SUVREMENI OBLICI KIBERNETIČKOG KRIMINALA - RANSOMWARE

Regvar, Kristijan

Veleučilište u Karlovcu
Odjel Sigurnosti i zaštite

Stručni studij sigurnosti i zaštite

Kristijan Regvar

SUVREMENI OBLICI KIBERNETIČKOG KRIMINALA - RANSOMWARE

ZAVRŠNI RAD

Karlovac, 2022.

Karlovac University of Applied Sciences
Safety and Protection Department

Professional undergraduate study of Safety and Protection

Kristijan Regvar

CONTEMPORARY FORMS OF CYBERCRIME - RANSOMWARE

Final paper

Karlovac, 2022.

Veleučilište u Karlovcu
Odjel Sigurnosti i zaštite

Stručni studij sigurnosti i zaštite

Kristijan Regvar

SUVREMENI OBLICI KIBERNETIČKOG KRIMINALA - RANSOMWARE

ZAVRŠNI RAD

Mentor:
dr. sc. Damir Kralj, prof. v. š.

Karlovac, 2022.

VELEUČILIŠTE U KARLOVCU
Karlovac University of Applied Sciences

VELEUČILIŠTE U KARLOVCU

Preddiplomski stručni studij Sigurnosti i zaštite

Usmjerenje: Zaštita na radu Karlovac, 17.08.2021.

ZADATAK ZAVRŠNOG RADA

Student: Kristijan Regvar Matični broj: 0416615086

Naslov: SUVREMENI OBLICI KIBERNETIČKOG KRIMINALA - RANSOMWARE

Opis zadatka:

- analizirati opće stanje ugroze od suvremenih oblika kibernetičkog kriminala u svijetu i kod nas uz osvrt na aktualne regulatorne odredbe o suzbijanju
- okvirno analizirati i opisati najzastupljenije oblike kibernetičkih napada na poslovne informacijske sustave i privatna osobna računala
- u eksperimentalnom dijelu detaljnije analizirati način i posljedice napada putem ucjenjivačkog softvera tzv. ransomwarea te dati analizu konkretnih primjera napada
- dati mišljenje o aktualnoj situaciji i predložiti moguća poboljšanja stanja

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
17.08.2021.	19.05.2022.	26.05.2022.

Mentor: Predsjednik Ispitnog povjerenstva:

dr. sc. Damir Kralj, prof. v. š. dr. sc. Vladimir Tudić, prof. v. š.

PREDGOVOR

Izjavljujem da sam ovaj završni rad izradio samostalno koristeći u popisu literature navedene tiskane i mrežne izvore, vlastita iskustva, kroz školovanje stečena znanja te uz pomoć i savjete mentora.

SAŽETAK

Kibernetički kriminal definiran je kao zločin u kojem je računalo predmet zločina ili se koristi kao oruđe za počinjenje kaznenog djela. Kibernetički kriminalac može koristiti uređaj za pristup osobnim podacima korisnika, povjerljivim poslovnim podacima, državnim podacima ili onemogućiti uređaj. Također je kibernetički kriminal prodavati ili izazivati gore navedene podatke na internetu. Jedan od najtežih oblika računalnog kriminala je opasnost od ucjenjivačkog softvera – ransomwarea u kojem će najviše biti riječi u ovom poglavlju. Kao primjer slučaja velikog napada ransomwarea biti će objašnjen napad na nacionalni zdravstveni sustav Velike Britanije. Primjer pokazuje da propusti u zaštiti od kibernetičkog kriminala mogu dovesti do ugroze života i zdravlja ljudi.

Ključne riječi: računalni kriminal, oblici računalnog kriminala, ransomware, sigurnost i zaštita

ABSTRACT

Cybercrime is defined as a crime in which a computer is the subject of a crime or is used as a tool to commit a crime. A cybercriminal can use the device to access users' personal data, confidential business data, government data, or disable the device. It is also a cybercrime to sell or provoke the above data online. One of the most serious forms of computer crime is the danger of blackmail software - ransomware, which will be the most discussed in this paper. An example of a large case of ransomware attacks will be the attack on the UK national health service. The example shows that failures in protection against cybercrime can lead to threats to human life and health.

Keywords: computer crime, forms of computer crime, ransomware, security and protection

SADRŽAJ

1. UVOD

1.1. Predmet i cilj rada

Ransomware je softver koji blokira informacijske sustave čekajući otkupninu. Ovakav računalni kriminal postao je primarna prijetnja na području kibernetičke sigurnosti. Napadi ransomware-a imaju ozbiljan utjecaj na tvrtke i često dopuštaju kibernetičkim kriminalcima zarade od desetak do stotine milijuna eura. Ovi napadi uspijevaju iz dva razloga: visoke isplativosti operacija i virtualne nekažnjivosti počinitelja. U ovom radu predmet rada bit će analiza općenito računalnog kriminala s posebnim osvrtom na ransomware kao jedan od vodećih prijetnji kibernetičke sigurnosti koje pogađaju tvrtke. U 2020. godini ovaj računalni kriminal je imao najveći utjecaj na proizvodnju, ugled i financije žrtava stoga napadi ransomware-a zaslužuju posebnu pozornost.

Cilj rada je na primjeru iz stvarne prakse objasniti kako je ta vrsta računalnog kriminala funkcionirala u stvarnosti te je isti pojašnjen na primjeru Nacionalnog zdravstvenog sustava u Velikoj Britaniji koji je zahvatio cijeli sustav i napravio kolaps u zdravstvenom sustavu.

1.2. Metodologija i izvori prikupljanja podataka

U svrhu izrade rada koristiti će se deskriptivna metoda kojom će se opisati glavni pojmovi vezani za računalni kriminal te posebne oblike računalnog kriminala. Za podjelu oblika računalnog kriminala i klasifikaciju istog koristit će se metoda klasifikacija. Kod donošenja zaključka i izvođenja glavne poante u dijelovima rada korištena će biti metoda indukcije i dedukcije. Metoda analize i sinteze također je korištena u radu ponajprije u analizi specifičnog oblika ransomware-a.

Za istraživanje konkretnog slučaja ransomware-a korišteni su stručni članici na tu temu a dio podataka izvučen je iz publikacija Nacionalnog zdravstvenog sustava Velike Britanije na čijem se konkretnom slučaju obrađuje slučaj napada.

1.3. Sadržaj i struktura rada

Ovaj rad sastoji se od šest poglavlja – nakon uvodnog dijela obrađen je pojam računalnog kriminala te je analiziran njegov povijesni razvoj.

Treće poglavlje analizira oblike računalnog kriminala koji se odnosi na zlouporabu računalnih tehnologija i kibernetičkog ratovanja. Od najbezazlenijih do najtežih napada opisani su oblici napada u ovom poglavlju.

