SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1077

ODREĐIVANJE ULAGANJA I DOBITI NAPADAČA U PROVOĐENJU NAPADA

Ivor Baričević

Zagreb, lipanj 2023.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 1077

ODREĐIVANJE ULAGANJA I DOBITI NAPADAČA U PROVOĐENJU NAPADA

Ivor Baričević

Zagreb, lipanj 2023.

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 10. ožujka 2023.

ZAVRŠNI ZADATAK br. 1077

Pristupnik: **Ivor Baričević (0036530642)**

Studij: Elektrotehnika i informacijska tehnologija i Računarstvo

Modul: Računarstvo

Mentor: izv. prof. dr. sc. Stjepan Groš

Zadatak: **Određivanje ulaganja i dobiti napadača u provođenje napada**

Opis zadatka:

Tijekom i nakon kibernetičkog napada napadači moraju trošiti određene resurse kako bi proveli napad. Količina utrošenih resursa i dobiti određuje hoće li napadač započeti napad te hoće li ga provesti do kraja. Jako je malo poznate literature koja se bavi tim pitanjem budući da su obično ponašanja napadača slabo dokumentirana u odnosu na ponašanja branitelja. Zahvaljujući načinu kako se u CCS-u provode napadi postoji mogućnost preciznijeg određivanja koliko napadači mogu uložite te koju dobit će imati. U sklopu završnog rada potrebno je uzeti model neke generičke organizacije te u toj organizaciji definirati što je moguće više mjesta na kojima napadač troši resurse. Ta mjesta ulaganje je potrebno ugraditi u model napadače te potom simulirati napad i obranu i odrediti ulaganje i dobit napadača korištenjem simulatora CCS. Citirati korištenu literaturu i navesti dobivenu pomoć.

Rok za predaju rada: 9. lipnja 2023.

Sadržaj

1. Uvod

U današnjem digitalnom dobu, sigurnost informacija je postala ključna u održavanju stabilnosti i uspjeha organizacija. Međutim, dok se intenzivno usmjerava na jačanje obrambenih sustava, često se zanemaruje razumijevanje perspektive napadača. Unatoč činjenici da je ulaganje napadača u provođenju kibernetičkog napada neophodno za razumijevanje šire slike informacijske sigurnosti, ovaj aspekt je relativno slabo istražen u akademskoj literaturi.

Računalni napadi često su motivirani financijskom dobiti. Financijska dobit predstavlja razliku između prihoda i uloženog novca. Ako je moguće odrediti financijsku dobit napada, može se procijeniti vjerojatnost njegove realizacije. Veća financijska dobit podiže vjerojatnost napada, i obrnuto. Određivanje troška napada predstavlja iznimno izazovan problem, s obzirom na mnoštvo načina na koje napad može biti proveden.

Trošak napadača se može procijeniti s relativnom točnošću samo ako se posjeduje popis svih korištenih resursa tijekom napada. Informacije o djelovanju napadačkih organizacija su, zbog njihove prikrivene prirode, rijetko javno dostupne. Zahvaljujući alatu za simulaciju kibernetičkih napada, *Cyber Conflict Simlatoru*-u (u nastavku CCS), postoji mogućnost proučavanja svih resursa koje napadači koriste prilikom napada.

Cilj ovog rada je pratiti tijek napada na organizaciju i identificirati sve resurse koje su napadači koristili kako bi mogla biti određena isplativost takvog napada. Za simulaciju će biti korišten CCS, alat specifično dizajniran za modeliranje i simuliranje kibernetičkih napada.

Rad je organiziran na sljedeći način. U drugom poglavlju opisana je napadačka organizacija i metodologija mjerenja troška unutar CCS-a. U trećem poglavlju je predstavljena skripta koja će asistirati u procjeni troška i prihoda napadača na segmentima koje CCS ne pokriva. U četvrtom poglavlju je procijenjena dobit napadača u odabranom scenariju. Peto poglavlje obuhvaća zaključak na temelju prethodno prikazanih rezultata i analiza. Šesto poglavlje predstavlja popis korištene literature, pružajući detaljan uvid u reference koje su korištene za potporu istraživanju.

2. Napadačka organizacija unutar CCS-a

CCS je program koji omogućava simulaciju računalnog napada na određenu organizaciju. Njegova glavna svrha je održavanje kibernetičkih vježbi u kojima se simuliraju uvjeti sličnim onima u slučaju napada. Tako se timovi zaduženi za obranu kibernetičkih sustava mogu uvježbati prije nego što se dogodi stvarni napad. U određenoj vježbi sudjeluju dva tima – napadači i branitelji. Vježba se održava preko poligona koji je izrađen tako da što podrobnije opisuje sustav koji se koristi u produkciji. CCS se sastoji od dva dijela. Prvi dio je *Simulator* u kojem se simulacija pokreće i kontrolira. Drugi dio je *Editor* u kojemu se stvaraju topologije organizacija koje sudjeluju u simulaciji. Detaljniji opis CCS alata je dostupan u [3].

2.1. Napadačka organizacija i njeni resursi

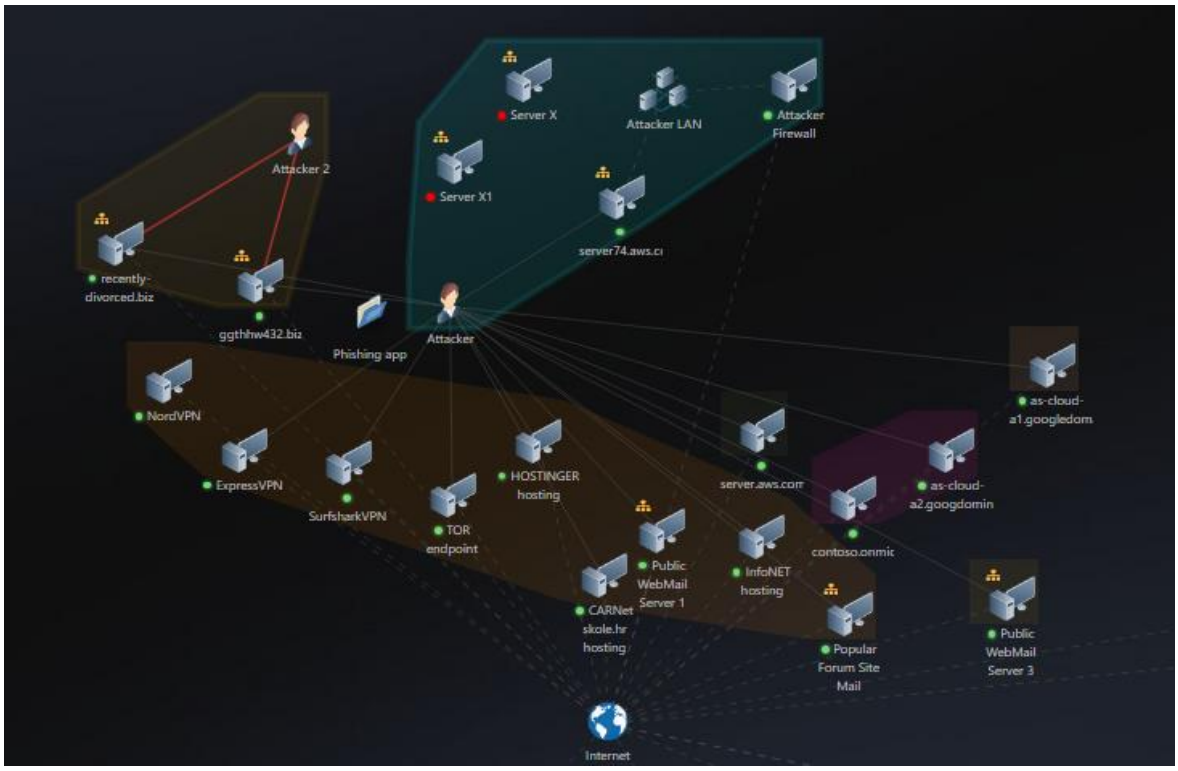
Cjelokupna napadačka infrastruktura je prikazana na slici 2.1. Infrastrukturu čini mnoštvo objekata s vlastitim atributima koji su predefinirani u *Editoru* prije početka same simulacije. Svi objekti koji se nalaze na istoj fizičkoj lokaciji su okruženi „poljem“ iste boje. Sa slike 2.1 se može uočiti da napadačku organizaciju čine dva napadača koji nisu na istom fizičkom prostoru. Oba napadača u svojem vlasništvu posjeduju poslužitelje koje prilikom napada mogu koristiti za razne napadačke aktivnosti. Na svakom od poslužitelja se nalaze zlonamjerne datoteke i maliciozni programi. Napadači tijekom napada mogu koristiti i umrežene usluge poput usluga mrežnog posluživanja, virtualnih privatnih mreža (u nastavku VPN), usluga u oblaku, elektroničke pošte i *The Union Router* uslugu (u nastavku TOR). Napadači imaju pristup internetu.

Poslužitelji, programi, datoteke te dostupne umrežene usluge čine sve resurse koje napadačka organizacija može koristiti prilikom napada unutar CCS-a. Napadačku organizaciju čine dva napadača – *Attacker 1* i *Attacker 2*. *Attacker 1* je na slici 2.1 označen unutar svijetlo plavog polja, a *Attacker 2* unutar smeđeg polja. Napadačka organizacija je gledana iz perspektive *Attackera 1*, tako da se svi ostali napadači koji sudjeluju s njime u napadu računaju kao vanjski ljudski resursi.

Ukupni trošak napada treba biti precizno izračunat kako bi se dobila realna slika mogućeg gubitka. U tom kontekstu, neefikasno je i potencijalno konfuzno ubrajati troškove svih resursa koje napadači mogu koristiti. Umjesto toga, potrebno se usredotočiti na troškove onih resursa koji su eksplicitno korišteni tijekom napada.

