dobije uspješan pristup SCADA sustavima te sam uzrokuje prekid dovoda struje [52].

4.2.1. Dijamantni model

U ovom potpoglavlju bit će prikazano modeliranje napada pomoću dijamantnog modela koji će biti mapirani na kibernetički lanac prekidanja. Analiza je temeljena na izvješćima [52] [54] [55]. Na slici 4.2 prikazana je dretva aktivnosti napada koja će u nastavku detaljnije biti objašnjena.

Veze predstavljaju uzročno-posljedičnu poveznicu između događaja odnosno koji događaji se moraju izvršiti prije nego se neki drugi događaj može uspješno izvršiti. Hipotetski događaji i veze predstavljeni su isprekidanim linijama.



Slika 4.2 Dretva aktivnosti Ukrajinskog napada

Ne postoje izvješća o vidljivom izviđanju na ciljane distribucijske centre. Međutim, analiza 3 distribucijska centra pokazala je da sva 3 imaju vrlo visoki stupanj automatiziranosti te da postoji mogućnost udaljenog upravljanja prekidačima za distribuciju električne energije. Također, zbog velike koordiniranosti i sofisticiranosti napada, može se s velikom vjerojatnošću pretpostaviti da je detaljno izviđanje krenulo mjesecima ranije i da taj napad nije oportunistički. Prema tome, mogu se kreirati 3 događaja dretve aktivnosti:

- Događaj 1 je hipotetski. Napadač u sklopu veće maliciozne kampanje koja je ciljala sve aspekte Ukrajinske kritične infrastrukture istražuje strukturu Ukrajinskog elektro-energetskog sustava.
- Događaj 2 je hipotetski. Na temelju saznanja iz događaja 1 napadač odabire distribucijske centre koji su najviše u skladu s njegovim mogućnostima i ciljevima.
- Događaj 3 je hipotetski. Nakon detaljnijeg istraživanja specifičnih distribucijskih centara napadač radi detaljnije izviđanje infrastrukture te ljudi u svrhu povećanja vjerojatnosti uspješnosti ciljanih malicioznih poruka elektroničke pošte.

U fazi naoružavanja napadači svoje prethodno dobiveno znanje koriste kako bi uspješno pripremili sve potrebne maliciozne programe i alate kako bi dobili inicijalni pristup sustavima za sve kasnije potrebne aktivnosti. Znanje o naoružavanju malicioznih poruka elektroničke pošte prikupljeno je na temelju analize maliciozne kampanje koja je malicioznim porukama elektroničke pošte napadala veliki broj organizacija u Ukrajini. Znanje o ostalim specifičnim malicioznim programima prikupljeno je tijekom analize napada na distribucijske centre. Prema tome mogu se kreirati 3 događaja dretve aktivnosti:

- Događaj 4 je stvaran. Naoružavanje Microsoft Word i Excel dokumenata s Black Energy 3 malicioznim kodom sa svrhom dobivanja inicijalnog pristupa.
- Događaj 5 je stvaran. Izgradnja KillDisk malicioznog programa koji služi za onemogućavanje korištenja računala brisanjem Master boot record sektora na tvrdom disku te brisanje sistemskih zapisa.
- Događaj 6 je stvaran. Napadač izgrađuje specifično podešen i maliciozni firmware za serijsko-ethernetske komunikacijske uređaje koji omogućuju udaljen pristup stanicama za distribuciju električne energije. Nije jasno kako su napadači saznali za specifične uređaje te postoji mogućnost da su maliciozni firmware napravili tek kada su upali u SCADA sustav. Međutim zbog sofisticiranosti napada vjeruje se da su napadači unaprijed pripremili maliciozni program i detaljno ga testirali, a nisu se oslanjali na čistu sreću.

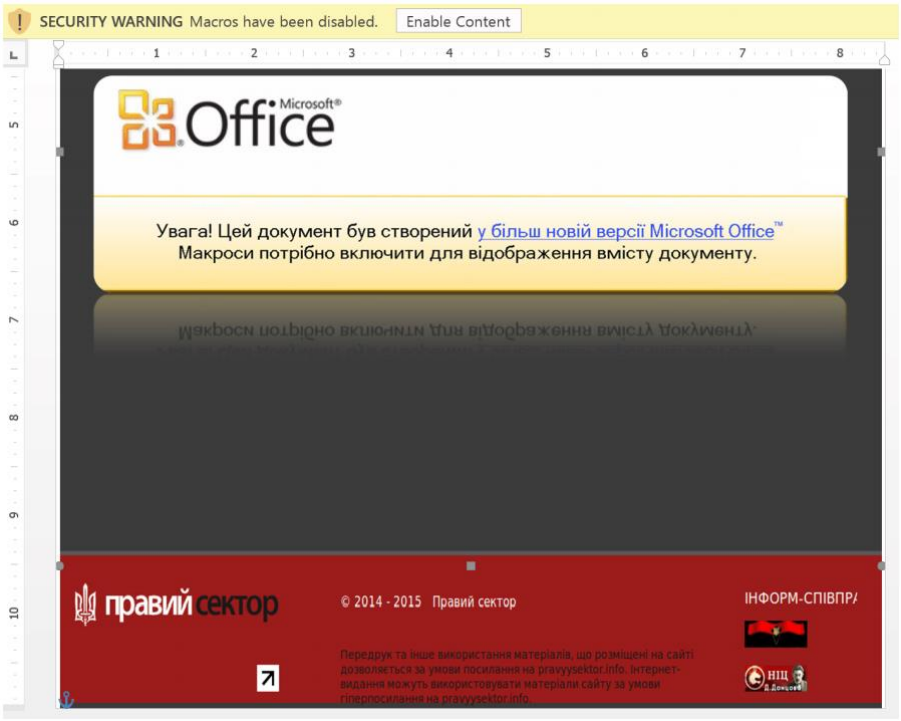
Kao što je i ranije spomenuto faza dostavljanja obuhvaćala je veću malicioznu kampanju koja je ciljala veliki broj organizacija u Ukrajini, od kojih je većina bila na neki način povezana s kritičnom infrastrukturom. Prema tome može se kreirati 1 događaj dretve aktivnosti:

- Događaj 7 je stvaran. Napadač šalje poruke elektroničke pošte koje sadrže maliciozne Excel dokumente ranije identificiranom administrativnom ili tehničkom osoblju koje je zaduženo za računalne sustave i mreže distribucijskih centara.

- Događaj 8 je hipotetski. Napadač šalje maliciozne poruke elektroničke pošte koje sadrže maliciozne Word dokumente ranije identificiranom administrativnom ili tehničkom osoblju koje je zaduženo za računalne sustave i mreže distribucijskih centara.

U fazi instalacije osoblje u distribucijskim centrima otvorilo je maliciozne poruke i time omogućilo početak izvršavanja Black Energy 3 malicioznog koda. Na slici 4.3 prikazana je poruka koja je dočekala osoblje kada su otvorili maliciozni Excel dokument. Za uspješno pokretanje maliciozni program zahtjeva samo omogućavanje makro funkcionalnosti te nije postojala nikakva eksploatacija poznatih ili nepoznatih ranjivosti (zbog toga niti ne postoji događaj u fazi eksploatacije). Omogućavanje makro funkcionalnosti za instaliranje malicioznih programa je vrlo česta praksa, što ukazuje da su poruke elektroničke pošte bilo vrlo vjerodostojno napisane. Nakon omogućavanja instalacija Black Energy 3 kod se pokreće. Prema tome 1 događaj dretve aktivnosti je:

- Događaj 9 je stvaran. Osoblje u distribucijskim centrima koje je primilo maliciozni poruku elektroničke otvara maliciozni Word ili Excel dokument te omogućava makro funkcionalnost koja pokreće prvu fazu instalacije Black Energy 3 malicioznog programa.



Slika 4.3 Izgled maliciozne poruke nakon otvaranja [52]

Nakon uspješne instalacije, Black Enery 3 maliciozni program kontaktira poslužitelj kojim upravljaju napadači i omogućava mu stalni pristup na zaraženo računalo. Uz to što početno

uspostavlja perzistenciju na zaraženom računalu, vrlo važna karakteristika Black Energy 3 malicioznog programa je velika modularnost koja omogućava napadaču da koristi dodatke koje želi. Prema tome 1 događaj dretve aktivnosti se može stvoriti:

- Događaj 10 je stvaran. Nakon uspješne instalacije Black Energy 3 je uspostavio komunikaciju s poslužiteljem te mu time omogućava pristup kompromitiranim računalima.