U četvrtom poglavlju prikazana je opasnost od ucjenjivačkog softvera ransomware. Prikazan je njegov povijesni razvoj, opisane su vrste ransomware-a te je na kraju poglavlja slikovito prikazan jedan primjer ransomware-a.

Peto poglavlje donosi konkretan slučaj napada ransomware-om, Nacionalnog zdravstvenog sustava Velike Britanije koji je zahvatio kompletan sustav i narušio poslovanje i privatnost korisnika sustava kao i osoba koje su direktno i indirektno bile povezane sa sustavom.

U šestom poglavlju iznesen je zaključak rada.

2. RAČUNALNI KRIMINAL

2.1. Povijesni razvoj računalnog kriminala

Računalni kriminal nije uvijek bio kršenje formalnog prava. Tek od 1979. godine Ministarstvo pravosuđa SAD-a je definiralo računalni kriminal kao bilo koji nelegalni akt za čije počinjenje je upotrijebljeno računalo ili računalna tehnologija. Potrebu za ovim je nametnula činjenica, da je samo krajem 70-ih godina već bilo nekoliko stotina (preko 500) kaznenih djela učinjenih upotrebom računala [1].

Osamdesetih godina činilo se da su računala vrhunac razvoja u Rusiji u području elektronike. Izraz računalni zločin (*njem. Computerkriminalität*) stoga je prvi put upotrijebljen u pravnim tekstovima. Izraz je kao takav bio primjeren zločin, povezan s računalima. Bez obzira na to, izraz "računalni kriminal" bitno je i formalno neprikladan. Kriminalistički pravni teoretičari predložili su uporabu izraza računalni kriminal, pri čemu je činjenica da je računalo "samo oruđe u rukama“ [2].

Odgovor na pitanje "kako bismo trebali reagirati na devijantno ponašanje na internetu?" jasno ovisi o tome kako definiramo takvo ponašanje i o tome kako definiramo kibernetički kriminal. (Sličnu) riječ cyberspace smislio je William Gibson u svom poznatom cyberpunk romanu Neuromancer 1984. Autor je osmislio zamišljeni svijet i jezik da ga opiše, desetljeće prije "informacijske revolucije" i širenja interneta. Razumijevanje temeljnih ontoloških pojmova kiberprostora koji je proizašao iz cyberpunk pokreta osamdesetih čini se da je neophodan za pravilno razumijevanje (barem nekih oblika) cyber kriminala [2].

„Cyberpunk“ karakterizira vjera u korištenje tehnologije za podršku i njegovanje individualizma te dopuštanje mogućnosti „samoodređenog ljudskog bića“. Izraz govori o vjernosti i inzistiranju na ideji samostvaranja, neovisnim odabirom identiteta koje tradicija više ne određuje. Svi ti atributi cyberpunk-a su sve tipično postmodernističke karakteristike, atributi koji su migrirali devedesetih daleko izvan znanstveno-fantastične literature kao pojma kibernetičke kulture koja je postala dio svakodnevnog života [3].

Korijeni cyber kulture mogu se pronaći u revolucionarnom, kontrakulturnom razdoblju koje je obilježilo šezdesete godine prošlog stoljeća. Ovo je uglavnom bilo doba definirano borbom protiv znanstvenog ili preempirijskog shvaćanja stvarnosti i tehnologije. Kasnije se dogodila transformacija 1980-ih kada se kontrakultura ujedinila (paradoksalno i ironično pokazalo se) s oblicima tehnologije za koje se činilo da nude neka sredstva bježeći od društvene kontrole. U tim terminima, cyber kultura obuhvaća težnju k emancipaciji pojedinca koje su postepeno preuzimali i sputavali veliki transnacionalni tehnološki sustavi.

2.2. Pojmovno određenje računalnog kriminala – računalni kriminal danas

Zločin i kriminal povezani su s čovjekom od njegova postojanja. Različite nacije donijele su različite strategije za borbu protiv kriminala, ovisno o njihovoj prirodi i opsegu. Jedno je sigurno, to je da narod s velikom učestalošću zločina ne može rasti ili se razvijati. Zločin ostavlja negativne društvene i ekonomske posljedice te je izravna suprotnost razvoju.

Podrazumijeva se da računalni kriminal obuhvaća dva elementa: ili je računalo moralo biti korišteno kao sredstvo ili objekt napada, ili počinjenje kaznenog djela proizlazi iz stručnog znanja počinitelja o računalnoj ili informacijskoj znanosti. S obzirom na činjenicu da se stručno znanje smatralo kao bitan element, neki kriminalistički stručnjaci preporučuju upotrebu tog izraza kriminal u informacijskoj znanosti (Fr. la Criminalitéinformatique) [1] .

Računalni kriminal definiran je kao zločin počinjen na internetu pomoću računala kao alata ili ciljanu žrtvu. Vrlo je teško općenito klasificirati zločine u različite skupine jer se mnogi zločini razvijaju svakodnevno. Čak i u stvarnom svijetu zločini poput silovanja, ubojstva ili krađe ne moraju nužno biti odvojeni. Međutim, svi kibernetički zločini uključuju i računalo i osobu iza njega kao žrtve, samo ovisi o tome koja je od njih dvije glavna meta. Zbog toga se računalo može promatrati kao meta ili kao alat. Na primjer, hakiranje uključuje napad na podatke računala i druge resurse. Važno je uzeti u obzir da se

preklapanje događa u mnogim slučajevima i nemoguće je imati savršen sustav klasifikacije [4].

Računalo kao alat podrazumijeva situaciju kada je pojedinac glavna meta kibernetičkog kriminala, računalo se može smatrati alatom, a ne metom. Ovi zločini općenito uključuju manje stručne vještine jer se nanesena šteta očituje u stvarnom svijetu. Općenito se iskorištavaju ljudske slabosti. Nanesena šteta u velikoj je mjeri psihološka i nematerijalna, što otežava pravne radnje. To su zločini koji stoljećima postoje i izvan mreže. Prevare, krađe i slično postojali su i prije razvoja opreme visoke tehnologije. Isti je zločinac jednostavno dobio alat koji povećava njegov potencijalni broj žrtava i otežava mu praćenje i hvatanje [4].

Računalo kao meta podrazumijeva situaciju koju provodi odabrana skupina kriminalaca. Za razliku od zločina koji koriste računalo kao oruđe, ti zločini zahtijevaju tehničko znanje počinitelja. Ti su zločini relativno novi, postoje samo onoliko koliko postoje računala - što objašnjava koliko su društvo i svijet općenito nepripremljeni u borbi protiv ovih zločina. Na internetu se svakodnevno čine brojni zločini ove prirode.