Razlozi za ovo su višestruki:

- Točnost procjene
    - Izračunavanjem troškova samo onih resursa koji se koriste tijekom napada dobiva se preciznija procjena potencijalnog financijskog utjecaja. To može biti ključno za planiranje i implementaciju sigurnosnih mjera.
- Specifičnost napada
    - Svaki napad je jedinstven, i resursi potrebni za izvođenje jednog napada mogu se značajno razlikovati od onih potrebnih za drugi. Uključivanje svih mogućih resursa može dovesti do prevelikih procjena troškova.
- Efikasnost u planiranju
    - Ukoliko se u izračun ukupnog troška napada uključe samo resursi koji su direktno iskorišteni, to može omogućiti bolje razumijevanje točnih područja na koja bi se trebalo usredotočiti pri planiranju i provedbi sigurnosnih mjera.
- Jednostavnost i praktičnost
    - Ograničavanjem izračuna na resurse koji su eksplicitno korišteni tijekom napada, proces izračuna troškova je znatno jednostavniji i praktičniji.



Slika 2.1 Prikaz napadačke infrastrukture u *Editoru*

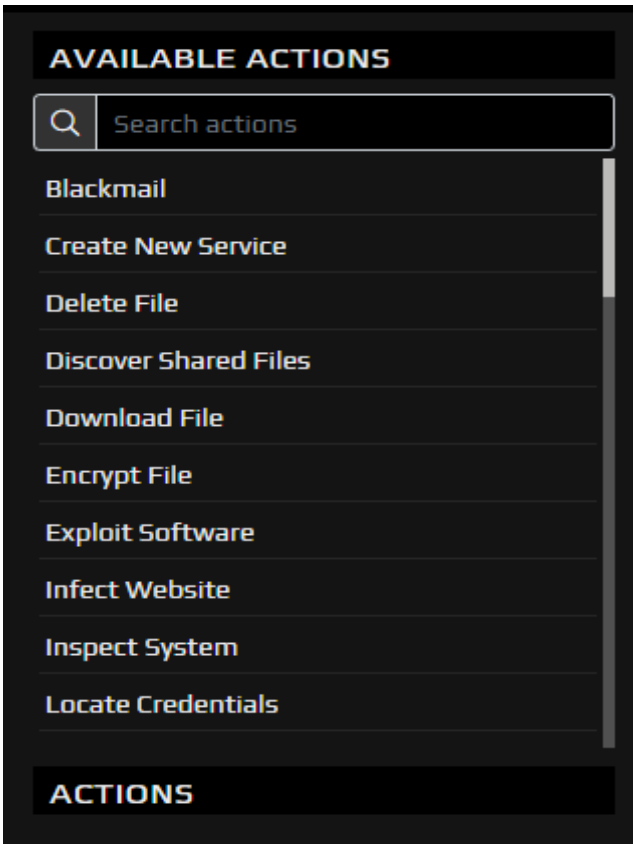
2.2. Napadačke akcije i dnevnik akcija

Svaka od organizacija ima popis akcija koje su im na raspolaganju za djelovanje. Neke od tipičnih akcija su *Turn Machine On*, *Download File*, *Run Software*, *Logout* i *Upload file*.

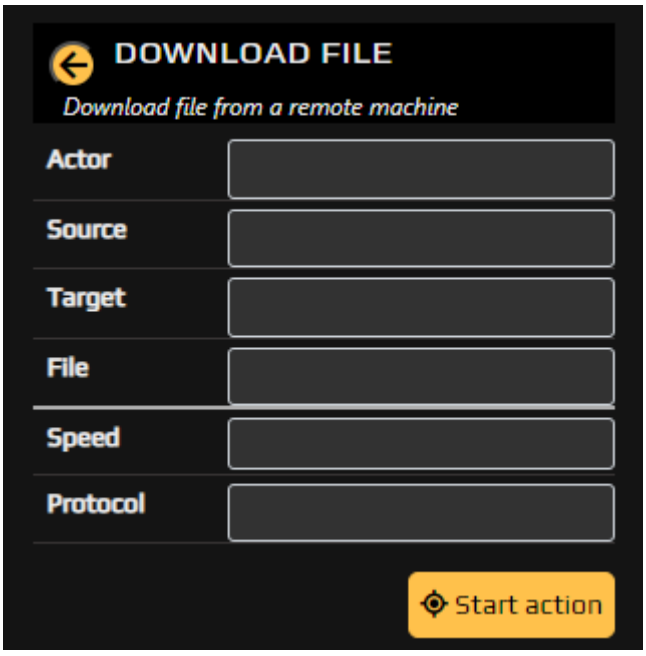
Na slici 2.2 je vidljiv prikaz nekih akcija koje napadači mogu pokrenuti u određenom trenutku simulacije. To znači da imaju ispunjene uvjete da ih pokrenu. Na primjer, ako napadači nemaju na nekom od dostupnih računala upaljen program s funkcionalnošću krađe podataka, ne mogu pokrenuti akciju *Begin Keylogging*.

Svaka akcija ima određene parametre koje napadači moraju odabrati. Na slici 2.3 su vidljivi parametri za akciju *Download File*. Kako bi napadači mogli izvesti navedenu akciju moraju izabrati izvršitelja radnje, računalo s kojeg datoteku žele preuzeti, računalo na koje ju žele preuzeti, samu datoteku, brzinu preuzimanja te protokol.

Kroz izvršavanje akcija, napadači stječu resurse koji im omogućuju da poduzmu nove radnje. Na primjer, ako su saznali za nekoliko adresa elektroničke pošte obrambene organizacije te unutar napadačke infrastrukture postoji datoteka s metodom iskorištavanja, mogu pokrenuti akciju *Create Spearphishing Mail with Exploit*.



Slika 2.2 Neke od mogućih akcije napadača prilikom napada



Slika 2.3 Parametri za akciju *Download File*

CCS pruža funkcionalnost snimanja radnji tijekom provođenja simulacije. U simulatoru se može kliknuti na gumb s natpisom *Open sequence dialog* te izabrati jedan od scenarija za kojeg se želi vidjeti snimljene akcije. Snimljeni scenarij se može pokrenuti. Po završetku

scenarija, moguće je kliknuti na opciju *Download Scenario Review* koja se nalazi u postavkama, točnije unutar prozora *Settings*. Pritiskom na gumb, na korisnikovo računalo je preuzeta *Excel* datoteka s dvije stranice. Na prvoj stranici *Chronology* su prikazane sve akcije te njihovi parametri. Mogu se vidjeti i određeni zapisi koji pobliže opisuju samu akciju.

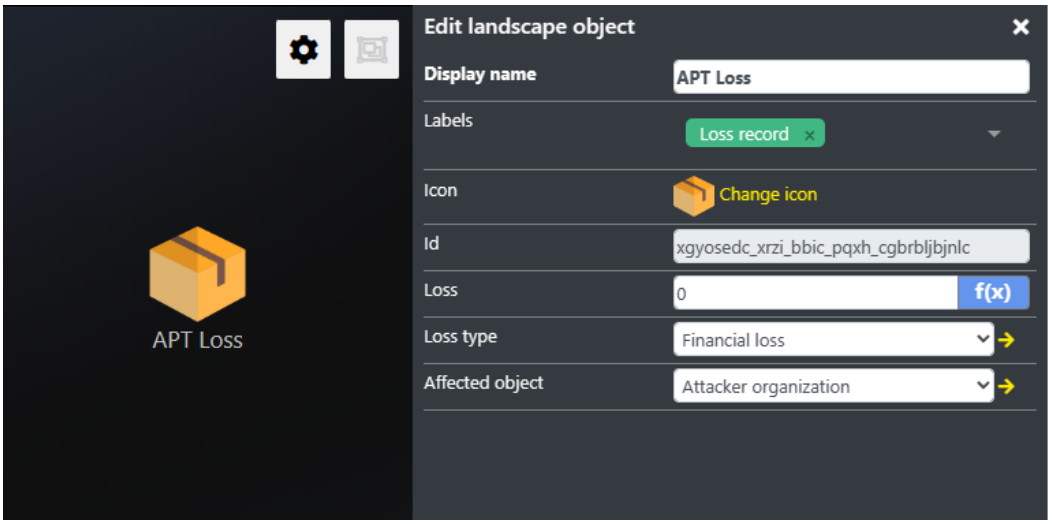
Na drugoj stranici *Indicators* su prikazane informacije o određenim parametrima koji su se mjerili tijekom simulacije. Jedan od njih je *Financial Loss – IT* koji mjeri ekonomski trošak IT podgrupe obrambene organizacije (Slika 2.3).

Time/Data	Financial Loss - IT (€)
01.07 08:00	100000
01.07 09:00	1700000
01.07 10:00	2900000
01.07 11:30	4200000
01.07 12:30	5500000
01.07 13:30	6600000
01.07 14:30	7800000
01.07 16:00	9000000
01.07 17:00	10000000
01.07 18:00	11100000
01.07 19:00	12400000

Slika 2.3 Primjer prikaza štete IT grupe u dnevniku zapisa

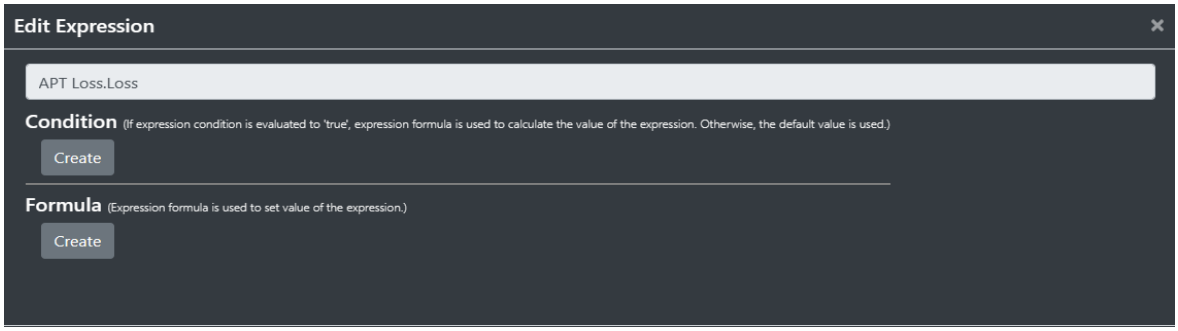
2.2 Mogućnost ekonomske procjene napada u CCS-u

Kako bi izračun troška bio moguć, CCS nudi mogućnost kreiranja objekata koji računaju i spremaju trošak. Ti objekti trebaju biti stvoreni u *Editoru* prije početka simulacije klikom na gumb *New Item*. Pritiskom na gumb se otvara novi prozor koji zahtijeva da se za novostvoreni objekt odabere oznaka. Oznaka objekta za praćenje štete je *Loss Record*. Nakon definiranja oznake, potrebno je definirati i ostale atribute vezane za *Loss Record*. Kao *Loss type* se izabire *Financial loss*, a kao *Affected object* organizacija za koju se želi računati trošak. *Financial loss* je objekt koji predstavlja vrstu troška. Za potrebe rada će biti stvoren objekt *APT Loss* koji će mjeriti trošak napadača (Slika 2.4).