U fazi djelovanja prema cilju napadači su uspjeli kreirati perzistentnu okolinu za svoje akcije u poslovnoj mreži distribucijskih sustava, propagirati se u SCADA sustave te time izvršiti svoj cilj. Napadači su imali dovoljno vremena neprimjetno i promišljeno se propagirati kroz mrežu jer indikatori pokazuju da su inicijalni pristup dobili najmanje 6 mjeseci ranije. Događaji dretve aktivnosti su:

- Događaj 11 je stvaran. Prikupljanje vjerodajnica i informacija s kompromitiranog računala za daljnje širenje unutar mreže.
- Događaj 12 je stvaran. Unutarnje istraživanje za otkrivanje daljnjih sustava u poslovnoj mreži te traženja SCADA sustava.
- Događaj 13 je stvaran. Napadač je vrlo brzo iskoristio otkrivene vjerodajnice i informacije o unutarnjoj mreži za izmjenu autentifikacijskih i autorizacijskih sustava s ciljem da se što bolje uklopi kao legitiman korisnik. Napadač je time uspostavio trajnu perzistenciju kroz cijelu poslovnu mrežu.
- Događaj 14 je stvaran. Napadači kradu vjerodajnice za virtualnu privatnu mrežu i zbog nepostojanja dvo-faktorske autentifikacije uspješno ulaze u SCADA sustav.
- Događaj 15 je hipotetski. Pretpostavlja se da su napadači koristili i administrativne alate da uđu iz poslovne mreže u SCADA sustav.
- Događaj 16 je stvaran. Napadači rade unutarnje istraživanje SCADA sustava.
- Događaj 17 je stvaran. Informacije koje su pronađene unutarnjim istraživanjem omogućilo je napadačima da se prošire kroz cijeli sustav SCADA mreže.
- Događaj 18 je stvaran. Napadači su u barem jednom od 3 distribucijska centra detektirali pomoćni neprekidni izvor napajanja (engl. *Uninterruptible power supply,* UPS) te ga rekonfigurirali da se ugasi kada će i oni ugasiti distribuciju električne energije. Time su osigurali da će i sam distribucijski centar ostati bez električne energije.
- Događaj 19 je stvaran. Napadači instaliraju KillDisk maliciozni program unutar SCADA mreže sa svrhom onemogućavanja računala jednom kada odluči izvršiti svoj krajnji cilj. Puni potencijala KillDisk malicioznog programa bio je uočen tek nakon što su zaposlenici probali ponovno pokrenuti računalne sustave te su onda uočili nemogućnost podizanja operacijskog sustava.
- Događaj 20 je stvaran. Napadač mijenja vjerodajnice za kritične sustave sa svrhom onemogućavanja prijave legitimnih korisnika.
- Događaj 21 je stvaran. Napadač učitava svoj maliciozni firmware sa svrhom onemogućavanja udaljenog pristupa udaljenim stanicama. Posljedica toga je da su zaposlenici distribucijskih centara morali fizički ići do stanica koje su bile ugašene.

- Događaj 22 je stvaran. Napadač pokreće napad, tj. napadač počinje s udaljene lokacije koristeći SCADA sustave prekidati opskrbu električnom energijom. Na taj način ugašeno je 30 distributivnih stanica.
- Događaj 23 je stvaran. Napadač zatrpava lažnim telefonskim pozivima pozivne centre distribucijskih institucija, te time onemogućava stanovnicima Ukrajine da prijave nestanak električne energije.

5. Alati za emulaciju napadača

U okviru ovog poglavlja bit će predstavljeni alati za emulaciju napadača. Alati ovakvog tipa imaju višestruku korist za organizaciju, ali dvije najvažnije funkcije su omogućavanje jednostavnijeg i efektivnijeg djelovanja crvenog tima (engl. *Red team*) unutar organizacije i omogućavanje braniteljima da ispitaju svoje obrambene mehanizme.

U prvom potpoglavlju ukratko su opisani svi alati i način na koji pojedini alati rade. Naglasak je na alatima koji su besplatni i otvorenog koda. U sljedećem potpoglavlju dana je usporedba alata s ciljem da organizacija može lakše razlučiti koje alate koristiti u određenim situacijama. Na kraju je dan primjer korištenja Caldera alata kojim se demonstrira kako bi organizacija mogla iskoristiti tehnike emulacije napadača.

5.1. Opis Alata

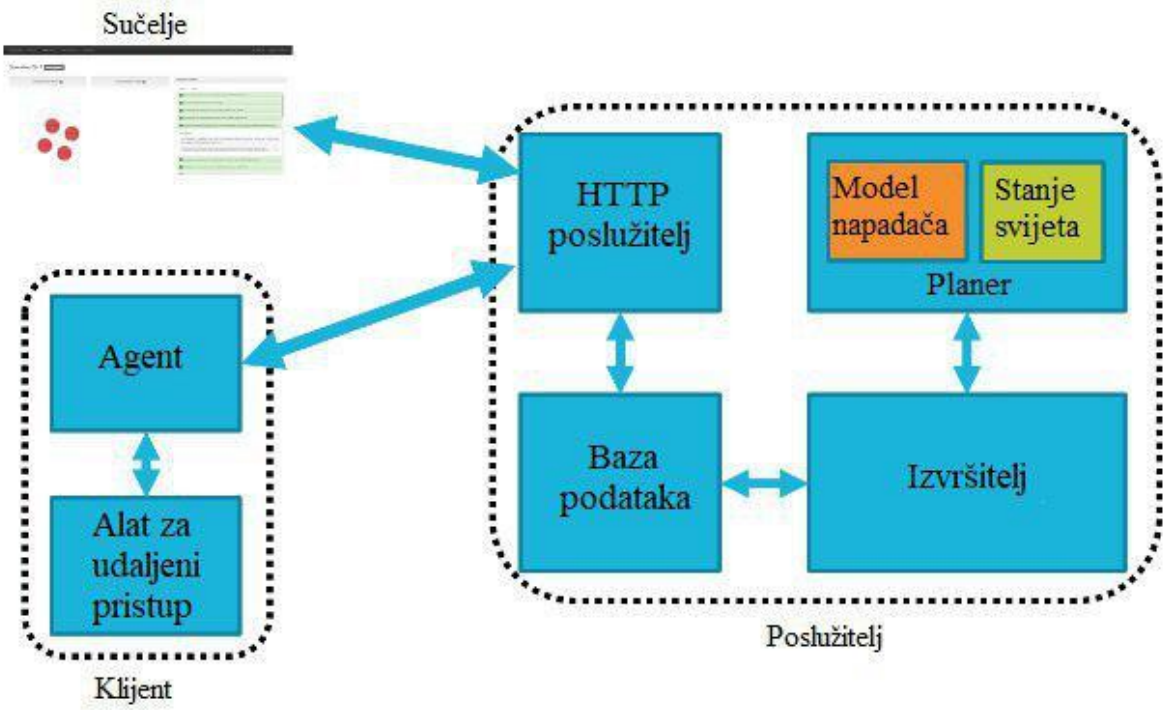
5.1.1. Caldera

Caldera [62] je alat koji je temeljen na ATT&CK modelu, a razvila ga je 2017. godine MITRE organizacija. Alat podržava veliki broj tehnika iz ATT&CK modela. Podržava testiranje samo Windows mreža (engl. *Windows Enterprise Netowrk*) i minimalno je potreban 1 Windows server i 2 Windows klijentska operacijska sustava za njegovo pokretanje.

Na slici 5.1 prikazana je arhitektura Caldere. Sastoji se od dvije komponente: klijent i poslužitelj. Klijent sadrži dvije komponente: agent i alat za udaljeni pristup. Te dvije komponente služe za komunikaciju s poslužiteljem prije, tijekom i poslije izvršavanja emulacije napada. Poslužitelj se sastoji od HTTP poslužitelja koji pruža korisniku korisničko sučelje, baze podataka u kojoj je spremljeno znanje o okolini, izvršitelja koji izvodi tehnike i osvježava bazu podataka te planera koji je komponenta koja odlučuje što će Caldera dalje učiniti.

Korisnik na početku treba kreirati scenarij zadajući niz koraka, a Caldera zatim izvodi automatski sve korake i to zahvaljujući planeru koji je središnja komponenta Caldere. Planer je temeljen na metodi umjetne inteligencije koja se zove planiranje. Metoda planiranja omogućuje Caldera planeru da odluči sljedeću najbolju akciju na temelju trenutnog znanja o okolini i trenutno dostupnim akcijama. Da bi planer mogao donositi odluke, svaka akcija sastoji se od preduvjeta i posljedica koje donosi. Koraci algoritma po kojem radi planer su:

1. Osvježi stanje okoline
2. Pronađi sve validne akcije
3. Konstruiraj planove koji počinju tim akcijama
4. Pokreni heuristiku da se odredi najbolji plan
5. Izvrši prvu akciju u odabranom planu
6. Ponovi



Slika 5.1 Arhitektura sustava Caldera

Neki od glavnih nedostataka Caldere su da ne emulira napadački poslužitelj (engl. *Command and Control Server*) te da je planer računalno vrlo zahtjevan i ne preporučuje se pokretati Caldera emulacije s više od 20 čvorova.