Danas se razmatra i pojam računalnog zločina i njegovi derivati preusko ili za označavanje samo prve generacije kibernetičkog kriminala [5]. Računala i njihove komponente - mikroprocesori - sve su prisutne: mogu se pronaći u ručnim satovima, kućanskim aparatima, vozilima itd. Kasnije razvijene tehnologije temelje se na prijenosu podataka između računala i omogućuju komunikaciju. Umjesto izraza "računalo" općenitiji izraz, informacijsko-komunikacijska tehnologija (ICT) danas postaje primjereniji izraz. Osim računala, razvoj ICT-a donio je i druge terminale uređaje poput mobilnih telefona, automatiziranih mrežnih sučelja i druge hibridne tehnologije koje spajaju postojeće zasebne tehnologije (televizija, radio, video, telefonija, satelitska navigacija itd.). Zajednički nazivnik ovih tehnologija postala je prisutnost podataka i mreže - otuda i pojam ICT kriminal [6].

Karakteristika računalnog kriminala je da se u vrlo malo slučaja otkriju napadači. Invaziju na računalo često je teško otkriti u vrijeme napada i obično zahtijevaju mjere

zaštite softvera, kao i odgovarajuće tehničko znanje. Posebno teške vrste računalnog kriminala za otkrivanje su špijunski softver i putnici podataka, programi koji „putuju“ kroz računala i izvještavaju o njihovom sadržaju počinitelja. Još jedan nedostižan kriminalni program poznat je kao lažni brojčanik, koji traži rupe u sigurnosnim programima i dodiruje računalo žrtve [6].

3. OBLICI RAČUNALNOG KRIMINALA

Najčešći oblici računalnog kriminala opisani će biti unutar ovog poglavlja.

3.1. Zlouporaba računalnih tehnologija

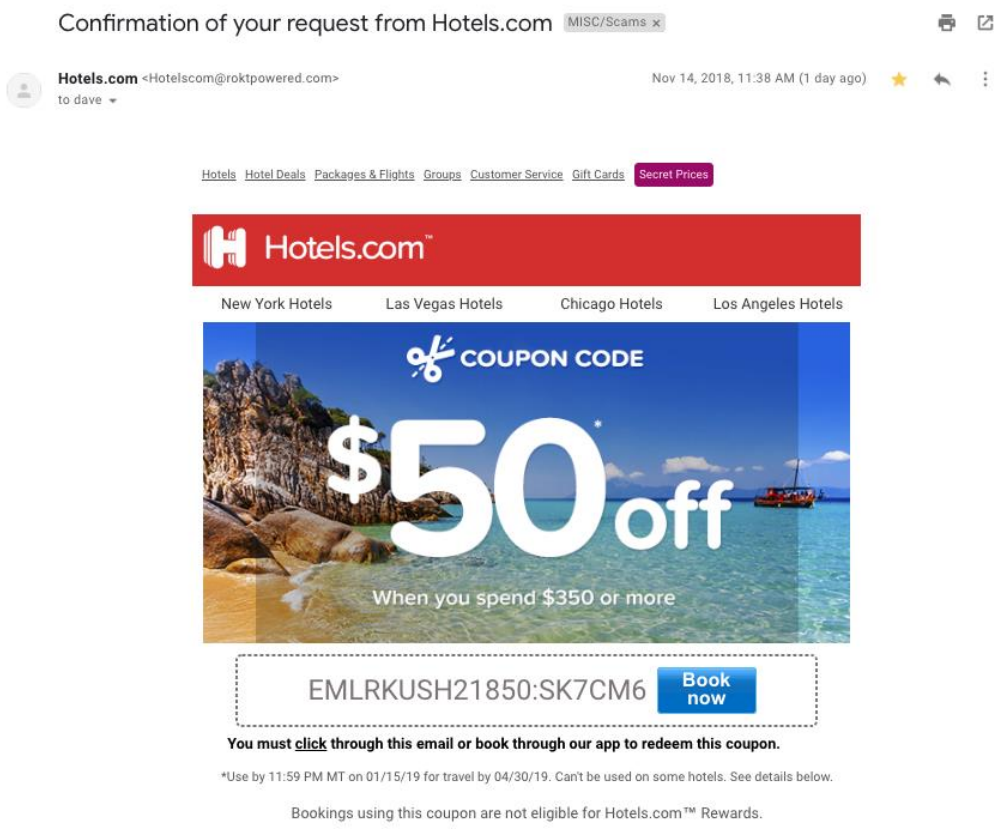
3.1.1. Neželjena pošta - SPAM

Jedno od najranijih internetskih kriminalnih partnerstava sklopljeno je između autora zlonamjernog softvera i pošiljatelja neželjene e-pošte, koji su društveno projektirali e-poštu za širenje zlonamjernog softvera na računala i druge digitalne uređaje; e-pošta ostaje jedan od glavnih vektora za širenje zlonamjernog softvera. Za razliku od kibernetičkog kriminala koji cilja na manje žrtve, velike vrijednosti poput banaka i zahtijeva napredne mogućnosti hakiranja, neželjena pošta dopušta zlonamjernom softveru da dosegne ciljeve velike vrijednosti, za koje je manje vjerojatno da će imati učinkovit virus ili druge protumjere. Tipičan primjer bila bi zlonamjerna e-poruka koja sadržajem tjera primatelje da kliknu na URL vezu do zlonamjerne web stranice ili da preuzme zlonamjerni prilog [7] .

Neželjena pošta distribucija je masovne e-pošte koja oglašava proizvode, usluge ili sheme ulaganja, koje bi se mogle pokazati lažnim. Svrha neželjene pošte je prevariti ili obmanuti kupce da vjeruju da će dobiti pravi proizvod ili uslugu, obično po sniženoj cijeni. Međutim, *„spammer“*[1] traži novac ili sigurnosne podatke, poput broja kreditne kartice ili druge osobne podatke prije nego što dođe do dogovora. Nakon što su otkriju svoje sigurnosne informacije, korisnik nikada više ne može kontaktirati pošiljatelja neželjene pošte. Danas pošiljatelji neželjene pošte koji šire zlonamjeran kod i neželjenu e-poštu i dalje traže najbolji način da dođu do korisnika računala pomoću društvenog inženjeringa i tehničkog napretka [7].

[1] Osoba koja šalje neželjenu poštu.

Formati takve e-pošte dobro su razumljivi, i formirani su pomoću standardnog SMTP-a. Slika 1 prikazuje strukturu tipične zlonamjerne neželjene e -pošte bez osobnih metapodataka. Primjer e-pošte predstavljen je u formatu neobrađenog teksta, s napomenama koje prikazuju dijelove e-pošte. Zaglavlje e-pošte sadrži upute za isporuku za poslužitelje pošte, a tijelo e-pošte može imati mnogo teksta i priloga. Predmetni i tekstualni sadržaj zlonamjernog neželjenog sadržaja može otkriti metode društvenog inženjeringa različite razine sofisticiranosti koje nastoje manipulirati primateljima da prvo pročitaju, a zatim i odgovaraju i postupaju prema naputku iz e-pošte.