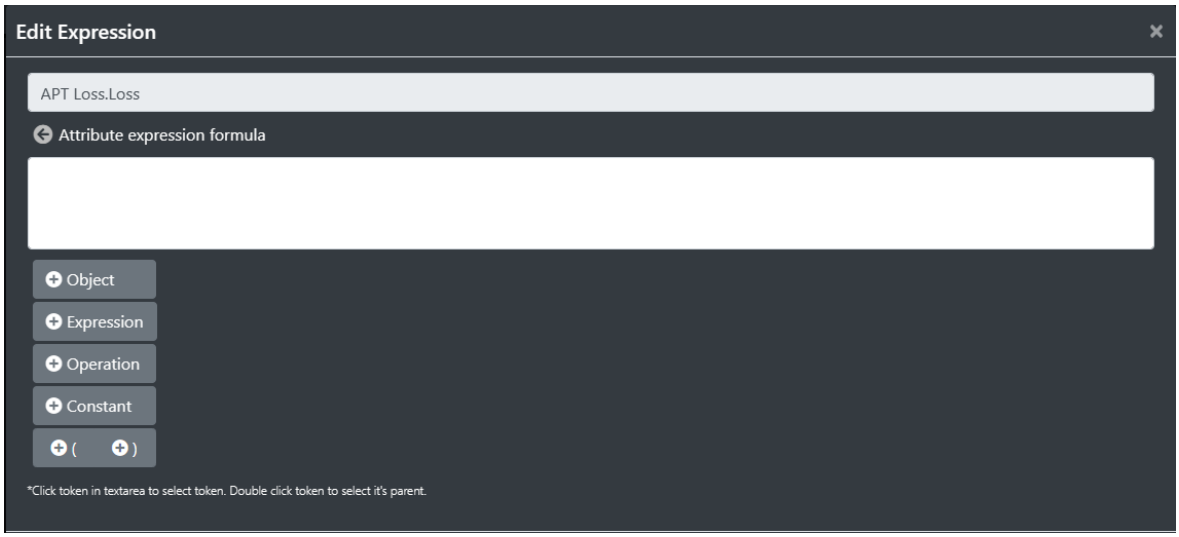
Slika 2.4 Prikaz objekta *Apt Loss* i njegovih parametara

Najbitniji atribut je *Loss* u kojemu se može definirati formula kojom će biti računat trošak. Klikom na gumb *f(x)* pokraj *Loss* atributa otvara se prozor (Slika 2.5). U tom prozoru postoji opcija koja omogućuje definiranje uvjeta kako bi se primijenila formula za izračun štete samo ako su ispunjeni određeni uvjeti. Ako uvjet nije definiran, formula će biti primijenjena za izračun štete tijekom simulacije.



Slika 2.5 Prozor koji se otvori klikom na f(x) gumb

Klikom na gumb *Create* ispod natpisa *Formula* na slici 2.5 otvoren je prozor u kojem se definira sama formula kao što je prikazano na slici 2.6. Formule se opisuju pomoću objekata, njihovih atributa, osnovnih računskih operacija, konstanti, zagrada i izraza. Neki od izraza su *PathExists* koji vraća *True* ako su dva objekta mrežno povezana, *Accumulator* koji svake sekunde zbraja određenu vrijednost u odabranu varijablu i *Iif* koji predstavlja uvjetno grananje.



Slika 2.6 Prozor za upis formule

Izrazi mogu biti korisni prilikom određivanja troškova obrambene organizacije, ali njihova upotrebljivost u izračunu troškova napadača je ograničena. Izračunavanje troškova napadača zahtijeva određivanje trenutaka kada napadači koriste specifične resurse, a to je informacija koju izrazi ne mogu pružiti.

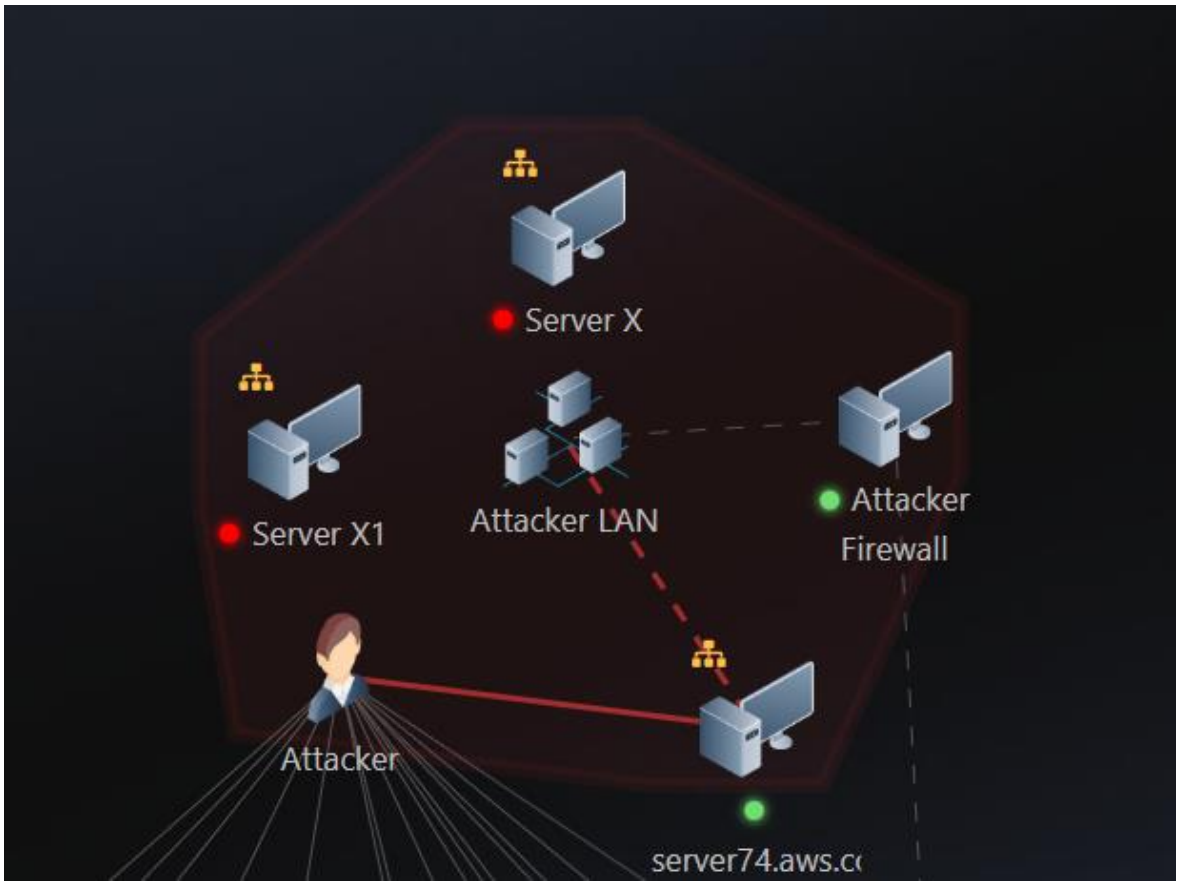
Tablicom 2.7 je pružen popis te kratko objašnjenje svih dostupnih izraza u CCS-u. Među njima, izraz *PathExits* može biti djelomično koristan, ali prisutnost mrežne veze između napadača i određene umrežene usluge u CCS-u ne implicira nužno da napadač koristi tu uslugu, već samo da mu je usluga dostupna tijekom napada. Ovaj rad se koncentrira na resurse koje napadači stvarno koriste tijekom napada, a ne na one koje bi potencijalno mogli koristiti. Za svaki resurs koji napadači ne koriste prilikom napada je pretpostavljeno da ne postoji te njegov trošak neće biti uzet u obzir.

Jedina relevantna informacija za izračun troška napadača, koju formule mogu pružiti, odnosi se na poslužitelje koje napadači koriste, konkretno one unutar svoje fizičke lokacije. Na slici 2.8 je prikazana fizička zona u kojoj se *Attacker 1* nalazi, uključujući sve uređaje unutar te zone. Svaki uređaj sa slike 2.8 ima atribut *Is on*, koji označava je li uključen. Prethodno simulaciji, u *Editoru* se mogu isključiti svi poslužitelji. Ako napadaču bude potreban određeni poslužitelj tijekom napada, on će ga uključiti. Ako napadač aktivira poslužitelj tijekom napada, može se zaključiti da ga koristi, te će trošak upotrebe poslužitelja biti pridodan ukupnom trošku napada.

Ime	Opis
PathExists	Checks if the path exists between start node and end node. Returns boolean.
Round	Rounds the value to specified number of decimals.
RandFunction	Returns random double in respect to the given range value.
Min	Returns the smaller of ther two values given.
Max	Returns the larger of the two values given.
Inject	Triggers inject for organization with specified message.
IsAvailablefor	Checks if the file is available for organization. Includes checking if organization has a key to decrypt the file if it's encrypted.
Accumulator	Calculates the new value by adding value val*time to accumulated.
Availabilty	Checks availability of the object if it exists. Return double.
isServiceActive	Checks if the current time is within given working hours.
businessServiceLoss	Calculates generic loss for business service. Takes into account its availability level and whether it should be working according to worktime schedule.
TotalOrganizationLoss	Returns the sum of all losses mapped on an organization or its business service of given loss type.
Iif	Inline if – if condition is true returns trueValue, else falseValue.
Fit	Fits the value into given range.

Tablica 2.7 Popis svih izraza pomoću kojih se može definirati formula troška

Dodatno, formule ne nude uvid u potencijalni prihod napadača. U kontekstu CCS-a, jedini scenariji kojima napadači mogu ostvariti dobit uključuju prodaju kompromitiranih podataka ili pristanak obrambene organizacije na njihovu ucjenu. Formule ne sadrže logičku strukturu koja bi potvrdila da su se spomenute radnje odvile tijekom simulacije.