U potpoglavlju 5.3. bit će prikazan rad s Calderom.

5.1.2. Red Team Automation

Red Team Automation (RTA) [63] je radni okvir koji omogućuje organizacijama testiranje mogućnosti detekcije obrambenih mehanizama na maliciozne radnje. Alat je 2018. godine razvila tvrtka Endgame koja se bavi razvojem alata za zaštitu krajnjih točaka (engl. *Endpoint*) kao što su stolna i prijenosna računala i mobilni uređaji.

Alat je izgrađen na temelju ATT&CK modela, a nastao je u svrhu popunjavanja nedostataka koje ima ATT&CK model. ATT&CK pruža raznovrstan popis tehnika, ali problem je da napadač može pojedinu tehniku izvršiti na više načina, što braniteljima predstavlja problem u smislu razumijevanja količine mogućnosti, a i vremenskih mogućnosti. RTA se sastoji od 38 Python skripti i potpornih izvršnih datoteka potrebnih za izvršavanje više od 50 tehnika iz ATT&CK modela, koje pružaju dobru podlogu za testiranje i generiranje realističnih malicioznih artefakta. RTA je namijenjen za testiranje primarno na Windows operacijskom sustavu te neke skripte koriste potporne izvršne datoteke za uspješno izvođenje.

Primjer tehnika koje RTA podržava su:

- Korištenje predinstaliranih alata za skidanje malicioznih udaljenih programa
- Izvršavanje razni anti-forenzičkih tehnika
- Kreiranje raznih metoda ustrajnosti za maliciozne programe

U ispisu 5.1. dan je primjer skripte RTA alata koja koristi predinstalirani alat *wevtutil.exe* na Windows operacijskom sustavu sa svrhom brisanja sigurnosnih, aplikacijskih i sistemskih zapisa.

Ispis 5.1 Primjer skripte RTA alata

```
# Name: Clearing Windows Event Logs
# rta: wevutil_log_clear.py
# ATT&CK: T1070
# Description: Uses the native Windows Event utility to clear
the Security, Application and System event logs.
import time
import common
def main():
    common.log("Clearing Windows Event Logs", "!")
    time.sleep(3)
    wevtutil = "wevtutil.exe"
    for log in ["security", "application", "system"]:
        common.execute([wevtutil, "cl", log])
if __name__ == "__main__":
    exit(main())
```

5.1.3. Atomic Red Team

Atomic Red Team [64] je alat koji je 2017. godine razvila tvrtka Red Canary. Kao i RTA alat, zasniva se na ATT&CK modelu. Za razliku od RTA, ovaj alat ne zahtijeva nikakvu instalaciju jer sve tehnike zapisuje u YAML (engl. *YAML Ain't Markup Language*) i korisnik ručno mora pokretati sve tehnike pomoću komandne linije. Sadrži više od 90 tehnika koje su raspoređene na Linux, Windows i macOS operacijske sustave. Atomic Red Team pruža dodatno aplikacijsko programsko sučelje pisano u Ruby programskom jeziku za jednostavnije navigiranje kroz mogućnosti alata ili kreiranje dokumentacije.

U ispisu 5.2 nalazi se primjer YAML datoteke koja opisuje kako doći u posjed privatnih ključeva na Windows operacijskom sustavu. Kao što se može vidjeti YAML datoteka sadrži opis tehnike, koje su podržani operacijski sustavi, i kod koji izvodi tehniku.

Ispis 5.2 Primjer YAML datoteke

```
---
attack_technique: T1145
display_name: Private Keys
atomic_tests:
- name: Private Keys
  description: |
    Find private keys on the Windows file system.
    File extensions include: .key, .pgp, .gpg, .ppk., .p12,
.pem, pfx, .cer, .p7b, .asc
  supported_platforms:
    - windows
  executor:
    name: command_prompt
    command: |
      echo "ATOMICREDTEAM" > %windir%\cert.key
      dir c:\ /b /s .key | findstr /e .key
```

5.1.4. Metta

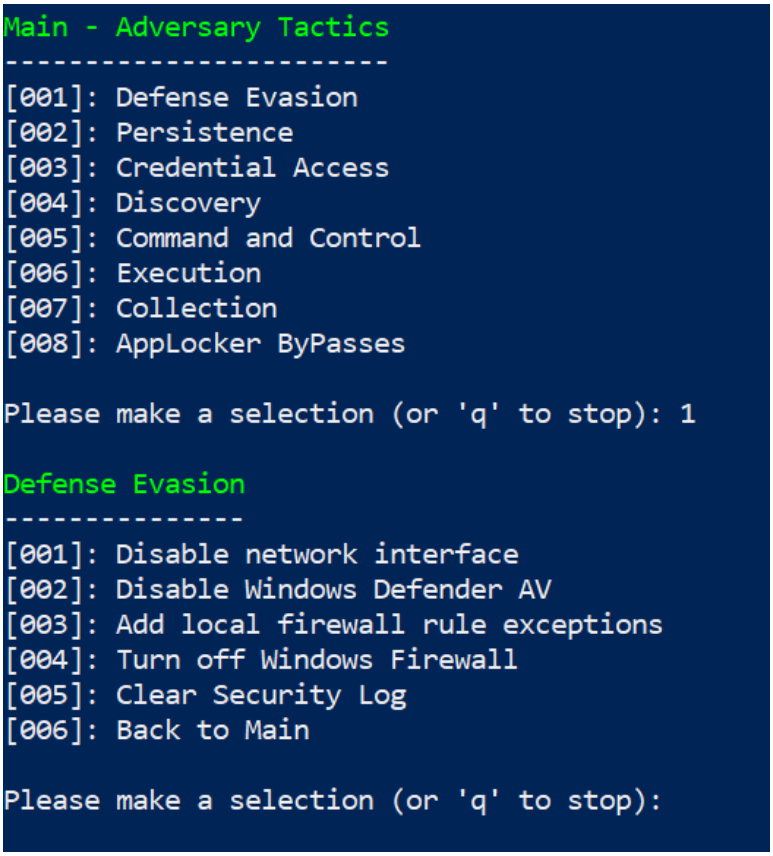
Metta [65] je alat za simulaciju napadača koji se zasniva na ATT&CK modelu, a razvila ga je 2018. godine tvrtka Ubera. Metta koristi Redis/Celery project, Python i Vagrant radni okvir pa je zbog toga dosta kompleksna za instalaciju. Sadrži veliki broj tehnika iz ATT&CK modela koji su raspoređeni na Windows, Linux i macOS operacijske sustave. Izvorni kod je javno dostupan.

Tehnike su spremljene u YAML datoteke kao i kod Atomic Red Team alata, ali su detaljnije opisane. Za razliku od Atomic Red Team alata, Metta ima konfiguracijske YAML datoteke pomoću kojih se mogu opisivati scenariji.

5.1.5. Invoke-Adversary

Invoke-Adversary [66] je PowerShell skripta koja se zasniva na ATT&CK modelu. Alata ne sadrži mogućnost izgradnje scenarija. Ne zahtijeva nikakvu instalaciju i namijenjen je samo za Windows operacijski sustav.

Alat sadrži 8 glavnih skupina taktika: zaobilaženje obrana, ustrajnost, dohvat vjerodajnica, otkrivanje, naredba i kontrola, izvršavanje, sakupljanje i zaobilaženje AppLockera. Izgled sučelja prikazan je na slici 5.2 nakon odabira prve taktike, a to je zaobilaženje obrana.