Slika 1. Primjer opasne neželjene pošte [8]

Preuzimanjem komprimirane datoteke prenio bi se zlonamjerni virus i oštetio računalo. Komprimirana datoteka skriva izvršni zlonamjerni softver iz skenera virusa koje primjenjuje poslužitelj pošte, davatelj internetskih usluga potencijalne žrtve ili administrator lokalnog sustava. U ovom primjeru URL djeluje kao sekundarna metoda

isporuke zlonamjernog sadržaja. Poput akata, zlonamjerni URL-ovi mogu prikriti zlonamjernu ili ugroženu web stranicu dodavanjem poddomena koje predstavljaju poznatu i sigurnu web stranicu. Ovaj primjer također prikazuje tipičan predložak neželjene pošte, gdje prilozi ili URL-ovi mogu imati različite nazive, ali istu zlonamjernu svrhu.

3.1.2. Malware

Maliciozni računalni programi poznati su pod raznim imenima (virusi, crvi, trojanci i sl.), a zajednički naziv im je malware. Oni su nastali u posljednjih par desetljeća prošlog stoljeća, iako problemi koje oni izazivaju su uvijek trenutni te izazivaju štetu u realnom vremenu [8]. Analiziranje malicioznih računalnih programa može predstavljati važan alat za progon počinitelja računalnog kriminala, a poznavanje takvih alata kao i samih malicioznih računalnih programa može pomoći istražiteljima i osobama koje su zadužene za sigurnost računalnih sustava u prepoznavanju njihovih učinaka. Kada se govori o malware-u govori se o zločinačkoj organizaciji koja ujedinjuje viruse, crve, trojance i druge zloćudne i nedobronamjerne aplikacije u svrhu ostvarivanja počiniteljima protupravne koristi koja je u većini slučajeva materijalne prirode (iako može imati i neke druge oblike poput uznemiravanja) [1].

Osnovne karakteristike malware-a su: [1]

- modularnost,
- prodornost i razornost,
- financije,
- uključenje na zahtjev,
- homogenost,
- kontaminacija,
- konkurentnost i
- neprimjetnost.

Modularnim pristupom potencijalni programi onemogućeni su u borbi protiv malware-a, dok se prodornost i razornost očituje u tome kada se jednom „zarazi“ domaćina, onemogućen je *firewall* i u načelu se pokušava osigurati dobit za autora malware-a. Malware polučuje veoma značajnu dobit stoga su financije također jedan od razloga zašto dolazi do navedenog kriminala. Uključenje na zahtjev uključuje unajmljivanje zombi servera za računalni napad. Jednom kada se malware „useli“ on počinje s kontaminiranjem. Može se širiti zavaravanjem i širenjem drugih slabih točaka [1].

Postoje različite vrste zlonamjernog softvera. Najčešći su sljedeći:[1]

1. *Crvi* se šire putem softverskih ranjivosti ili phishing napada. Nakon što se crv instalirao u memoriju računala, počinje ugrožavati cijelo računalo, a u nekim slučajevima i cijelu mrežu. Ovisno o vrsti crva i vašim sigurnosnim mjerama, mogu nanijeti ozbiljnu štetu. Oni mogu:
    - izmijeniti i izbrisati datoteke,
    - postaviti zlonamjerni softver na računala,
    - uvijek se ponavljaju kako bi iscrpili resurse sustava,
    - ukrasti podatke i
    - instalirati prikladan ulaz za hakere.
2. *Virusima* je za razliku od crva, potreban već zaražen aktivni operacijski sustav ili program. Oni su obično povezani s izvršnom datotekom ili word dokumentom. Većina ljudi vjerojatno je svjesna da ekstenzija datoteke .exe može dovesti do problema ako nije iz pouzdanog izvora. No, postoje stotine drugih ekstenzija datoteka koje označavaju izvršnu datoteku. Obično se širi putem zaraženih web stranica, dijeljenjem datoteka ili preuzimanjem privitaka e-pošte, virus će mirovati sve dok se ne aktivira zaražena datoteka ili program domaćina. Kad se to dogodi, virus se može replicirati i širiti vašim sustavima.
3. Botovi i botneti su računala zaražena zlonamjernim softverom pa ih haker može daljinski kontrolirati. Taj bot (poznat i kao zombi računalo) tada se može koristiti za pokretanje više napada ili za uključivanje u zbirku botova (poznatih kao botnet). Botneti su popularni među hakerima (što više botova prikupite, jači ste haker) i

cyber kriminalcima koji šire ransomware. Botneti mogu uključivati milijune uređaja koji se šire neopaženo. Botneti pomažu hakerima u svim vrstama zlonamjernih aktivnosti, uključujući:

- DDoS napadi,
- zapisivanje tipki, snimke zaslona i pristup web kameri,
- širenje drugih vrsta zlonamjernog softvera,
- slanje neželjene i phishing poruke.

4. Trojanski konji su zlonamjerni programi koji se prerušavaju u legitimnu datoteku. Budući da izgleda pouzdano, korisnici ga preuzimaju. Za razliku od crva, za rad im je potreban domaćin. Nakon što se trojanac instalira na uređaj, hakeri ga mogu koristiti za:
   - brisanje, mijenjanje i snimanje podataka,
   - skupite svoj uređaj kao dio botneta,
   - špijunažu uređaja,
   - ostvarivanje pristupa mreži.
5. Ransomware odbija ili ograničava pristup vlastitim datotekama. Zatim zahtijeva plaćanje (obično kriptovalutama) u zamjenu za povratak. U svibnju 2017. napad ransomware-a proširio se na 150 zemalja i kompromitirao preko 200 tisuća računala u samo jednom danu. Prikladno nazvan WannaCry, napad je prouzročio štetu procijenjenu na stotine milijuna do milijardi dolara. WannaCry je utjecao na operacijske sustave MS koji nisu imali instaliranu najnoviju zakrpu zbog poznate ranjivosti. Više o ovom obliku kriminala u četvrtom poglavlju.
6. Oglasi i prijevare je jedna od poznatijih vrsta zlonamjernog softvera. Funkcionira na način da izbacuje skočne prozore i prikazne oglase koji često nisu relevantni. Neki će korisnici podnijeti određene vrste oglasnog softvera u zamjenu za besplatni softver (igre na primjer). No nisu svi oglasni programi jednaki. U najboljem slučaju, to smeta i usporava računalo. U najgorem slučaju, oglasi povezuju web stranice na kojima zlonamjerna preuzimanja čekaju korisnike koji ništa ne slute. Oglasni softver također može isporučiti špijunski softver i često se lako hakira, čineći uređaje na kojima je instaliran mekanom metom za hakere, lažljivce i prevarante.