Slika 2.8 Fizička zona *Attackera 1*

2.3 Formula za procjenu troška napada

Budući da iz formula može biti zaključeno koje poslužitelje unutar vlastite fizičke zone napadači koriste, potrebno je napraviti formulu koja će za svaki korišteni poslužitelj pribrajati potrebni trošak u ukupni trošak napada. Sav trošak će računati prethodno kreirani *APT Loss* objekt.

Troškovi vezani za korištenje vlastitog poslužitelja su sljedeći:

- cijena poslužitelja
- cijena operacijskog sustava (u nastavku OS)
- cijena struje

- cijena interneta
- cijena domene

Za izradu formule će se koristiti izrazi *Accumulate* i *Iif* te atribut *Is on*. Trošak struje, interneta i domene treba biti pridodan ukupnom trošku svakog mjeseca, no jedini izraz kojim trošak može biti dodan s obzirom na vrijeme *je Accumulate*. Izraz *Accumulate* svake sekunde pribraja određen iznos u ukupan trošak, stoga će se mjesečne cijene morati izraziti u cijeni po sekundi. Atribut *Is On* vraća *True* ako je uređaj uključen i *False* ako nije. On će se koristiti u kombinaciji s *Iif* izrazom kako bi se trošak pridodao samo kada je uređaj uključen.

Formula (1) predstavlja formulu za izračun troškova struje i domene za poslužitelje unutar fizičke zone napadača. Funkcija *Accumulate* nadgleda status poslužitelja (da li je upaljen ili ne), a ukoliko je poslužitelj uključen, dodaje trošak struje i domene u *Loss* atribut objekta *APT Loss*. Varijabla *Poslužitelj* predstavlja ime poslužitelja za kojeg se računa trošak, varijabla *cijenaStrujePoSekundi* cijenu struje po sekundi u zemlji u kojoj se poslužitelj nalazi, a *cijenaDomenePoSekundi* cijenu korištenja domene izraženu u cijeni po sekundi.

Accumulate (Apt Loss.Loss, If (Poslužitelj.Is on (cijenaStrujePoSekundi
+ cijenaDomenePoSekundi, 0), time) (1)

Formula (2) opisuje formulu koja u ukupni trošak dodaje cijenu poslužitelja i OS-a ovisno o tome je li poslužitelj upaljen. Varijabla *Poslužitelj* predstavlja ime poslužitelja za kojeg se računa trošak, varijabla *cijenaPoslužitelja* tržišnu cijenu samog poslužitelja, a *cijenaOS-a* tržišnu cijenu OS-a.

Iif (Poslužitelj.Is on, cijenaPoslužitelja + cijenaOS-a, 0) (2)

Formula (3) opisuje općenitu formulu koja će u trošak dodati cijenu interneta ako napadač koristi barem jedan od poslužitelja unutar svoje fizičke zone. *Poslužitelj 1, Poslužitelj 2 i Poslužitelj 3* su varijable koje predstavljaju sve poslužitelje unutar iste fizičke zone.

Accumulate (Apt Loss.Loss, Iif (Poslužitelj 1. Is on or Poslužitelj 2. Is on
orPoslužitelj3. Is on, cijenaInternetaPoSekundi, 0), time) (3)

U CCS-u tehničke specifikacije poslužitelja nisu eksplicitno navedene, stoga će za procjenu biti korištena pretpostavka da konfiguracija poslužitelja, koje napadači koriste, odgovara minimalnim konfiguracijama primjenjivima u poslovnom okruženju. Prema informacijama dostupnim u [4], uobičajena cijena takvog poslužitelja iznosi 1718 $.

U CCS-u su veoma oskudno navedene vrste i verzije OS-a koje poslužitelji koriste. Za neke poslužitelje piše vrsta OS-a, a ne piše verzija, dok za ostale ne piše ni jedno ni drugo. Stoga je prepostavljeno da svi poslužitelji napadačke organizacije koriste *Linux* OS [18]. *Linux* je besplatan OS, tako da je trošak OS-a poslužitelja jednak nuli.

U pogledu troškova interneta i struje, bitno je razmotriti geografsku lokaciju napadača. *Attacker 1,* zajedno s njegovim uređajima, smješten je u Brazilu, stoga se prosječne brazilske cijene primjenjuju na trošak interneta i struje koji njegovi uređaji koriste. Prosječna mjesečna cijena interneta u Brazilu iznosi 20 $ [5], dok je cijena kilovat-sata (u nastavku kWh) struje u Brazilu 0.17 $ [6]. S druge strane, *Attacker 2* se nalazi u Rusiji, pa se troškovi interneta i struje za njega izračunavaju temeljem prosječnih ruskih cijena. U Rusiji, prosječna mjesečna cijena interneta je 6.77 $ [11], dok prosječna cijena kWh struje iznosi 0.063 $ [12].

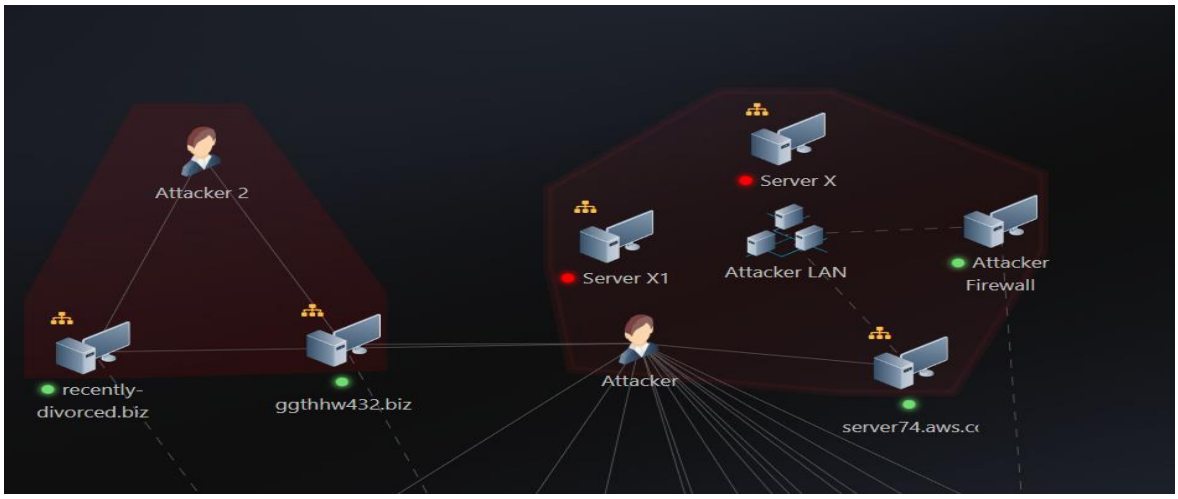
Ako se koristi podatak da prosječni poslužitelj godišnje potroši 1900 kWh [7], za poslužitelj u Rusiji mjesečna cijena struje iznosi 9.98 $, a za poslužitelj u Brazilu 27 $.

Što se tiče cijene domene, nađen je podatak da tipična cijena domene na jednom od najvećih registara internet domena na svijetu košta 2 do 20 $ godišnje [19]. Kao procjena troška domene je uzeta srednja vrijednost od 10 $ godišnje.

U infrastrukturi *Attackera 1,* prisutan je i vatrozid koji, ako je uključen, također doprinosi ukupnom trošku. U trošak vatrozida ulaze trošak samog uređaja te trošak struje koju koristi. Prema podacima u [8], minimalna cijena vatrozida varira između 700 i 1000 $, pa će za procjenu troška biti primijenjena vrijednost od 850 $. Na internetu je nađen kalkulator [20] koji izračunava trošak struje za vatrozid, ovisno o radnim satima dnevno i cijeni kWh struje. Ukoliko je vatrozid aktivan tijekom napada, pretpostavka je da radi 24 sata dnevno, pa će u kalkulatoru za parametar radnih sati dnevno biti uneseno 24. Ta se pretpostavka temelji na činjenici da napadači često trebaju održavati svoje uređaje aktivnim tijekom noći za komunikaciju sa zaraženim računalima [34]. Cijena kWh struje temelji se na prosječnoj cijeni u Brazilu, koja iznosi 0.17 $. Kalkulator računa vrijednost

od 0.255 $ po satu, što će biti osnova za procjenu troška struje koju vatrozid koristi. S obzirom da vatrozid ne zahtijeva domenu, trošak domene za vatrozid je jednak nuli.

Slika 2.9 prikazuje fizičke zone *Attackera 1* i *Attackera 2*. Za svaki uređaj unutar fizičke zone svakog napadača potrebno je primijeniti formule (1) i (2), dok se za svaku fizičku zonu primjenjuje formula (3). Za procjenu cijena koriste se prethodno navedene vrijednosti čiji je sadržaj dodatno prikazan u tablici 2.12. Cijene prikazane unutar izraza *Accumulate* izražene su kao cijena po sekundi. Sumiranjem svih dobivenih formula i dodavanjem rezultata u formulu ukupnog troška unutar objekta *APT Loss*, rezultira složenom i teško čitljivom formulom. Radi bolje preglednosti, kreirani su posebni objekti koji zasebno izračunavaju trošak za svaki uređaj, kao i objekti koji računaju trošak interneta za obje fizičke zone. Stoga, formula za ukupni trošak sadržava sumu troškova svih ovih novonapravljenih objekata. Formule su dostupne u privitku.