Slika 5.2 Sučelje alata Invoke-Adversary

5.1.6. Infection Monkey

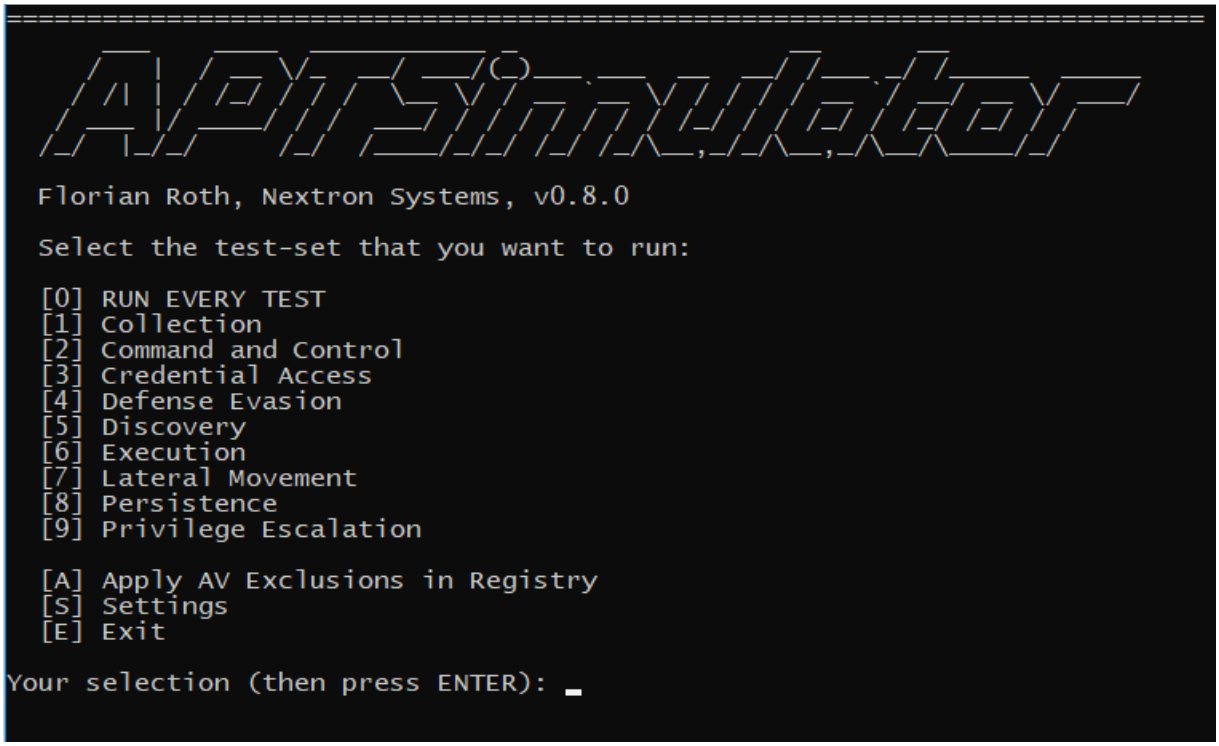
Infection Monkey [67] razvila je 2016. godine GuardiCore tvrtka. Radi se o alatu koji je nastao s ciljem da kombinira najbolje aspekte iz tehnike skeniranja ranjivosti i penetracijskog testiranja. Dobra karakteristika skeniranja ranjivosti je da se na automatizirani način jednostavno može naći veliki broj ranjivosti, a dobra strana penetracijskog testiranja je da može simulirati stvarnog napadača. Problem tehnike skeniranja ranjivosti je da nema mogućnost propagacije i eksploatacije ranjivosti koje nalazi, dok je problem penetracijskog testiranja da je to process kojeg obavlja čovjek. Cilj Infection Monkeya je da automatski radi skeniranje ranjivosti, te da automatski radi propagaciju kroz mrežu. Alat ima mogućnost otkrivanja ranjivosti i eksploatacije istih na Windows i Linux operacijskim sustavima.

Alat se sastoji od dva dijela, Infection Monkey i Monkey Island. Infection Monkey iako je ujedno i ime cijelog alata, u ovom kontekstu je program koji automatski traži ranjivosti i propagira se kroz mrežu, tj. Infection Monkey radi kao i crv (engl. *Worm*) maliciozni program. Infection Monkey koristi razne metode propagacije i eksploatacije. Monkey Island je Web sučelje koje simulira kontrolni i naredbeni poslužitelj s kojim Infection Monkey komunicira, a ujedno služi i za vizualizaciju napretka i podešavanja svih parametara rada Infection Monkeya.

5.1.7. APTSimulator

APTSimulator [69] je skup skripti i izvršnih datoteka za operacijski sustav Windows koje služe za simuliranje kompromitiranog računala. Alat je razvila 2018. godine tvrtka Nextron Systems. Alat služi za testiranje detekcijskih sigurnosnih kontrola i može poslužiti za kreiranje okoline za vježbe digitalne forenzike. Za razliku od nekih prethodnih alata, ovaj alat ne zahtijeva instalaciju i vrlo je jednostavan za korištenje. Velika prednost alata je jednostavno dodavanje vlastitih mogućnosti.

Na slici 5.3 prikazano je početno sučelje programa. Alat nudi 9 taktika koje automatski izvršava: prikupljanje, naredba i kontrola, pristup vjerodajnicama, zaobilaženje obrambenih mehanizama, otkrivanje, izvršavanje, lateralno kretanje, ustrajnost te eskalacija privilegija.



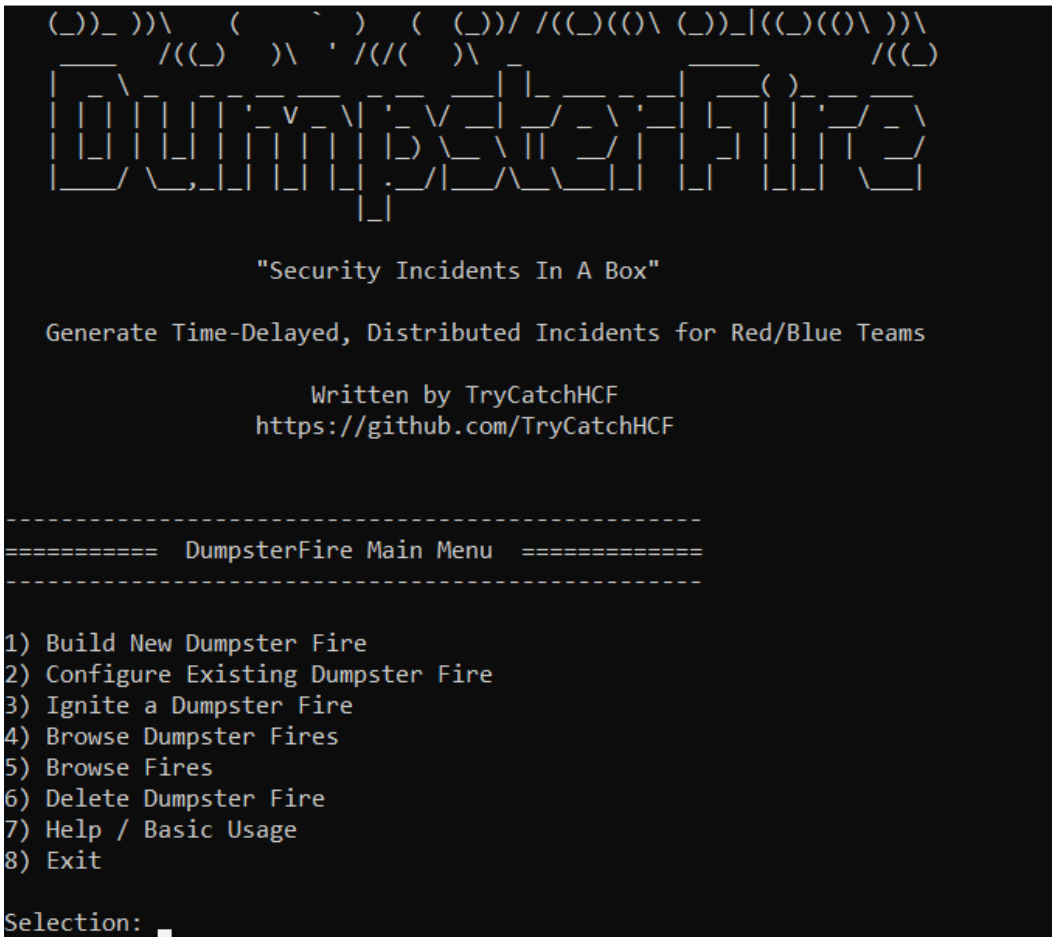
Slika 5.3 Prikaz sučelja APT Simulator alata

5.1.8. DumpsterFire

Dumpsterfire [68] je modularan alat koji služi za izgradnju ponovljivih, vremenski odgođenih i distribuiranih sigurnosnih događaja. Alata je napravljen 2017. godine. Sama ideja alata je da se jednostavno mogu kreirati scenariji napada, s naglaskom da se početak pojedine akcije u

scenariju može vremenski podesiti. Alat je baziran na Python programskom jeziku i moguće ga je koristiti na Windows, Linux i macOS operacijskim sustavima.

Na slici 5.4 nalazi se prikaz početnog sučelja alata.



Slika 5.4 Sučelje alata DumpsterFire

5.2. Usporedba alata

Nakon opisa alata u prošlom potpoglavlju u ovom potpoglavlju alati su uspoređeni po karakteristikama koje mogu omogućiti organizacijama da lakše odaberu alate koji im najbolje odgovaraju. Usporedba se nalazi u tablici 5.1.