3.1.3.“Phishing“ prijevare

Pod „phishing“ prijevarama podrazumijevaju se pokušaji prevare kupaca u otkrivanju njihovih osobnih sigurnosnih podataka; brojeva kreditnih kartica, podataka o bankovnom računu ili drugih osjetljivih podataka tako što se u e-pošti predstavljaju kao pouzdane kompanije i tvrtke. Njihove poruke mogu zatražiti od primatelja da "ažuriraju" ili "potvrde" podatke o svom računu. Krađa identiteta je dvostruka prijevara, prvo se ukrade identitet tvrtke, a zatim se njome žrtvuje potrošač krađom njihovog kreditnog identiteta. Izraz „phishing (koji se naziva i lažiranjem) dolazi do činjenice da internetski prevaranti koriste sve sofisticiranije mamce dok "love" korisničke financijske podatke i podatke o lozinkama. Podatke o lozinkama je vrlo jednostavno izvesti, nije potrebna izravna komunikacija između hakera i žrtve (tj. haker ne mora telefonirati svom plijenu, pretvarajući se da je osoblje tehničke podrške itd.). Slanje masovne pošte tisućama potencijalnih žrtava povećava šansu da se netko „ulovi“ [10].

Obično postoje tri odvojena koraka kako bi takvi napadi funkcionirali, a to su:

1. postavljanje lažnog web mjesta,
2. slanje uvjerljivo lažne e-pošte, namamljujući korisnike na to lažno web mjesto,
3. dobivanjem informacija korisnici preusmjeravaju se na stvarnu web lokaciju.

U prvom koraku haker krade identitet organizacije i stvara sličnu web stranicu. To se lako može učiniti pregledavanjem izvornog koda ciljane stranice, zatim kopiranjem svih grafika i HTML redaka s te stvarne web stranice. Zbog ove taktike, čak bi i iskusnom korisniku bilo jako teško uočiti razlike. Na oponašajućoj web stranici obično se nalazi obrazac za prijavu koji od korisnika traži da unese tajne osobne podatke. Nakon što se podaci unesu ovdje, skripta na strani poslužitelja će obraditi podnošenje, prikupiti podatke i poslati ih hakeru, a zatim preusmjeriti korisnike na stvarnu web stranicu kako bi sve izgledalo nesumnjivo.

Najteži dio „phishing“ napada koji izaziva većinu hakera je u drugom koraku. To ne znači da je tehnički teško, ali gramatički jest. U ovom koraku haker će napraviti uvjerljivo

lažnu e-poštu koju će kasnije poslati zanimljivi sadržaj za slanje e-pošte, omogućujući hakeru da lažira izvornu adresu e-pošte. Glavna svrha ove lažne e-pošte je potaknuti korisnike da posjete imitirajuću web stranicu i unesu svoje podatke koje su hakeri htjeli uhvatiti. Uobičajeno korištena taktika traži od korisnika da odgovore na hitne slučajeve, poput upozorenja da se korisnici moraju odmah prijaviti ili bi im računi mogli biti blokirani; obavijest da netko samo šalje korisniku nešto novca i da se moraju prijaviti kako bi ga dobili (ovo je obično učinkovita zamka za korisnike PayPala) itd. Unutar ove lažne e-pošte, korisnici često pronalaze hipervezu, koji jednom kliknu, otvorit će oponašajuću lažnu web stranicu kako bi se mogli "prijaviti". Najlakši način za brzo prepoznavanje lažne e-pošte nije samo gledanje izvora adrese (budući da se može promijeniti u bilo što), već provjera gramatike engleskog jezika u e-pošti. Osam od deset prijevara e-pošte ima očite gramatičke pogreške. Bez obzira na to, žrtve se i dalje „hvataju“. U posljednjem koraku, nakon što korisnik otvori web stranicu i „prijavi se“, njihove će podatke obraditi skripta na strani poslužitelja. Te će informacije kasnije biti poslane hakeru putem e-pošte, a korisnik će biti preusmjeren na stvarnu web stranicu. Međutim, sada je prekršena povjerljivost financijskih podataka korisnika ili tajne lozinke [11] .

Zbog financijske krize, spajanja i preuzimanja, na financijskom su se tržištu dogodile mnoge promjene. Ove su promjene potaknule hakere na traženje pojedinosti korisnika. Ključne točke su: [12]

- napadi društvenog inženjeringa imaju najveću uspješnost,
- prevencija uključuje obrazovanje ljudi o vrijednosti informacija i njihovo osposobljavanje da ih zaštite,
- povećanje svijesti ljudi o tome kako su društveni inženjering funkcionira,
- važno je ne „klikati“ na veze u poruci e-pošte i
- prijevara u krađi identiteta u ovom ili onom obliku prisutna od veljače 2004. i čini se da se još uvijek razvija, slično načinu na koji autori virusa dijele i evoluiraju kôd.

Jedan od primjera gdje često dolazi do phishinga su pdf datoteke.

Od 2019. do 2020. zamjetan je dramatičan porast zlonamjernih PDF datoteka od 1.160%-sa 411.800 zlonamjernih datoteka na 5.224.056. PDF datoteke su primamljivi vektor krađe

identiteta budući da su međuplatformske i omogućuju napadačima interakciju s korisnicima, čineći njihove sheme vjerodostojnijima za razliku od e-pošte zasnovane na tekstu s jednostavnom vezom [13]

Kako bi namamili korisnike da kliknu na ugrađene veze i gumbe u phishing PDF datotekama, identificirano je pet najboljih shema koje su napadači koristili 2020. za izvođenje phishing napada, a koje se mogu klasificirati kao: [13]

- lažna Captcha,
- kupon,
- gumb za reprodukciju,
- dijeljenje datoteka i
- e-trgovina.

Prema istraživanjima iz 2020.[2] primijećeno je povećanje postotka zlonamjernih PDF datoteka u odnosu na 2019. godinu (tablica 1.)

Tablica 1. Primjer porasta phishinga među pdf datotekama [13]

	Zlonamjerni softver (Malware)	Ukupno viđeno PDF datoteka	Postotak zlonamjernog softvera za PDF	Povećanje postotka
2019.	411,800	4,558,826,227	0.009%	1,160%
2020.	5,224,056	6,707,266,410	0.08%	

3.1.4. Hakiranje

Hakiranje je jedan od najčešće analiziranih i raspravljanih oblika cyber-kriminalnih aktivnosti i služi kao intenzivan fokus za zabrinutost javnosti zbog prijetnje koju takva

[2] Istraživanje Palo Alto Networks WildFire platform

aktivnost predstavlja za društvo. Jasna definicija hakiranja je "neovlašteni pristup i naknadna uporaba tuđih računalnih sustava" [14] .