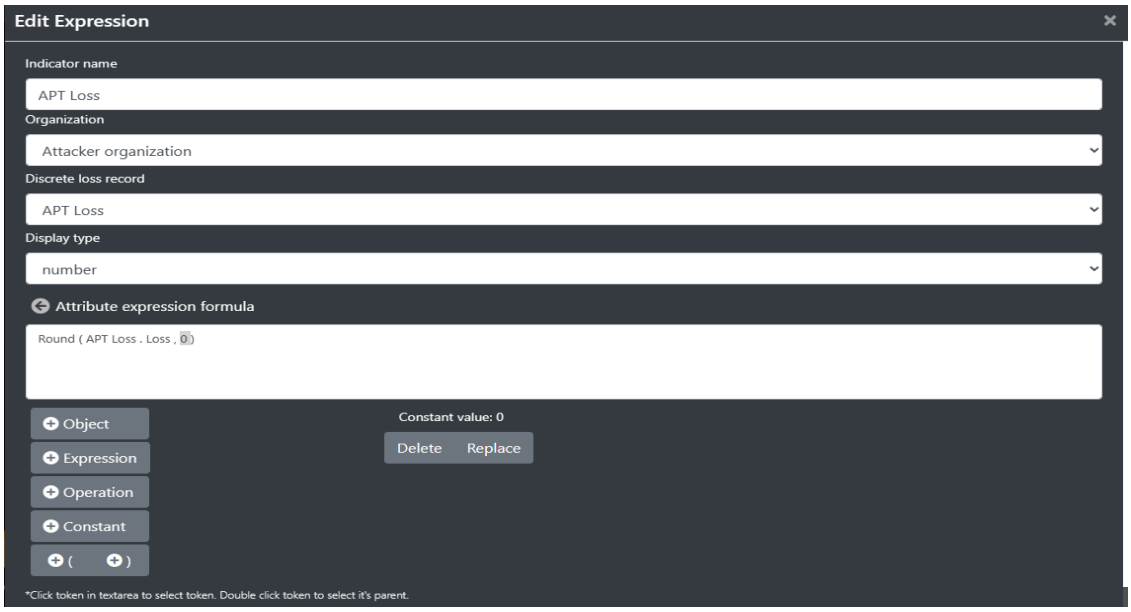


Slika 2.9 Fizičke zone *Attackera* 1 i *Attackera* 2

Preduvjet za ispravan rad formule ukupnog troška je da se u *Editoru* prije napada isključe svi uređaji te da ih napadači uključuju po potrebi. Tako može biti zaključeno koji od uređaja su uistinu potrebni prilikom napada.

Kako bi *Loss* vrijednost *Apt Loss* objekta bila vidljiva na stranici *Indicators* dnevnika akcija, objektu je potrebno pridružiti odgovarajući indikator. Indikatori se stvaraju klikom na gumb *New Indicator* u *Editoru* (Slika 2.10). Na slici 2.11 dan je primjer parametara *Indicator* elementa koji služi za prikaz štete u *APT Loss* objektu. Formula koju je ovdje potrebno upisati je formula koja zaokružuje vrijednost izračunatog gubitka na cijeli broj.

Slika 2.10 Izborna traka u kojoj je gumb *New Indicator* označen crvenom bojom



Slika 2.11 Parametri *APT Loss* indikatora

Trošak	Cijena / $
Trošak struje za poslužitelj u Brazilu po sekundi	$109 * 10^{-7}$
Trošak struje za poslužitelj u Rusiji po sekundi	$38 * 10^{-7}$
Cijena domene po sekundi	$32*10^{-8}$
Cijena interneta po sekundi u Brazilu	$772*10^{-8}$
Cijena interneta po sekundi u Rusiji	$257*10^{-8}$
Fiksna cijena poslužitelja	1718
Fiksna cijena vatrozida	850
Trošak struje za vatrozid u Brazilu po sekundi	$708*10^{-7}$
Fiksna cijena OS-a	0

Tablica 2.12 Troškovi rada uređaja unutar fizičke zone napadača

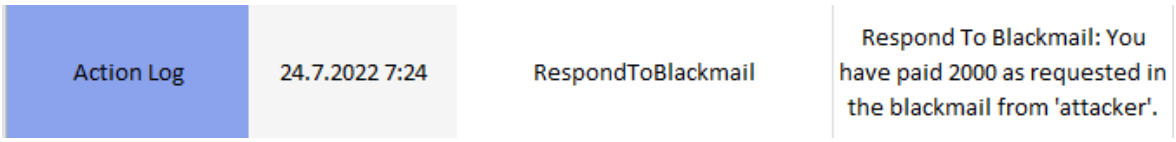
3. Skripta za računanje troška i dobiti

U prethodnom poglavlju identificirana su značajna ograničenja u CCS formulama prilikom izračunavanja troškova i dobiti napadača. Formule ne omogućavaju zaključivanje o programima, datotekama i mrežnim uslugama koje napadači koriste tijekom napada. Kada je riječ o prihodu, nemoguće je utvrditi kada su napadači prodali podatke ili kada je obrambena organizacija prihvatila ucjenu. Srećom, sve te informacije mogu se pronaći u ranije spomenutom dnevniku akcija. Za potrebe pronalaska potrebnih informacija iz dnevnika akcija, izrađena je odgovarajuća skripta u *Pythonu – dobit.py*. Skripta je dostupna u [36] unutar direktorija *Skripta_i_potrebne_datoteke*.

3.1. Način rada skripte

Skripta je dizajnirana da iterira kroz parametre svih akcija unutar dnevnika akcija pri čemu pohranjuje sve resurse iskorištene tijekom izvršenja akcija u listu. Da bi se identificirali parametri akcije koji pripadaju resursima, kreirana je tekstualna datoteka koja sadrži popis svih resursa koje napadači mogu koristiti tijekom napada. Ova datoteka uključuje sve programe, datoteke i mrežne usluge koji se nalaze unutar infrastrukture napadačke organizacije. Trošak uređaja napadačke organizacije računa *Apt Loss* objekt u CCS-u, stoga njihov trošak skripta ne pokriva. Osim praćenja resursa, skripta također broji ukupan broj sati rada za sve napadače koji nisu *Attacker 1*. Popis svih resursa čiji trošak skripta pokriva se nalazi u datoteci *resursi.txt* koja se nalazi u [36] unutar direktorija *Skripta_i_potrebne_datoteke*.

U pogledu dobiti napadača, skripta za svaku akciju provjerava tko je izvršitelj i koja je akcija izvršena. Na ovaj način, skripta može prepoznati kada se izvršava akcija *Sell Data* ili *Respond to Blackmail*. Akcija *Sell Data* kao parametar prima datoteku koja je prodana, omogućavajući skripti da identificira koje je ukradene datoteke napadačka organizacija prodala. Akcija *Respond to Blackmail* ne prima iznos isplate kao parametar, no u dnevniku akcija se nakon prihvaćanja ucjene pojavljuje zapis u kojem je naveden isplaćeni iznos (Slika 3.1). Skripta prepoznaje ovaj zapis i iznos dodaje u ukupni prihod napadača.



Slika 3.1 Dio zapisa o novčanoj zaradi napadača prilikom prihvaćanja ucjene

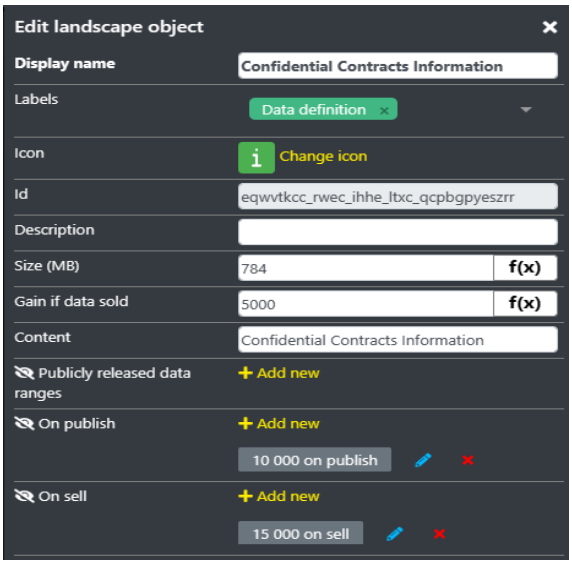
Prolaskom kroz dnevnik akcija skripta je odredila:

- popis svih programa, datoteka i umreženih usluga koji su parametar napadačevih akcija
- ukupan broj sati rada svih napadača osim *Attackera 1*
- sve datoteke obrambene organizacije koje su napadači prodali
- prihod napadača prilikom uspješne ucjene

Kako bi se izračunao ukupni trošak napada, potrebno je odrediti cijenu svakog korištenog resursa. Tako će skripta korištenom resursu pridružiti odgovarajući trošak. Iz tih potreba je napravljena datoteka u kojoj se nalazi popis svih mogućih resursa i odgovarajućih troškova (u nastavku datoteka troškova).

Nekima od korištenih resursa, poput umreženih usluga, nije moguće pridružiti jedinstven trošak. Za izračun njihovog troška je potrebno izračunati vremensko trajanje napada u mjesecima te pomnožiti s mjesečnom cijenom njihove usluge. Iz tog razloga skripta računa i ukupno vremensko trajanje napada u mjesecima. Pretpostavljeno je da napadači korištenu umreženu uslugu plaćaju tijekom čitavog napada.

Dodatno, potrebno je u datoteku troškova unijeti cijenu svake od datoteka koju napadači mogu ukrasti i prodati prilikom simulacije. Tako skripta povezuje ukradene datoteke s njihovom cijenom te cijenu dodaje u prihod napadača. Ovi podaci dostupni su unutar CCS-a i prikazani su kao atribut *Gain if data sold* specifičnog objekta koji detaljno opisuje datoteku. Primjer takvog objekta je *Confidential Contracts Information* (Slika 3.2).



Slika 3.2 *Confidential Contracts Information* objekt

Datoteka troškova *Trošak.xlsx* se nalazi u [36] unutar direktorija *Skripta_i_potrebne_datoteke*. Datoteka sadrži tri lista. Prvi list *MjesecneCijene* sadrži popis svih resursa čiji se trošak mjeri na mjesečnoj bazi te odgovarajuće troškove. Drugi list *Cijene* sadrži popis svih resursa koji imaju fiksni trošak te njihove troškove. Treći list *UkradeniPodaciCijena* sadrži popis datoteka obrambene organizacije koje napadači mogu ukrasti te zaradu koju napadači ostvare ako prodaju bilo koju od tih datoteka.

3.2. Cijene resursa

Za popunjavanje datoteke troškova, potrebno je odrediti cijene svih ostalih resursa koje napadači mogu koristiti. U ovom poglavlju, izvršena je analiza svih programa, datoteka i mrežnih usluga unutar infrastrukture napadača kako bi se procijenili troškovi svake pojedinačne komponente. Za resurse poput zlćudnih programa i metoda za iskorištavanje je pretpostavljeno da su kupljeni jer CCS ne pruža dovoljno detalja da bi se mogao procijeniti trošak izrade samih resursa.