Karakteristike po kojima su alati evaluirani su:

- Operacijski sustavi na koje su alati primjenjivi
- Jednostavno instalacije
- Dostupnost dokumentacije

- Model opisan u 3. poglavlju na kojem su bazirani
- Tehnologije i alati na kojima je alat izgrađen

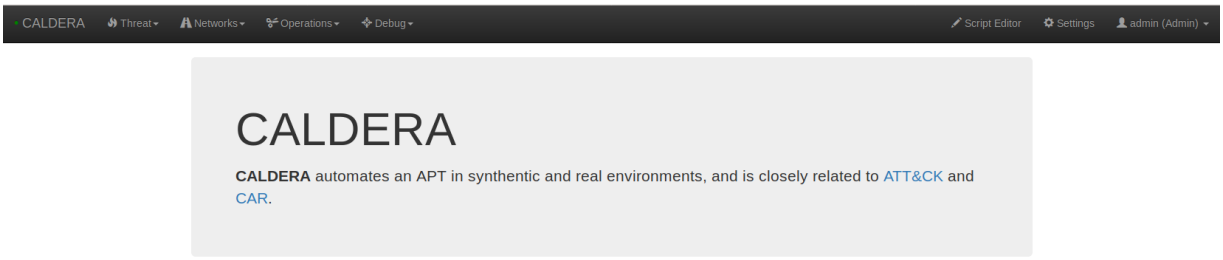
Tablica 5.1 Usporedba alata opisanih u potpoglavlju 5.1.

	Operacijski sustavi	Instalacija	Dokumentacija	Model	Tehnologije
Caldera	Windows	Kompleksna	Vrlo detaljna	ATT&CK	Python, MongoDB, Visual C++, Poslužitelj/Klijent
Red Team Automation	Windows	Minimalna i jednostavna	Minimalna	ATT&CK	Python
Atomic Red Team	Windows, Linux, macOS	Nema instalacije	Vrlo detaljna	ATT&CK	PowerShell, Ruby
Metta	Windows, Linux, macOS	Kompleksna	Minimalna	ATT&CK	Python, Redis, Celery, Vagrant
Invoke-Adversary	Windows	Nema instalacije	Vrlo detaljna	ATT&CK	PowerShell
Infection Monkey	Windows, Linux	Umjereno zahtjevna	Umjereno detaljna	Nema model	Python, Poslužitelj/Klijent
APTSimulator	Windows	Nema instalacije	Vrlo detaljna	Nema model	PowerShell
DumpsterFire	Windows, Linux, macOS	Nema instalacije	Vrlo detaljna	Nema model	Python

5.3. Primjer korištenja alata

U ovom potpoglavlju bit će prikazano korištenje Caldera alata koji je prethodno objašnjen te će ukratko biti objašnjene ostale funkcionalnosti alata. Caldera je namijenjena za korištenje u Windows mrežama, ali zbog nedostatka stvarno okruženja potrebno je stvoriti vlastito laboratorijsko okruženje. Za potrebe demonstracije napravljeno je Windows poslovno okruženje koje se sastoji od Windows Server 2012 R2 poslužitelj i 2 Windows Enterprise 10 računala koji se nalaze na domeni *thesis.net*. Na sva 3 računala instaliran je Caldera klijent za uspješnu komunikaciju s Caldera poslužiteljem koji je instaliran na Ubuntu 18.04 računalu. Cijela mreža postavljena je unutar VMware okruženja.

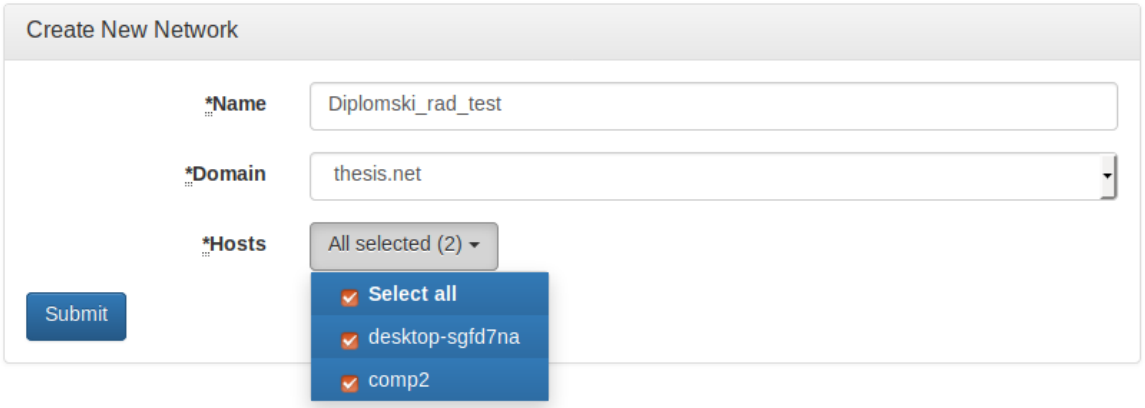
Nakon uspješnog prijavljivanja na Caldera server prikazuje se početno sučelje alata. Na slici 5.5 prikaza prikazano je početno sučelje alata koje se sastoji od 4 glavne sekcije: *Threat, Networks, Operations* i *Debug*. Postoje i 3 pomoćne sekcije: *Script Editor, Settings* i *admin (Admin),* ali one se neće detaljnije objašnjavati jer nisu relevantne za uspješno izvođenje emulacije napadača. U nastavku će detaljnije biti objašnjene sve 4 glavne sekcije i njihove podsekcije pomoću primjera izvođenja emulacije napadača na kreiranoj laboratorijskoj mreži.



Slika 5.5 Početno sučelje alata Caldera

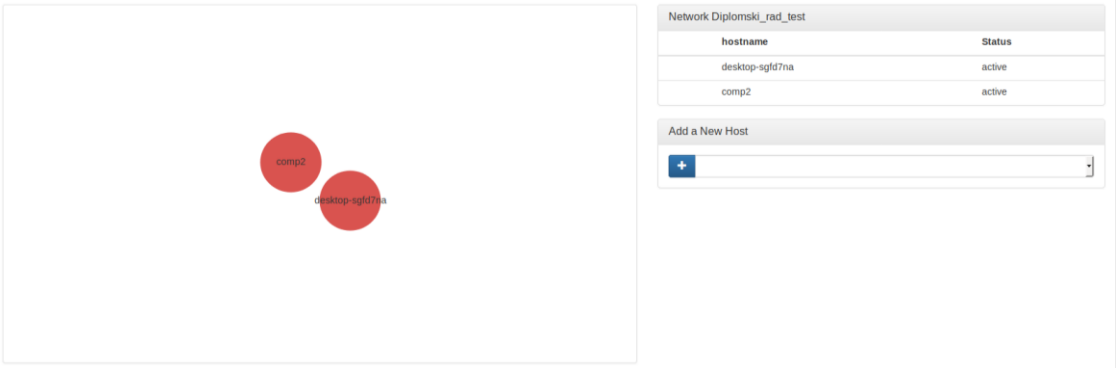
Debug sekcija Caldera alata prva je koja se koristi tijekom procesa izvođenja emulacije napadača jer nam omogućava provjeru konekcije između alata i računala koji se žele testirati. U *Debug* sekciji mogu se pronaći sva računala koja su spojeni s Caldera poslužiteljem te se pomoću naredbenog retka mogu izvoditi naredbe na pojedinim računalima.

Nakon uspješne provjere povezanosti svih željenih sustava s Caldera poslužiteljem potrebno je stvoriti mrežu računala na kojoj će Caldera izvoditi emulaciju napadača, a za tu primjenu služi upravo *Network* sekcija. Sekcija se sastoji od podsekcije *Create Network* i *View networks*. U *Create Network* podsekciji odabire se ime mreže koja će biti napadnuta te koja će sve računala biti u toj mreži. Na slici 5.6 nalazi se prikaz kreiranja mreže pod imenom Diplomski_rad_test, na domeni thesis.net koja uključuje dva računala desktop-sgfd7na i comp2.