Prijašnji hakeri voljeli su tehnologiju i cilj im je bio potisnuti programe izvan onoga za što su dizajnirani. Riječ haker nije imala negativnu konotaciju kao danas. Napadi se odvijaju u nekoliko faza, poput prikupljanja informacija ili izviđanja, skeniranja i konačnog ulaska u ciljni sustav. Prikupljanje informacija uključuje metode dobivanja informacija ili otvaranja sigurnosnih rupa. To je baš kao i način na koji se provodi tradicionalna vrsta pljačke. Razbojnik će prije pokušaja saznati sve podatke o mjestu koje želi opljačkati. Upravo će ovako računalni napadač pokušati saznati informacije o meti. Društveni inženjering jedna je od metoda koju napadač koristi za dobivanje informacija. Postoje dvije glavne kategorije u koje se mogu klasificirati svi pokušaji društvenog inženjeringa, računalna ili tehnološka obmana i obmana zasnovana na ljudima [15].

Pristup temeljen na tehnologiji je zavaravanje korisnika u uvjerenju da je u interakciji s "pravim" računalnim sustavom (kao što je skočni prozor, obavještavanje korisnika da je računalna aplikacija imala problem i slično) te navođenje korisnika da pruži povjerljive podatke. Ljudski pristup postignut je obmanom, iskorištavanjem žrtvinog neznanja i prirodne ljudske sklonosti da bude od pomoći. Prijetnja organiziranog kriminala i terorističkih aktivnosti postaje sve sofisticiranija kako sposobnost ulaska, kontrole i uništavanja elektroničkih i sigurnosnih sustava raste podjednakom brzinom. Danas su svakako e-pošta i Internet najčešće korišteni oblici komunikacije i razmjene informacija. Nešto više od 2 milijarde ljudi koristi internet svaki dan.

3.1.5. Kibernetičko uznemiravanje ili zastrašivanje

Kibernetičko uznemiravanje ili zastrašivanje upotreba je elektroničkih informacija i komunikacijskih uređaja kao što su e-pošta, trenutne poruke, tekstualne poruke, blogovi, mobilni telefoni, dojavljivači, trenutne poruke i web stranice za zlostavljanje ili na drugi način uznemiravanje pojedinca ili neka druga sredstva [15].

Cyber-maltretiranje, podsmjehivanje, uvrede i uznemiravanje putem Interneta ili tekstualne poruke poslane s mobilnih telefona postale su rasprostranjene među mladima, u nekim slučajevima s tragičnim posljedicama.

3.1.6. Krađa identiteta

Krađa identiteta je radnja pribavljanja osjetljivih podataka o drugoj osobi bez njezinog znanja i korištenje tih podataka za počinjenje krađe ili prijevare. Internet je kibernetičkim kriminalcima dao priliku da takve podatke dobiju iz baze podataka ranjivih tvrtki. Također im je omogućio da navedu žrtve da vjeruju da otkrivaju osjetljive osobne podatke legitimnom poslu; ponekad kao odgovor na e-poštu koja traži ažuriranje podataka o naplati ili članstvu; ponekad ima oblik prijave za (lažno) oglašavanje posla na Internetu.

Prema Parlamentarnoj skupini All Party, dostupna istraživanja, kako u Velikoj Britaniji, tako i na globalnoj razini, ukazuju na to da je prijevara identiteta veliki i rastući problem zbog eskalirajućih i razvijajućih metoda dobivanja i korištenja osobnih podataka. Nakon toga se očekuje daljnje povećanje u narednim godinama. Ovo je pitanje prepoznato na najvišim razinama vlasti [16].

3.1.7. Prevare s kreditnim karticama i ostale prijevare putem interneta

Prevara s kreditnom karticom je neovlašteno korištenje kreditnih kartica ili krađa kartice za dobivanje novca ili imovine. Ovakve prijevare obuhvaćaju sve prijevare koje uključuju plaćanje putem Interneta, telefonom ili poštom. Problem u suzbijanju ove vrste prijevara leži u činjenici da niti kartica niti njezin vlasnik nisu prisutni na fizičkom mjestu do trgovine u trgovini. Postoje brojni načini koje prevaranti koriste za dobivanje kartica i podataka o kartici, poput krađe identiteta, slanja neželjene e-pošte ili hakiranja baze podataka tvrtki.

Prijevara na internetskoj aukciji nastaje kada su kupljeni predmeti lažna ili ukradena roba ili kada prodavatelj oglašava nepostojeće artikle za prodaju, što znači da se roba plaća, ali nikada ne stiže. Prevaranti često koriste usluge prijenosa novca jer im je lakše primiti novac bez otkrivanja svog pravog identiteta. Prijevara na aukcijama klasičan je primjer

kriminalaca koji se oslanja na anonimnost interneta. Neke od najčešćih pritužbi uključuju: [15]

- kupce koji kasne s primanjem robe ili je uopće ne dobivaju,
- prodavatelje koji ne primaju uplate,
- kupce koji primaju robu koja je ili manje vrijedna od one koja je oglašena ili se značajno razlikuje od izvornog opisa,
- neuspjeh kako bi otkrili relevantne informacije o proizvodu ili uvjetima prodaje.

Ovi lažni "prodavači" koriste ukradene osobne iskaznice kada se registriraju na aukcijskim stranicama pa je njihovo praćenje općenito vrlo težak zadatak.

3.2. Kibernetičko ratovanje

Svaka internetska aplikacija potencijalni je prijenosnik nekog od virusa ili drugog zlonamjernog softvera; stoga slanje internetskih poruka nije iznimno. Kriminalci koriste ove uobičajene metode chata u svrhe krađe osobnih dokumenata upoznavajući pojedince s kojima komuniciraju ili putem širenja zlonamjernog softvera, špijunskog softvera i virusa. E-pošta kritičan je alat u rukama kriminalaca. Ne samo da je e-pošta jedan od najbržih i najjeftinijih medija koji šalju neželjenu poštu i krađu identiteta, već ih je lako manipulirati u prijenos smrtonosnih virusnih napada koji mogu uništiti cijelu korporacijsku mrežu u roku od nekoliko minuta [15].