3.2.1. Tehnički resursi

Sve dostupne umrežene usluge vidljive u napadačkoj infrastrukturi su :

- *SurfsharkVPN*
- *NordVPN*
- *ExpressVPN*

- *Hostinger hosting*
- *InfoNet hosting*
- *TOR*
- *Public webmail server 1*
- *Public webmail server 3*
- *Popular forum site mail*
- *Serveraws.com*
- *as-cloud-a2.googdomin.com,*
- *as-cloud-a1.googledomains.com*
- *contoso.onmicrosoft.com*

Mjesečni trošak VPN usluge je dostupan na internetu. Mjesečna cijena *SurfsharkVPN-a* i *ExpressVPN-a* na službenoj stranici iznosi 12.95 $, a *NordVPN-a* 12.99 $ [14][15][16].

Hostinger hosting i *Infonet hosting* napadači koriste za usluge mrežnog posluživanja. *Mrežno posluživanje* je usluga koja pruža prostor na internetu za pohranu web stranica i njihovih podataka, čime se omogućuje njihova dostupnost korisnicima putem interneta [31].

Obje usluge nude više mjesečnih paketa. Za *Hostinger hosting* je odabrana opcija posluživanja do 100 stranica za 4 $ mjesečno kao opcija koju napadač koristi, a za *Infonet Hosting* opcija *multi paket* koja košta 5.84 $ mjesečno [23][24].

Tor i usluge elektroničke pošte su besplatne, tako da resursima *TOR, Public webmail server 1* i *Public webmail server 3* nije pridružen trošak.

Internet stranica *Popular forum site mail* neće imati pridružen trošak, budući da se radi o javno dostupnom resursu.

Serveraws.com, as-cloud-a2.googdomin.com, as-cloud-a1.googdomin.com i *contoso.onmicrosoft.com* su usluge u oblaku. Nađen je podatak da prosječni mjesečni trošak korištenja usluga u oblaku iznosi 313 $ mjesečno, stoga je trošak svih navedenih usluga u oblaku procijenjen tom vrijednošću [9].

Sve metode iskorištavanja dostupne napadačima su:

- *Exploit_Office*
- *Squirel Webmail Exploit*
- *W7_KJFG_Exp_L*
- *W7_MNTR_Exp_R*
- *Cent_OS_6_MDHZ_R*
- *41f0_be*
- *W10_HTZJ_Exp_R*
- *Exploit MFP Linux*
- *W08_19_VSRT_Exp_R*

Kod procjene troškova navedenih metoda iskorištavanja, pretpostavljeno je da nijedna od metoda nije metoda nultog dana. U [36] unutar direktorija *Skripta_i_potrebne_datoteke* se nalazi i datoteka *0dayexploitprices.xlsx* koja obuhvaća procjenu troškova svih navedenih metoda iskorištavanja, uzimajući u obzir mogućnost da je riječ o iskorištavanjima nultog dana. Skripta prima odgovarajući parametar koji označava koju pretpostavku o trošku treba uzeti u obzir - odnosno, da li su korištene metode iskorištavanja metode nultog dana ili ne.

Metoda iskorištavanja *Exploit_Office* cilja na ranjivosti u verzijama *Microsoft Office* programa starijim od 2014, omogućavajući napadaču udaljeni pristup. Postoje dvije usporedive ranjivosti za koje se procjenjuje da trošak njihovih metoda iskorištavanja varira između 0 i 5000 $ [21][22]. Stoga će se za ovu metodu iskorištavanja kao procjena troška uzeti prosječna vrijednost – 2500 $.

Metoda iskorištavanja *Squirell_Webmail Exploit* cilja na ranjivosti unutar SquirrelMail-a, programa koji omogućava korisnicima pregled, slanje i organiziranje e-pošte putem web preglednika. Na internetu je dostupna javno objavljena metoda iskorištavanja s istim funkcionalnostima, zbog čega je trošak ove metode iskorištavanja procjenjen na nulu [25].

Metoda iskorištavanja *W7_KJFG_Exp_L* cilja na ranjivosti unutar operacijskog sustava *Windows*, specifično na verzije manje od 8, omogućujući napadaču udaljeni pristup. Iako slične metode iskorištavanja nisu pronađene na internetu, dostupan je podatak da je prosječna cijena metoda iskorištavanja za *Windows* i mrežne aplikacije na jednoj stranici na crnom tržištu 2540 $ [1]. Na temelju toga, trošak ovog resursa procijenjen je na 2540 $.

Slično tome, trošak metode iskorištavanja *W7_MNTR_Exp_R,* čije su funkcionalnosti identične *W7_KJFG_Exp_L,* također je procijenjen na 2540 $.

Cent_OS_6_MDHZ_R predstavlja metodu iskorištavanja koja cilja na ranjivosti verzija manjih od 6.10 *Centos* OS-a. Na internetu je otkrivena slična metoda iskorištavanja, čija se cijena procjenjuje u rasponu od 0 do 5000 $ [26]. Slijedom navedenog, trošak ovog resursa procijenjen je na 2500 $.

41f0_be predstavlja metodu iskorištavanja koja iskorištavanja ranjivosti unutar *Windows* OS verzije 10 i nižih, s ciljem omogućavanja udaljenog pristupa napadaču. Jedan od primjera metode iskorištavanja koja cilja na ranjivost unutar *Windows* 10 OS-a i omogućava funkcionalnost udaljenog pristupa je CVE-2018-8174 [27]. Ova specifična metoda iskorištavanja se može na crnom tržištu nabaviti za 1600 $ [1].

W10_HTZJ_Exp_R je metoda iskorištavanja koja ima slične funkcionalnosti kao i *41f0_be.* Stoga, trošak ovog resursa je procijenjen na 1600 $.

Exploit MFP Linux je metoda iskorištavanja koja iskorištava ranjivosti multifunkcionalnih printera s *Debian Linux* OS-om. Radi na *Debian Linux 8 i* manjim verzijama te napadaču daje mogućnost udaljenog pristupa. Metoda iskorištavanja sa sličnim funkcionalnostima je CVE-2021-39238 [28]. Njena cijena je između 5 000 $ i 25 000 $, stoga će se pretpostaviti srednja vrijednost od 15 000 $ kao procjena troška za *Exploit MFP Linux* [29].

W08_19_WSRT_Exp_R je metoda iskorištavanja koja iskorištava ranjivost u verzijama manjim od 2020 *Windows Server* OS-a te sadrži funkcionalnost udaljenog pristupa. Na intrenetu nije nađena aproksimacija cijene ovog resursa. Kao procjena cijene ovog resursa je opet uzet podatak o srednjoj cijeni metoda iskorištavanja na stranici na crnom tržištu – 2540 $.

Zloćudni programi koje napadači imaju na raspolaganju u svojoj infrastrukturi su:

- *Application Tools MX01*
- *Application tools MX02*
- *Corel Photo Draw*
- *Irfan View x86*
- *MaIwarebytes Anti-Malware*
- *Advanced Task Manager*

- *Carabalt_tookt*
- *Fast PC Cleaner*
- *Fast PC Cleaner_L*
- *Ultimate Antivirus Free edition*

Svi navedeni programi su zlćudni programi koji imaju relativno slične funkcionalnosti poput krađe podataka, provedbe napada ucjenjivačkim kodom, skeniranja mreže i udaljenog pristupa. Sve njihove funkcionalnosti, osim provedbe napada ucjenjivačkim kodom, pokriva program *Cobalt Strike* [17].

Cobalt Strike predstavlja komercijalni alat za penetracijsko testiranje s namjenom obavljanja probojnih analiza, dizajniran s ciljem emuliranja naprednih ustrajnih prijetnji. Licenca za *Cobalt Strike* se na crnom tržištu procjenjuje na vrijednost između 30 000 i 40 000 $ [1]. Prilikom procjene, svaki od navedenih malicioznih programa će biti zamijenjen *Cobalt Strike* programom, stoga će, kada napadači koriste bilo koji od njih, srednja vrijednost od 35 000 $ biti dodana ukupnom trošku. Ova procjena je poduprta statistikom koja pokazuje da 48% APT grupacija koriste alate za penetracijsko testiranje [1].

Što se tiče zlćudnih programa koji služe za provođenje napada ucjenjivačkim kodom, nađen je podatak da prosječna cijena takvog malicioznog programa na crnom tržištu košta 270 $ [2]. Ako je korišten maliciozni program s tom funkcionalnošću, trošak će biti povećan za 270 $.

Ostale datoteke i programi u napadačkoj infrastrukturi su :

- *Phishing app*
- *CooIinarika.com*
- *Recently-divoreced.biz - app*
- *Mail server app*

Phishing app funkcionalnostima najbliže odgovara *phishing kitu. Phishing kit* skup je softverskih alata, kao što su *HTML,* slike i kod koje prevaranti mogu koristiti za izradu i pokretanje phishing napada [32]. Utvrđeno je da prosječna cijena *phishing kita* na crnom tržištu 2019. godine iznosi 304 dolara [30]. Da bi stranica bila operativna, potrebna je i domena, što dodaje mjesečni trošak od 0.83 dolara na ukupne troškove upotrebe ovog

resursa. Izračun od 0.83 dolara dobiven je dijeljenjem prosječne godišnje cijene domene na *GoDaddy*-u s brojem mjeseci u godini [19].

Coolinarika.com i *recently-divorced.biz-app* su stranice pod kontrolom napadača. Specifični detalji o ovim stranicama nisu navedeni u CCS-u, pa se može pretpostaviti da su u osnovi jednostavne funkcionalnosti. Pretpostavka je da su napadači prekopirali kod već postojećih stranica i napravili minimalne modifikacije, stoga se trošak izrade procjenjuje na nulu. Mjesečni trošak resursa uključivat će 0.83 dolara za domenu.

Mail server softver je aplikacija koja omogućuje primanje, slanje i pohranu pošte preko mreže. S obzirom na dostupnost brojnih otvorenih kodova za ovakve programe [33], pretpostavlja se da je napadač mogao prekopirati i prilagoditi jedan od njih za svoje potrebe, stoga se cijena ovog programa procjenjuje na nulu. Kao i u prethodnim slučajevima, mjesečni trošak resursa uključivat će dodatnih 0.83 $ za domenu.