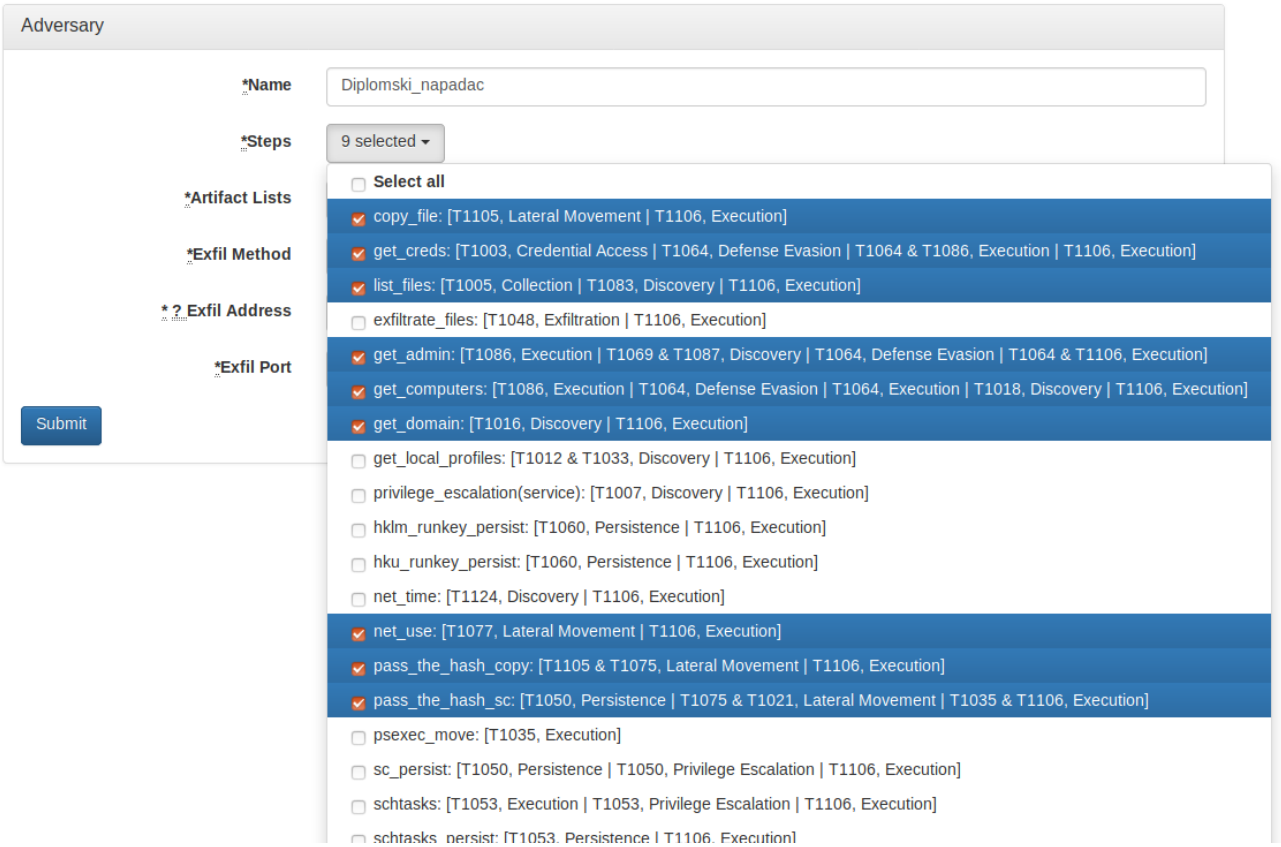
Slika 5.6 Kreiranje mreže

Nakon kreiranja mreže pojavljuje se vizualni prikaz mreže u drugoj podsekciji *View networks*. Na slici 5.7 vizualno su prikazana dva računala, njihov status i mogućnost dodavanja novih računala.



Slika 5.7 Vizualni prikaz mreže

Nakon uspješnog kreiranja mreže, potrebno je kreirati napadača i njegove akcije u obliku scenarija. To se radi pod sekcijom Threat. Sekcija Threat se sastoji od podsekcija *ATT&CK Matrix, View Steps, View Adverseries, Create Adversary, View Artifact Lists* i *Create Artifact List*. U ATT&CK Matrix podsekciji nalazi se cijela matrica ATT&CK modela i zelenom su bojom izražene tehnike koje Caldera alat podržava. *View Steps* sekcija detaljnije pojašnjava svaku tehniku koju Caldera podržava te kako su tehnike logički povezane međusobno. Profil napadača i sam scenarij napada kreira se u podsekciji *Create Adversary*. Na slici 5.8 prikazano je sučelje za kreiranje profila napadača. Za uspješno kreiranje profila potrebno je odabrati ime napadača i tehnike koje će Caldera koristiti. Za potrebe demonstracije odabrano je ime Diplomski_napadac, a odabrane tehnike prikazane su na slici 5.8.

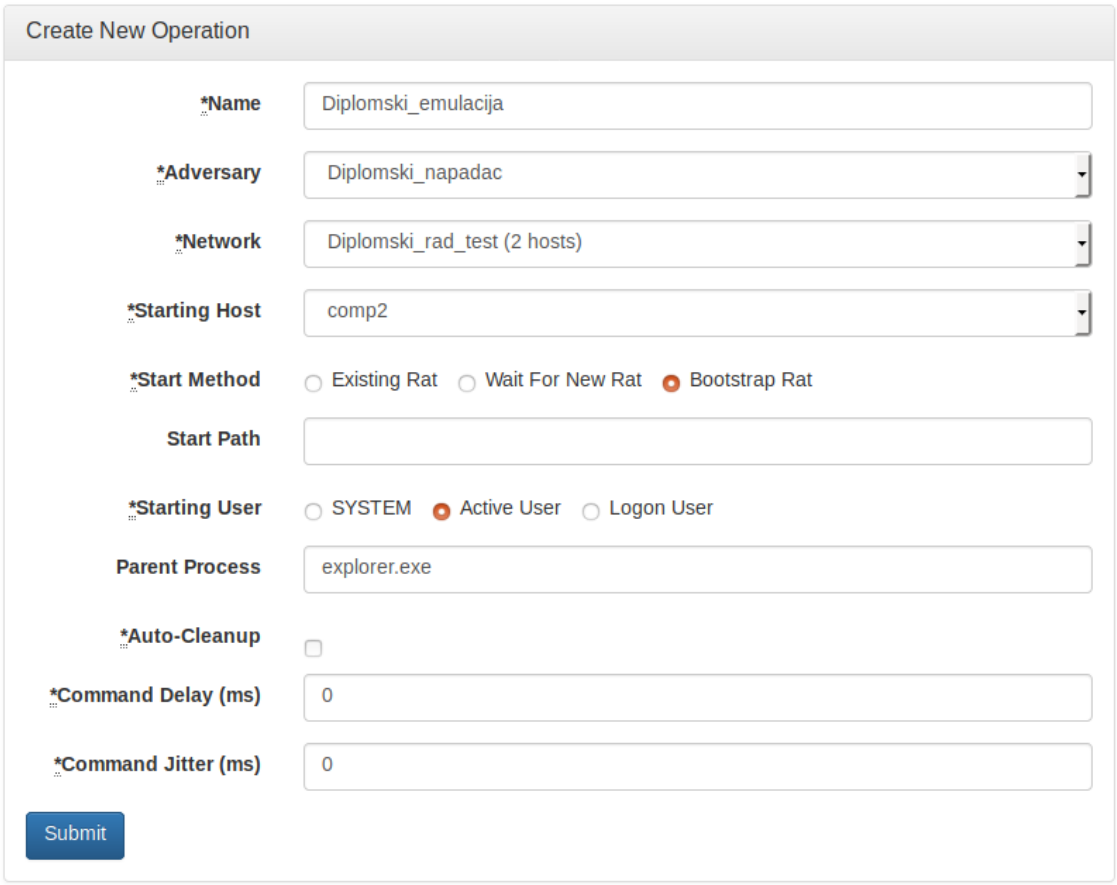


Slika 5.8 Odabir tehnika

Dodatno, prilikom kreiranja napadača moguće je odrediti parameter eksfiltracije kao što su IP adresa i pristupna točka na koji će se eksfiltracija obavljati te tehnika kojom će se obavljati. Također, moguće je odabrati način na koji će Caldera imenovati artefakte koje ostavlja na računalima koje napada. Iako Caldera ima pretpostavljene nazive u *Create Artifact List* podsekciji, moguće je kreirati vlastita imena za artefakte. Primjer artefakta za koji se može promijeniti ime je izvršna datoteka koju Caldera kopira s poslužitelja na računalo koje napada u sklopu neke tehnike. Mijenjanje naziva artefakata korisno je za testiranje sigurnosnih mehanizama koji rade provjeru na temelju imena izvršne datoteke. Sva vlastita kreirana imena artefakata mogu se vidjeti u podsekciji *View Artifact Lists*. Nakon uspješnog odabira svih parametara profila napadača nakon kreiranja profil se može vidjeti u podsekciji *View Adverseries*. Potrebno je napomenuti da Caldera dolazi s nekoliko predefiniranih profila napadača.