Neki se virusi prenose putem e-poruka bezopasnog izgleda i mogu se pokrenuti automatski bez potrebe za intervencijom korisnika. Tehnički, napadi na „sigurnost sustava koja se može provesti putem elektroničke pošte“ mogu se kategorizirati na sljedeće: [14]

1. napadi na aktivni sadržaj koji koriste različite aktivne HTML (jezik za označavanje hiperteksta) i druge značajke skriptiranja i programske pogreške.
2. napadi, gdje napadač šalje nešto preveliko da se uklopi u memorijski međuspremnik fiksne veličine primatelja e-pošte, u nadi da će dio koji se ne uklapa prebrisati kritične informacije, a ne biti sigurno odbačen.

4. OPASNOST OD UCJENJIVAČKOG SOFTVERA - RANSOMWARE (simulacija analiza) – primjer

Zlonamjerni softveri neprestano se pojavljuju kao prijetnje. Brzi razvoj Internet stvari (IoT) jednako je pridonio ovoj prijetnji pružajući veći prostor za napade. Sve što svakodnevno koristimo u svom životu sada ima potencijal da se poveže na mreži i surađuje kao jedno, a sve što je povezano je ranjivo. Ransomware je kategorija zlonamjernog softvera koja se širi poput crva i onemogućuje ili ograničava pristup korisnika njihovom sustavu, bilo zaključavanjem zaslona sustava ili šifriranjem i zaključavanjem datoteka korisnika, osim ako se ne plati otkupnina[17].

Ransomware je posebna klasa zlonamjernih programa koja zahtijeva plaćanje u zamjenu za ukradenu funkcionalnost, uglavnom podatke. Ova klasa zlonamjernog softvera identificirana je kao glavna prijetnja sigurnosti računala i mreže diljem svijeta[18]. Ransomware se tajno instalira na žrtvin uređaj kako bi se montirao napad kriptoviralnog iznuđivanja iz kriptovirologije koji drži žrtvine podatke kao taoce, ili napad kriptovirološkog curenja koji prijeti objavljivanjem podataka žrtve. Prava meta ovog oblika napada su kritični podaci koji su podjednako važni za pojedince i poduzeća. Zapravo, napad se proširio na mobilne uređaje i pristupi otkrivanja mobilnog zlonamjernog softvera nisu toliko učinkoviti zbog suptilne prirode zlonamjernih programa[19]. Stoga su milijarde korisnika mobilnih uređaja podložne ovom napadu.

Većina varijanti ransomware-a ovisi o šifriranju datoteke kao strategiji iznude. Podaci pohranjeni na uređaju žrtve šifrirani su dok haker traži otkupninu prije nego što se datoteke mogu dešifrirati. Ransomware može kriptirati tablicu glavnih datoteka računala (MFT) ili cijeli hard disk. To je napad uskraćivanja pristupa koji onemogućuje korisnicima računala pristup datotekama jer je nemoguće dešifrirati datoteke bez ključa za dešifriranje. Napadi otmičarskog softvera obično se izvode pomoću trojanca koji ima korisni teret prikriven kao legitimna datoteka. Iako su napredni algoritmi za šifriranje korisni za učinkovitu zaštitu vitalnih podataka poduzeća, postali su alati za zlonamjerne napade u

rukama cyber-kriminalaca. Zaštita podataka je stoga pod ozbiljnom prijetnjom jer hakeri nastavljaju koristiti poboljšane algoritme u napadima ransomware-a. Digitalno iznuđivanje značajno se povećalo u posljednjih šest godina kako broj online aplikacija i usluga, a pametni mobilni uređaji nastavljaju eksponencijalno rasti. Utjecaj ransomware-a postao je toliko ogroman da je sada ocijenjen kao najveća cyber prijevara koja je pogodila tvrtke. Oko 80% napada ransomware-a iskorištava ranjivosti u *Flashu* koje su tvrtke trebale zakrpati. Razorni ransomware može se sam širiti i držati čitave mreže (tj. Tvrtke) kao taoce[19].

Ransomware se obično sastoji od neuništive enkripcije koja posljedično onemogućuje dešifriranje. Napadači obično šifriraju kritične poslovne podatke organizacije nakon što su se infiltrirali u njezine sustave, nakon čega zahtijevaju novčanu uplatu u digitalnim gotovinskim formatima kao što je „Bitcoin“ [20]. Bitcoin se sastoji od tehnika šifriranja koje se koriste za reguliranje stvaranja novčanih jedinica, pri čemu se provjera prijenosa sredstava dovršava neovisno o središnjoj banci.

4.1. Povijesni razvoj ransomware-a

PC Cyborg prijavljen je kao prva varijanta ransomwarea [21]. Napad zlonamjernog softvera pokrenut je u prosincu 1989. Žrtva je prevarena prikazom poruke na kojoj je navedeno da je korisnička licenca istekla. Međutim, algoritam za šifriranje, simetričnu kriptografiju, nije bilo teško dešifrirati [22]. GpCode također je koristio prilagođenu simetričnu enkripciju, ali se zlonamjerni softver s vremenom poboljšavao. Zlonamjerni softver propagiran je kao oglas za posao putem privitka neželjene e-pošte. U svom prvom napadu u svibnju 2005., generiran je statički ključ za šifriranje svih datoteka izvan sustava. Izvorni podaci izbrisani su čim je šifriranje dovršeno [23]. Međutim, ključ je otkriven jednostavnom usporedbom izvornih podataka sa šifriranim podacima. Nova varijanta GpCodea, nazvana GpCode.AG otkrivena je u lipnju 2016. Njegova je enkripcija temeljena na 660-bitnom RSA javnom ključu. U lipnju 2008. identificirana je druga varijanta, GpCode.AK, no bilo ju je jako teško probiti zbog računalne potražnje. Reveton, također poznat kao Police Ransomware, obično se širi putem pornografskih web stranica [24].

Mijenja proširenja u mapi windows/system32 i prikazuje stranicu s obavijestima žrtvama [25].

Locker Ransomware je identificiran 2007. Ne dira podatke svojih žrtava, već samo zaključava njihove uređaje. Stoga se podaci na uređaju mogu prenijeti na drugo mjesto. Slično, ColdBrotherRansomware zaključava mobilne uređaje žrtava, fotografira kamerama mobilnih telefona, odgovara i odbacuje dolazne pozive te nastoji prevariti žrtve putem aplikacija za mobilno bankarstvo. Kripto Ransomware kriptira kritične datoteke na računalu žrtava kao korisno opterećenje za iznudu. Važne datoteke identificiraju se i šifriraju ključevima "teško pogodljivim". Odabir ključeva za šifriranje i koordinaciju napada vrši poslužitelj za naredbe i upravljanje CryptoWall, Tesla Crypt, CTB Locker i Lock sve su varijante Crypto Ransomwarea [25].