3.2.2. Ljudski resursi

Kao što je već navedeno, skripta računa broj sati rada svih dodatnih napadača koji sudjeluju u napadu. Za procjenu troška njihovog rada, potrebno je utvrditi vrijednost jednog sata njihovog rada. Ova procjena će se temeljiti na prosječnoj satnici etičkog hakera u SAD-u, koja iznosi 51 $ [10]. Na temelju toga, skripta ukupnom trošku napada dodaje vrijednost dobivenu množenjem broja sati rada ostalih napadača sa 51.

4. Procjena dobiti napadača u scenariju Blackmail

U ovom poglavlju razmotren je scenarij *Blackmail*. Nakon simulacije koristeći CCS i prateću skriptu, određena je ukupna dobit napadača. Scenarij *Blackmail* nalazi se na popisu snimljenih scenarija. Snimljene scenarije moguće je pokrenuti i pregledati prikaz svih poduzetih akcija. Većina akcija unutar scenarija *Blackmail* mogu se vidjeti klikom na zabilježenu sekvencu *2022_Deep_Scenarij01*. Za potrebe ovog rada, scenarij je morao biti nadopunjen izvršavanjem akcija slanja ucjene i prihvaćanja ucjene kako bi skripta mogla prepoznati ostvarenu dobit.

4.1. Radnja scenarija

Proces napada započinje infekcijom stranice koju zaposlenici ciljane organizacije redovito posjećuju. Poslužitelj na kojem se nalazi navedena stranica prethodno je inficiran programom koji napadaču omogućava udaljeni pristup, omogućavajući mu da zarazi samu stranicu koja se poslužuje na zaraženom poslužitelju. Infekcija se izvodi kroz metodu iskorištavanja *41f0_be*.

Nakon infekcije stranice, napadač pokreće aktivnost izviđanja ili *Recon*. *Recon* je proces prikupljanja informacija o ciljanoj organizaciji radi pružanja uvida u njezine karakteristike, slabosti ili potencijalne ranjivosti. Aktivnost uključuje istraživanje, nadzor i prikupljanje podataka kako bi se postavila osnova za daljnje akcije ili napade [35]. Prva akcija *Recon* ima za cilj *TSO Enterprise,* obrambenu organizaciju. Otkriveni su brojni poslovni servisi i zaposlenici organizacije.

Nakon identificiranja zaposlenika, izvedena je dodatna *Recon* aktivnost s radnicima kao metama. Cilj napadača je prikupiti što više informacija o njima, uključujući njihove adrese elektroničke pošte. Nakon što su adrese identificirane, napadač za svakog radnika stvara posebne *spearphishing* poruke s poveznicom na zaraženu stranicu.

Napadač čeka da žrtve otvore poruku i kliknu na poveznicu, omogućavajući mu udaljeni pristup njihovim računalima. Nakon što neki od primatelja otvore poveznicu, napadač stječe udaljeni pristup njihovim računalima. Prva radnja koju napadač izvodi na inficiranim računalima je pregled sustava, uključujući sve datoteke, mrežni promet i aktivne procese.

Nakon toga su na zaražena računala preuzeti maliciozni programi koji mu omogućavaju nove akcije poput skeniranja mreže, krađe podataka i napada ucjenivačkim kodom.

Skeniranje mreže omogućuje napadaču otkrivanje brojnih novih računala i multi funkcionalnog printera. Otkrivanjem ranjivosti na ovim uređajima, napadač preuzima odgovarajuće metode iskorištavanja kako bi zarazio ostala računala.

Na inficiranim računalima otkrivene su bitne datoteke poput *Supervisory Control and Data Acquisition* (u nastavku SCADA) konfiguracijskih datoteka, radnih ugovora i povjerljivih informacija o ugovorima. Navedeni podaci su ukradeni.

Na jednom od zaraženih računala napadač krade pristupne podatke koji mu omogućavaju pristup VPN-u koju koristi organizacija. Nakon spajanja na otkrivenu VPN mrežu, napadač skenira uređaje unutar mreže i otkriva dva SCADA poslužitelja. Skeniranjem otkriva ranjivosti na poslužiteljima i preuzima metode iskorištavanja za SCADA poslužitelje. Zatim pristupa SCADA poslužiteljima i krade bitne SCADA podatke. Na kraju napada, napadač šalje dvije ucjenjivačke poruke obranbenoj organizaciji (Ispis 4.1).

```
Blackmail sa SCADA podacima, „Unfortunately your organization fell
victim of Cyber Attack. For small compensation we are willing to
help you improve your security by revealing what have you done
wrong. This offer ends soon, our software is specially designed to
autodestruct if access to C2 servers is lost.”, amount 500 000.

Blackmail sa Contractima „GDPR penalties are high so decide if you
want to see your data publicly available or you will invest a
little bit in your Cyber Security. We are willing to show you how
to improve your systems. This offer ends soon, our software is
specially designed to autodestruct if access to C2 servers is
lost.”, amount 2 000 000.
```

Ispis 4.1 Sadržaj ucjenjivačkih poruka

Obrambena organizacija prihvaća obje ucjene što označava kraj napada.

4.2. Procjena troška i dobiti napada

Trošak napada mjeren je CCS formulom troška te skriptom. CCS je računao trošak korištenih uređaja a skripta trošak svih ostalih resursa te prihod napadača. Kako bi napad radio, morao se prehodno upaliti poslužitelj *serveraws72.com* te *Firewall.*

CCS je kao trošak scenarija izračunao cifru od 2586 $ što predstavlja trošak korištenja *serveraws72.com* poslužitelja i vatrozida, pošto su, od uređaja, samo oni korišteni u napadu. Skripta je nakon rada odredila korištene resurse te izračunala trošak, prihod i ukupnu dobit napadača (Tablica 4.2). Skripti je kao parametar proslijeđena vrijednost

'*not0'* što označava da je prilikom procjene troška pretpostavljeno da metode iskorištavanja nisu nultog dana.

Korišteni resursi	Trošak napada / $	Prihod napada / $	Dobit napada / $
SurfsharkVPN, Irfan View x64, Malwarebytes Anti-malware, 41f0_be, Exploit MFP Linux, W08_19_VSRT_exp_R, W10-HTZJ_exp_R, Popular Forum Site Mail	56 022.95	2 500 000	2 443 977.05

Tablica 4.2 Rezultati skripte za izračun dobiti napada nakon izvršavanja sa parametrom '*not0'*

Kako bi se odredila ukupna dobit napadača, od dobiti koju je skripta izračunala oduzeta je vrijednost troška kojeg je CCS izračunao. Ukupna dobit iznosi 2 441 391. 05 $.

S druge strane, ako je skripti proslijeđen parametar *'0'*, što označava da je prilikom procjene troška pretpostavljeno da su metode iskorištavanja nultog dana, skripta računa sadržaj prikazan u tablici 4.3.

Korišteni resursi	Trošak napada / $	Prihod napada / $	Dobit napada / $
SurfsharkVPN, Irfan View x64, Malwarebytes Anti-malware, 41f0_be, Exploit MFP Linux, W08_19_VSRT_exp_R, W10-HTZJ_exp_R, Popular Forum Site Mail	2 285 282.95	2 500 000	214 717.05

Tablica 4.3 Rezultati skripte za izračun dobiti napada nakon izvršavanja sa parametrom '*0'*

U ovom slučaju, nakon što se od dobiti izračunate u skripti oduzme trošak izračunat u CCS-u, ukupna dobit napadača iznosi 212 131.05 $.

5. Zaključak

Ovim radom je napravljena procjena dobiti napadača u scenariju *Blackmail*. Prilikom proučavanja mehanizama pomoću kojih bi se izmjerila dobit napadača unutar samog CCS-a su uočena velika ograničenja. CCS formule za računanje troška i dobiti ne sadrže potrebnu logiku sposobnu za zaključivanje kada napadači koriste koje resurse. Taj problem je riješen skriptom koja analizira sve akcije te izdvaja korištene resurse. Skriptom je na temelju akcija također izračunat ukupni prihod napadača. Na temelju analize rezultata, ustanovljeno je da u odabranom scenariju dobit ostvarena od strane napadača nadmašuje povezane troškove korištenih resursa. Dodatno, uočena je primjetna razlika u dobiti napadača kada se koriste metode nultog dana, u usporedbi s dobiti kada se koriste metode koje nisu nultog dana. Ova izražena razlika upućuje na potencijalni utjecaj korištenja metoda nultog dana na profitabilnost računalnog napada.

Korišteni resursi su precizno locirani, no procjena cijene korištenih resursa predstavlja veoma kompleksan zadatak. Element koji se čini najkompleksnijim je cijena metoda za iskorištavanje. Precizne podatke vezane za njihove cijene je gotovo nemoguće naći. Cijene malicioznih kodova su također javno nepoznate te komplicirane za procjeniti. Prilikom definiranja resursa u CCS-u bi se trebale detaljno istražiti cijene sličnih resursa na crnom tržištu. To predstavlja kompliciran zahtjev, jer je pristup tržištima napadačkih resursa veoma teško dobiti, no tako bi mogle biti određene najpreciznije vrijednosti troška.

Kako bi se procjena automatizirala, izrazi u CCS-u trebaju biti nadograđeni kako bi se moglo identificirati kada napadač koristi određene resurse i tko provodi samu akciju. Također, potrebno je dodati izraze koji mogu prepoznati kada organizacija prihvaća napadačevu ucjenu i kada napadač prodaje podatke na crnom tržištu. Ove promjene omogućile bi automatizirano izračunavanje procjene dobiti. U međuvremenu, napravljena skripta može pomoći prilikom izračuna ukupne dobiti napadača.

6. Literatura

[1] Positive Technologies, „Hack at all cost: putting a price on APT attacks“ ptsecurity 14. kolovoza 2019. [Online]. Dostupno: Advanced Persistent Threat (APT) Attack Cost Research: Analysis of Zero-Day Exploits and Tools (ptsecurity.com) [Pristupljeno 13. svibnja 2023.]

[2] Positive Technologies, „The Criminal cyberservices market“ ptsecurity 25. srpnja 2018. [Online]. Dostupno: Dark Web Markets 2018: Cyber Crime Statistics for Darknet Cyberservices and Tools (ptsecurity.com), [Pristupljeno 10. svibnja 2023.]