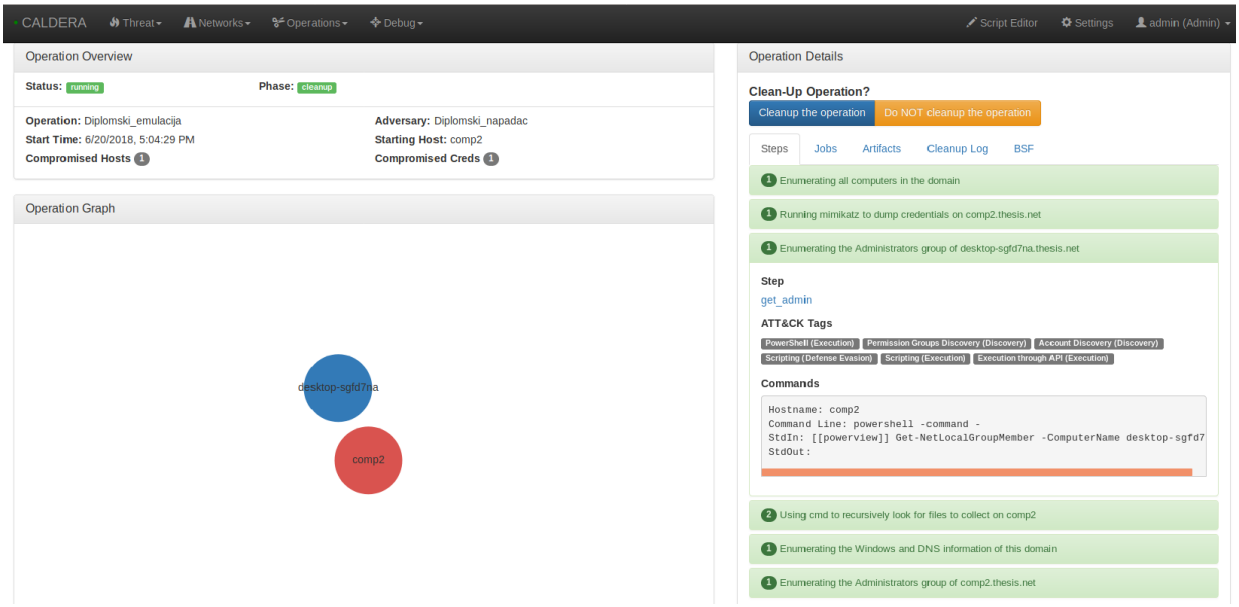
Nakon uspješnog kreiranja mreže i profila napadača potrebno je pokrenuti emulaciju. To se radi u sekciji *Operations*, preciznije u njezinoj podsekciji *Create Operation*. Za pokretanje emulacije potrebno je odrediti ime emulacije, profil napadača koji će se koristiti, mreža na kojoj će se emulacija izvoditi, početno računalo koje će Caldera pokušati kompromitirati za daljnju

propagaciju kroz mrežu, u kojem kontekstu će Caldera koristiti alat za udaljeni pristup i hoće li Caldera počistiti sve artefakte odmah nakon završetka emulacije. Na slici 5.9 prikazano je sučelje nakon odabira svih potrebnih parametara. Emulacija je nazvana Diplomski_emulacija, početno računalo koje će se probati kompromitirati je comp2, alat za udaljeni pristup će se izvoditi u kontekstu trenutno prijavljenog korisnika te Caldera neće brisati artefakte koje stvori.



Slika 5.9 Postavke prije pokretanja emulacije

Nakon odabira i potvrde svih željenih parametara, emulacija se automatski pokreće. Na slici 5.10 prikazano je sučelje koje sadrži dinamički prikaz trenutne emulacije. U središtu sučelja je graf koji prikazuje mrežu. Svako računalo predstavljeno je kao jedan čvor, a svaki čvor može biti bijele, plave ili crvene boje. Bijela boja označava da emulirani napadač još ne zna za postojanje tog računala, plava boja označava da napadač zna za računalo, ali ga nije još uspio kompromitirati, a crvena boja označava kompromitirano računalo. Na desnoj strani nalazi se popis svih koraka koje je napadač radio te pritiskom na određeni korak mogu se vidjeti detaljniji podaci što je točno radio.



Slika 5.10 Prikaz sučelja tijekom emulacije

Caldera emulirani napadač je na kraju uspješno kompromitirao sva računala na mreži. Alat se pokazao kao dobar način za testiranje sigurnosnih mehanizama protiv tehnika naprednih napadača te je intuitivan za korištenje. Potrebno je naglasiti da Caldera emulira rad napadača samo nakon inicijalne kompromitacije. Trenutni glavni nedostaci Caldere su da ne podržava sve tehnike iz ATT&CK modela te da radi samo na Windows mrežama, ali alat se aktivno održava i unapređuje pa je za očekivati da bi se ti nedostaci u budućnosti mogli riješiti.

6. Zaključak

U ovom radu dan je pregled najpoznatijih metoda za modeliranje napadača i pomoćnih modela te klasifikacija koje mogu povećati ekspresivnost modela napadača. Također, uz pomoć modela opisani su neki od najpoznatijih napada koji su se dogodili u stvarnom svijetu. Na kraju je dan pregled i evaluacija alata za emulaciju naprednih napadača koji se baziraju na ranije opisanim modelima, a koji služe kako bi organizacije mogle testirati svoje sigurnosne mehanizme. Kao primjer, kako bi organizacija mogla iskoristiti alate za emuliranje napadača, postavljeno je laboratorijsko okruženje i testiran je Caldera alat.

Modeliranje napadača relativno je nova tehnika u kibernetičkom svijetu koja može organizacijama omogućiti da se uspješno obrane od naprednih ustrajnih prijetnji. Međutim, danas se modeliranje napadača svodi većinom na ručni posao analitičara. Zbog velike količine napada i raznovrsnosti napadača potrebno je proces modeliranja automatizirati što je više moguće. Nadalje, potrebno je istražiti kako se te metode mogu integrirati u sigurnosne obrambene mehanizme i time poboljšati njihove trenutne nedostatke. Također, potrebno je istražiti kako znanje dobiveno tehnikom modeliranja napadača može poboljšati alate za emulaciju napadača, sa svrhom automatizacije procesa traženja i eksploatacije ranjivosti.

7. Literatura

[1] *History of the Internet*, Wikipedia - the free encyclopedia, https://en.wikipedia.org/wiki/History_of_the_Internet, 01.06.2018.

[2] Online Trust Alliance, *Cyber Incident& Breach Trends Report - Review and analysis of 2017 cyber incidents, trends and key issues to address*, The Internet Society (ISOC), 2018.

[3] *Why the Internet Is Vulnerable*, http://www.softheap.com/internet/why-the-internet-is-vulnerable.html, 01.06.2018.

[4] *Where does cybercrime come from? The origin & evolution of cybercrime*, LeVPN, https://www.le-vpn.com/history-cyber-crime-origin-evolution/, 01.06.2018

[5] A. Bochman, *Internet Insecurity*, Harvard Business Review, https://hbr.org/cover-story/2018/05/internet-insecurity, 10.06.2018.

[6] ENISA, *Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends*, ENISA, 2018.

[7] *What is an 'Asset',* Investopedia, https://www.investopedia.com/terms/a/asset.asp, 01.06.2018.

[8] NIST, *Glossary of Key Information Security Terms (NISTRI 7298)*, NIST, 2013.

[9] Shirey, Robert W. *"Internet security glossary, version 2."* (2007).

[10] *Glossary – NIST Computer Security Resource Center*, https://csrc.nist.gov/glossary, 05.06.2018.

[11] *Cybersecurity Fundamentals Glossary*, ISACA, http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf, 05.06.2018.

[12] L. Neely, *2017 Threat Landscape Survey: Users on the Front Line*, SANS Institute, 2017., https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910, 05.06.2018.

[13] EUROPLO, *Internet Organised Crime Threat Assessment (IOCTA) 2017*, EUROPOL, 2017.

[14] M. Bernier, *Military Activities and Cyber Effects (MACE) Taxonomy*, DRDC CORA TM 2013-226, 2013.

[15] *Types of Cyber Attackers and their Motivations*, Breacher Report, http://blog.ss8.com/types-of-cyber-attackers-and-their-motivations/, 08.06.2018

[16] de Bruijne, Mark, et al. *"Towards a new cyber threat actor typology."* Delft University of Technology (2017).

[17] *Proactive Defense: Understanding the 4 Main Threat Actor Types*, Recorded Future, https://www.recordedfuture.com/threat-actor-types/, 08.06.2018.

[18] R. Stoyanov, *Russian financial cybercrime: how it works*, SecureList, https://securelist.com/russian-financial-cybercrime-how-it-works/72782/, 09.06.2018.

[19] S. Northcutt, *Creating a Threat Profile for Your Organization*, SANS Institute, 2014.

[20] M. Loman, *The rise of nation state attacks – with intelligence gathering the aim*, SC Media UK, https://www.scmagazineuk.com/the-rise-of-nation-state-attacks--with-intelligence-gathering-the-aim/article/661661/, 16.06.2018.

[21] D. Bodeau, R. Graubart, *Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment*, MITRE, 2013.

[22] *Kill chain*, Wikipedia - the free encyclopedia, https://en.wikipedia.org/wiki/Kill_chain, 06.06.2018.