[3] K. Grubešić, “Izgradnja složenog kibernetičkog poligona za vježbe napada i obrane,” Diplomski rad, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, srpanj 2022.

[4] Eric Brinkman, “How Much Does a Server Cost For a Small Business in 2023? “, servermania 10. veljače 2023. [Online]. Dostupno:What's the Cost of a Server for Small Business (servermania.com) [Pristupljeno 16. svibnja 2023.]

[5] Federica Laricchia, “Brazil: cost of a month of internet in Sao Paulo 2018-2019“ , statista 18.siječnja 2022. [Online]. Dostupno: Cost of internet per month in São Paulo, Brazil 2019 | Statista [Pristupljeno 19. svibnja 2023.]

[6] GlobalPetrolPrices ,“Brazil Electricity prices“, GlobalPetrolPrices [Online]. Dostupno: Brazil energy prices | GlobalPetrolPrices.com [Pristupljeno: 19. svibnja 2023.]

[7] Josh Mahan, „Understanding Data Center Energy Consumption“ cc-techgroup, 20. travnja 2023. [Online]. Dostupno: https://cc-techgroup.com/data-center-energy-consumption/ [Pristupljeno 19. svibnja 2023.]

[8] Fortinet, „Network Firewall Price: comparing security costs“ , Fortinet [Online]. Dostupno: https://www.fortinet.com/products/network-firewall-pricing [Pristupljeno 19. svibnja 2023.]

[9] Sirius Office Solutions, “How Much Does a Cloud Server Cost for a Small Business?“, siriusofficesolutions [Online]. Dostupno: Cloud Server Price and Cloud Costs for a Small Business (siriusofficesolutions.com). [Pristupljeno 19. svibnja 2023.]

[10] Salary.com ,“Hourly Wage for Ethical Hacker in the United States“ Salary-com [Online]. Dostupno: https://www.salary.com/research/salary/posting/ethical-hacker-hourly-wages [Pristupljeno 20. svibnja 2023.]

[11] Numbeo, “Price Rankings by Country of Internet“ Numbeo [Online]. Dostupno: Price Rankings by Country of Internet (60 Mbps or More, Unlimited Data, Cable/ADSL) (Utilities (Monthly)) (numbeo.com) [Pristupljeno: 21. svibnja 2023.]

[12] GlobalPetrolPrices, “Russia Electricity prices“ ,GlobalPetrolPrices [Online]. Dostupno: Russia electricity prices, September 2022 | GlobalPetrolPrices.com [Pristupljeno: 22.svibnja 2023.]

[13] Mitre Corporation , „CVE-2018-8174“ , Mitre Corporation [Online]. Dostupno: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174 [Pristupljeno: 22. svibnja 2023.]

[14] Surfshark , „Surfshark cost and pricing“ Sursfhark, [Online]. Dostupno: Surfshark: secure online VPN service & more [Pristupljeno 23. svibnja 2023.]

[15] ExpressVpn, „Pricing“ , ExpressVpn [Online]. Dostupno: https://www.expressvpn.com/ [Pristupljeno 23. svibnja 2023.]

[16] NordVPN , „Pricing“, NordVPN [Online] Dostupno: VPN cost? Buy VPN with Credit Card, Crypto, PayPal | NordVPN [Pristupljeno 23. svibnja 2023]

[17] Strategic Cyber LLC, "Features," CobaltStrike [Online]. Dostupno: Features | Beacon, C2 Profiles, Attack Packages, and More | Cobalt Strike, [Pristupljeno 30. svibnja, 2023.]

[18] Sarah Delasko ,Weifeng Chen, “ Operating Systems of Choice for Professional Hackers“ Palcomtech [Online]. Dostupno : 6105.pdf (palcomtech.com) , [Pristupljeno 30. svibnja, 2023.]

[19] Maxym Maritnueau ,“How much does a domain name cost? Find out!“ , GoDaddy.com [Online]. Dostupno: How much does a domain name cost? Find out! | GoDaddy , [Pristupljeno 1. lipnja 2023.]

[20] Joteo , „Power consumption of a hardware firewall“, Joteo [Online]. Dostupno: https://joteo.net/electricity-usage-calculator/electricity-usage-of-a-hardware-firewall [Pristupljeno 1. lipnja 2023.]

[21] VulDB „Microsoft office 2007/2010/2013 document use after free“ ,VulDB [Online]. Dostupno : CVE-2015-1650: Microsoft Office Document use after free (MS15-033 / Nessus ID 82769) (vuldb.com) , [Pristupljeno 1. lipnja 2023.]

[22] VulDB „Microsoft office 2013 SP1 Office document remote code execution“ , VuldDB [Online]. Dostupno CVE-2015-1770: Microsoft Office Office Document Remote Code Execution (MS15-059 / Nessus ID 84055) (vuldb.com) , [Pristupljeno 1. lipnja 2023.]

[23] Hostinger „Web hosting prices“, Hostinger, [Online]. Dostupno: Web Hosting | Easy to Use, 24/7 Support, and More (hostinger.com) , [Pristupljeno 1. lipnja 2023.]

[24] Infonet „Neograničeni web hosting cijene“ ,Infonet, [Online]. Dostupno: Usporedba poslovnih web hosting paketa | InfoNET hosting, [Pristupljeno 1. lipnja 2023.]

[25] Legal hackers , „SquirrelMail-Exploit-Remote-Code-Exec-CVE-2017-7692“, Dostupno: SquirrelMail-Exploit-Remote-Code-Exec-CVE-2017-7692-Vuln (legalhackers.com) [Pristupljeno 1. lipnja 2023.]

[26] VulDB, „Centos Web Panel Prior 0.9.8.1107 apikey /user/Loader.PHP Scripts Acces Control“ ,VulDB, [Online]. Dostupno : CVE-2021-45467: CentOS Web Panel API Key access control (vuldb.com) [Pristupljeno 1. lipnja 2023.]

[27] CVE Details , „Vulnerability details : CVE – 2018-8174“ [Online]. Dostupno : https://www.cvedetails.com/cve/CVE-2018-8174/ [Pristupljeno 2. lipnja 2023.]

[28] NIST , “CVE – 2021-38238-Detail„ NIST , [Online]. Dostupno: https://nvd.nist.gov/vuln/detail/CVE-2021-39238 [Pristupljeno 2. lipnja 2023.]

[29] VulDB , „HP Enterprise Laserjet Buffer Overflow“ ,VulDB [Online]. Dostupno: https://vuldb.com/?id.185937 [Pristupljeno 2. lipnja 2023.]

[30] Group-IB , „How much is the phish? Undergorund market of phishing kits is booming“, 15. travnja 2020. Group-IB [Online]. Dostupno: https://www.group-ib.com/media-center/press-releases/how-much-is-the-phish/ [Pristupljeno 2. lipnja 2023.]

[31] Domantas G ,“What is Web Hosting – Web Hosting Explained for Beginners“, 6. lipnja 2023. Hostinger [Online]. Dostupno : What Is Web Hosting? Web Hosting Explained for Beginners (hostinger.com) [Pristupljeno 7 .lipnja 2023.]

[32] SOCRadar , „What is a phishing kit?“ , 4. travnja 2023. SOCRadar [Online]. Dostupno: What is a Phishing Kit? - SOCRadar® Cyber Intelligence Inc. [Pristupljeno 8. lipnja 2023.]

[33] James LePage , “The top open source email servers in 2023“, 7. siječnja 2022. Isotropic [Online]. Dostupno: The Top Open Source Email Servers in 2023 - Isotropic , [Pristupljeno 8. lipnja 2023.]

[34] ExtraHop ,“C2 Beaconing : Definition, Examples, and Prevention“, ExtraHop [Online]. Dostupno : C2 Beaconing - Definition, Examples, & Detection - ExtraHop , [Pristupljeno 8. lipnja 2023.]

[35] Tutorialspoint , „Ethical hacking -Reconnaissance“ , Tutorialspoint [Online]. Dostupno : Ethical Hacking - Reconnaissance (tutorialspoint.com) , [Pristupljeno 8. lipnja 2023.]

[36] Baričević, I. 1 lipnja 2023. Skripta za računanje prihoda i potrebne datoteke Dostupno na: GitHub - MladiGljivor/Zavrsni-Rad: Skripta i potrebne datoteke. [Pristupljeno 5. lipnja 2023].

Sažetak

Određivanje ulaganja i dobiti napadača u provođenju napada

Unatoč kontinuiranom rastu kibernetičkog kriminala, pouzdane procjene ekonomske štete napadačke strane su rijetke. Ovaj rad se bavi problemom izračunavanja ekonomske štete i ukupne dobiti napadačke organizacije. Za simulaciju napada se koristi alat *Cyber Conflict Simulator* (CCS), alat specifično dizajniran za modeliranje i simuliranje kibernetičkih napada.

U radu se daje pregled jedne napadačke organizacije te svih resursa koje njeni članovi troše prilikom napada. Pomoću dostupne literature je procjenjen trošak tih resursa te je model ukomponiran u napad. Za potrebe procjene troška je kreirana i *Python* skripta koja pokriva troškove na mjestima na kojima CCS nema sposobnost odrediti trošak. Izabran je jedan scenarij napada te se prolaskom kroz njega pokušala odrediti šteta i dobit napadačke organizacije koristeći sam CCS alat i napravljenu skriptu.

Kjučne riječi: napadačev trošak, napadačeva dobit, *Cyber Conflict Simulator*, napadački resursi, formula za izračun troška, skripta za izračun troška

Summary

Determining investment and gain for attackers when performing cyber attack

Despite the continuous growth of cybercrime, reliable estimates of the economic damage to the attacker side are rare. This paper deals with the problem of calculating the economic damage and profit of an attacker organization. The Cyber Conflict Simulator (CCS) tool, specifically designed for modeling and simulating cyber attacks, is used to simulate attacks.

The paper provides an overview of an attacker organization and all the resources it uses during an attack. The cost of these resources was estimated using available literature, and the model was incorporated into the attack. To estimate the cost, a Python script was created that covers costs in places where the CCS is unable to determine the cost. One attack scenario was chosen and an attempt was made to determine the damage and profit of the attacker organization using the CCS tool itself and the script made.

Keywords: attacker's cost, attacker's earnings, *Cyber Conflict Simulator*, attacker's resources, cost calculation formula, cost calculation script.