[23] Yadav, Tarun, and Arvind Mallari Rao. *"Technical aspects of cyber kill chain."* International Symposium on Security in Computing and Communication. Springer, Cham, 2015.

[24] *Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform*, Lockheed Martin Corporation, 2015.

[25] *Gaining The Advantage: Applying Cyber Kill Chain Methodology to Network Defense*, Lockheed Martin Corporation, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf, 10.06.2018.

[26] G. Engel, *Deconstructing The Cyber Kill Chain*, DARKReading, https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542, 10.06.2018.

[27] *Cyber Kill Chain II: Weponization*, Paradise Solutions Technology, https://psoltech.com/cyber-kill-chain-ii-weaponization/, 10.06.2018.

[28] Jym, *A survey of Attack Life-Cycle Models*, Medium, https://medium.com/@jym/a-survey-of-attack-life-cycle-models-8bd04557af72, 10.06.2018.

[29] Z. Bu, *Zero-Day Attacks are not the same as Zero-Day Vulnerabilities*, Fireeye, https://www.fireeye.com/blog/executive-perspective/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html, 10.06.2018.

[30] J. Aldridge, *Remediating Targeted-threat Instrusions*, Mandiant, BlackHat US, 2012.

[31] M. Laliberte, *A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack*, DARKReading, https://www.darkreading.com/attacks-breaches/a-twist-on-

the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952, 10.06.2018.

[32] P. Pols, *The Unified Kill Chain: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks*, Cyber Security Academy (CSA), 2017.

[33] J. Espenscheid, A. Gunn, *Threat Genomics*, Microsoft Trustworthy Computing, 2012.

[34] *Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)*, MITRE, https://attack.mitre.org/wiki/Main_Page, 25.05.2018.

[35] S. Caltagirone, *The Diamond Model of Intrusion Analysis - A Summary*, 2013.

[36] Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. *The diamond model of intrusion analysis*. CENTER FOR CYBER INTELLIGENCE ANALYSIS AND THREAT RESEARCH HANOVER MD, 2013.

[37] B. Schneier, *Attack Trees*, Schneier on Security, https://www.schneier.com/academic/archives/1999/12/attack_trees.html, 20.04.2018.

[38] *Attack tree*, Wikipedia - the free encyclopedia, https://en.wikipedia.org/wiki/Attack_tree, 20.04.2018.

[39] T. Ingoldsby, *Attack tree analysis*, Red Team Journal, https://redteamjournal.com/2009/01/attack-tree-analysis/, 22.04.2018.

[40] *What Are Attack Trees?*, Amenaza, https://www.amenaza.com/AT-whatAre.php, 22.04.2018.

[41] Pieters, Wolter, et al. *"TREsPASS: plug-and-play attacker profiles for security risk analysis."* IEEE Security & Privacy poster abstracts (2014).

[42] M. Dekker, *Using attack trees in #cybersecurity for threat and risk modeling*, Linkedin, https://www.linkedin.com/pulse/20140529230342-18705719-using-attack-trees-in-cybersecurity-for-threat-and-risk-modeling, 25.04.2018.

[43] Jhawar, Ravi, Karim Lounis, and Sjouke Mauw. *"A Stochastic Framework for Quantitative Analysis of Attack-Defense Trees."* International Workshop on Security and Trust Management. Springer, Cham, 2016.

[44] Kordy, Barbara, et al. *"Attack–defense trees and two-player binary zero-sum extensive form games are equivalent."* International Conference on Decision and Game Theory for Security. Springer, Berlin, Heidelberg, 2010.

[45] Hong, Jin B., and Dong Seong Kim. *"Performance analysis of scalable attack representation models."* IFIP International Information Security Conference. Springer, Berlin, Heidelberg, 2013.

[46] McDermott, James P. *"Attack net penetration testing."* Proceedings of the 2000 workshop on New security paradigms. ACM, 2001.

[47] Chen, Thomas M., Juan Carlos Sanchez-Aarnoutse, and John Buford. *"Petri net modeling of cyber-physical attacks on smart grid."* IEEE Transactions on Smart Grid 2.4 (2011): 741-749.

[48] D. Bianco, *The Pyramid of Pain*, Enterprise Detection & Response, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html, 15.05.2018.

[49] *Common Attack Pattern Enumeration and Classification (CAPEC)*, MITRE, https://capec.mitre.org/about/index.html, 16.05.2018.

[50] Barnum, Sean, and Amit Sethi. *"Attack patterns as a knowledge resource for building secure software."* OMG Software Assurance Workshop: Cigital. 2007.

[51] L. Franceschi-Bicchierai, *Who Hacked The Lights In Ukraine*, Motherboard, https://motherboard.vice.com/en_us/article/9a38jy/who-hacked-the-lights-in-ukraine, 04.06.2018.

[52] Case, Defense Use. *"Analysis of the cyber attack on the Ukrainian power grid."* Electricity Information Sharing and Analysis Center (E-ISAC) (2016).

[53] K. Zetter, *Inside the cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 04.06.2018.

[54] A. Shehod, *Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecruity Implications of Smart Grid Advancements in the US*, CISL MIT, 2016.

[55] S. Vijay, H. Hoikka, B. Kenneth, *Ukraine 2015 Power Grid Cyber Attack: ELEC-E7470 Cybersecruity L – Case Study*, 2017.

[56] *Target Corporation*, Wikipedia - the free encyclopedia https://en.wikipedia.org/wiki/Target_Corporation, 07.06.2018.

[57] *The Untold Story of the Target Attack: Step by Step*, Aorta Labs, 2014.

[58] R. Hackett, *How much do data breaches cost big companies? Shockingly little*, Fortune, http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/, 09.06.2018.

[59] Breach, Target Data. *"A "Kill Chain" Analysis of the 2013 Target Data Breach."*, (2014)., http://faculty.uml.edu/jyurcak/44.115/documents/20140325TargetKillChainAnalysis_SenateReport.pdf, 07.06.2018.

[60] *OWASP Top 10 2017*, https://www.owasp.org/index.php/Top_10-2017_Top_10, 01.06.2018.

[61] *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, US-CERT, 2012

[62] *Caldera*, https://github.com/mitre/caldera, 16.06.2018.

[63] *Red Team Automation*, https://github.com/endgameinc/RTA, 16.06.2018.

[64] *Atomic Red Team*, https://github.com/redcanaryco/atomic-red-team, 16.06.2018.

[65] *Metta*, https://github.com/uber-common/metta, 16.06.2018.

[66] *Invoke-Adversary*, https://github.com/CyberMonitor/Invoke-Adversary, 16.06.2018.

[67] *Infection Monkey*, https://github.com/guardicore/monkey, 16.06.2018.

[68] *DumpsterFire*, https://github.com/TryCatchHCF/DumpsterFire, 16.06.2018.

[69] *APTSimulator*, https://github.com/NextronSystems/APTSimulator, 16.06.2018.

[70] Kaspersky Lab Daily, *Lurk: Seek and destroy*, https://www.kaspersky.com/blog/bye-bye-lurk/12862/, 02.06.2018.

[71] *Angry IP scanner*, https://angryip.org/, 15.06.2018.

Sažetak

Naslov rada: Modeliranje ponašanja napadača na Internetu prije i tijekom provođenja napada

Sažetak: Napredne ustrajne prijetnje danas su veliki sigurnosni problem organizacijama. Da bi se organizacije uspješno obranile od takve vrste napadača potrebno je pratiti i detaljno analizirati njihovo djelovanje. U ovom radu opisana je tehnika modeliranje napadača koja može pomoći u praćenju djelovanja napadača na efikasan, efektivan i strukturiran način. Opisani su najpoznatiji modeli, te je dan primjer korištenja modela na primjerima napada koji su se dogodili u stvarnom svijetu. Također dan je pregled i evaluacija alata za emulaciju napadača koji se temelje na tim modelima, te je prikazan rad s Caldera alatom. Na kraju je dan prijedlog mogućih daljnjih smjerova istraživanja.

Ključne riječi: Modeliranje napadača, Napredne ustrajne prijetnje, Kibernetički lanac prekidanja, Dijamantni model, Stablo napada, Emulacija napadača

Abstract

Title: Modeling attackers on the Internet before and during attack execution

Summary: Advance persistent threats are a major cybersecurity problem for organizations. For successful defense against these attackers organizations need to analyze every action they made in detail. In this thesis technique called attack modeling is described to help organizations to effectively, efficiently and in structured manner represent actions that an attacker makes. Most famous and widely used models are described, and some models are used to describe famous attacks that happen in the real world. Also given is an overview and evaluation of tools used for attack emulation, that are based on previously described models, and in more depth is shown how to use Caldera tool. At the end possible further research directions are discussed.

Keywords: Attack modeling, Advance persistent threat, Cyber kill chain, Diamond model, Attack tree, Attack emulation