4.2. Vrste ransomware-a

Kada je riječ o vrstama ransomware-a razlikuju se [26]:

1. Šifrirani Ransomware - ransomware koji kombinira inovativne algoritme za šifriranje namijenjene blokiranju pristupa datotekama koje zahtijevaju otkupninu za dešifriranje datoteka. Primjeri šifrirajućeg ransomware-a su “CryptoLocker”, “Locky”, „CryptoWall”, a najnoviji je“ WannaCrypt ”.
2. Locker Ransomware je vrsta zlonamjernog softvera koji zaključava metu izvan operacijskog sustava, pa posljedično sprječava pristup radnoj površini, aplikacijama i datotekama. Primjer ovakvog ransomware-a je “Winlocker”.
3. Ransomware uobičajeni vektori napada. Odnose se na zlonamjere privitke e-pošte: Napadač kreira e-mail pretvarajući se da je iz vjerodostojnog izvora, na primjer računa, odjela za ljudske resurse ili informacijsku tehnologiju, te prilaže zlonamjernu datoteku u datoteku Microsoft Word ili sličnu datoteku dokumenta [26]. Primatelj e-pošte otvara privitak i nesvjesno preuzima ransomware koji inficira njihov sustav što dovodi do toga da se njihove datoteke drže kao otkupnina. Kripto-ransomware pod nazivom "Locky" infiltrira se u sustav žrtava putem e-pošte

kamuflirane kao faktura s usklađenim dokumentom Microsoft Word koji je ugrađen u zlonamjerne makronaredbe. Ove makronaredbe izvršava zlonamjerni softver nakon preuzimanja. Općenito, makronaredbe su zadano onemogućene u programu Microsoft Word; međutim omogućavanje makronaredbi čini sustav ranjivim na potencijalni zlonamjerni kod. Jednom kada je sustav zaražen, zlonamjerni softver Locky traži izravno spojene i mrežne diskove i šifrira datoteke s nastavkom ".locky" ostavljajući iza sebe otkupnu poruku za dešifriranje datoteka [26]. Zlonamjerne veze e-pošte - URL-ovi (*Uniform Resource Locator*) u obliku e-pošte šalju se iz navodno pouzdanih izvora. Nakon klika na te URL-ove, zlonamjerne datoteke preuzimaju se s Interneta i zaraze sustav i drže njegove datoteke za otkupninu. Evolucija napada zlonamjernim softverom pojednostavila je njegovo izvršavanje pa je svaka organizacija ili pojedinac postala moguća žrtva ransomware-a. Kompleti za iskorištavanje su sofisticirani alati za iskorištavanje ranjivosti definirani kao kompleti za iskorištavanje koji se izvršavaju kada žrtva posjeti ugroženu web stranicu. Zlonamjerno oglašavanje je zlonamjerni kod koji se često skriva u oglasu koji ga neopaženo preusmjerava na web stranicu kompleta za iskorištavanje. Na nezaštićenom sustavu izvršit će se preuzimanje zlonamjernog korisnog tereta putem pogona čime će se zaraziti sustav i zadržati njegove datoteke radi otkupnine. Trenutno najrazorniji komplet za iskorištavanje ransomware-a je "WannaCry" ili "WannaCrypt" ransomware.

4. Destruktivna skala podrške ransomware-u za Windows XP ukinuta je 8. travnja 2014. međutim Microsoft je isporučio dodatnu javnu zakrpu za 16 -godišnji operacijski sustav Windows XP za borbu protiv napada ransomware-a „WannaCrypt“ [24]. Ovaj krajnje neobičan korak učinjen je nakon što su klijenti diljem svijeta, uključujući englesku Nacionalnu zdravstvenu službu, pretrpjeli napad od strane programa "WannaCrypt" ransomware [24]. Microsoft je u ožujku zakrpao sve svoje trenutno podržane sustave kako bi popravio grešku, no nakon silnih učinaka ransomware-a WannaCrypt, Microsoft je objavio ažuriranje dostupno za nepodržane sustave kao što su Windows XP, Windows 8 i Windows Server 2003. Posljednje ažuriranje za Windows Service Pack 3 objavljeno je 13. svibnja 2017.

5. Plaćanja otkupljivača nakon postizanja šifriranja datoteka, softver za ransomware obično će prikazati prozor GUI koji prikazuje korisniku da su njegove datoteke šifrirane i nudi im način plaćanja za oporavak datoteka (Microsoft, 2017.) s potrebnim ključem za dešifriranje. Kao što je ranije rečeno, plaćanje ransomware-a vrši se putem Bitcoina. Dodatno šifriranje izvornog AES ključa javnim ključem onemogućuje dešifriranje datoteka bez privatnog ključa [24].

4.3. Primjer slučaja ransomware-a

Primjer BitPaymer

CrowdStrike® Intelligence identificirao je novu varijantu ransomware-a koja se identificira kao BitPaymer. Ova nova varijanta stajala je iza niza kampanja protiv ransomware-a koje su započele u lipnju 2019., uključujući napade na grad Edcouch u Teksasu i čileansko Ministarstvo poljoprivrede [27].

Ovaj novi ransomware nazvan je DoppelPaymer jer dijeli većinu svog koda s BitPaymer ransomware-om kojim upravlja INDRIK SPIDER. Međutim, postoje brojne razlike između DoppelPaymera i BitPaymera, što može značiti da su se jedan ili više članova INDRIK SPIDER-a odvojili od grupe i razdužili izvorni kod i Dridexa i BitPaymera kako bi započeli vlastitu operaciju otkupninskog softvera Big Game Hunting [27].

Podrijetlo Indrikspider-a

INDRIK SPIDER osnovan je 2014. bivši pripadnici kriminalne mreže GameOver Zeus koji su se interno nazivali "Poslovni klub". Ubrzo nakon osnivanja grupe, INDRIK SPIDER razvio je vlastiti prilagođeni zlonamjerni softver poznat kao Dridex. Rane verzije Dridex-a bile su primitivne, ali s godinama zlonamjerni softver postao je sve profesionalniji i sofisticiraniji. Zapravo, operacije Dridex-a bile su značajne tijekom 2015. i 2016. godine, što ga čini jednom od najčešćih obitelji zlonamjernog softvera eCrime. U to je vrijeme INDRIK SPIDER primarno provodio žičane prijevare, što je rezultiralo gubitkom milijuna dolara na globalnoj razini [27].

S vremenom je INDRIK SPIDER naišao na brojne prepreke u svojim operacijama prijevare putem žice. Prvo, 2015. grupa je morala prevladati operaciju uklanjanja, što je rezultiralo uhićenjem jedne od njezinih podružnica, koja je koristila pseudonim "Smilex". Nakon ovog zastoja uslijedila je operacija provođenja zakona u Velikoj Britaniji osmišljena da razbije mrežu za pranje novca koja podržava monetizaciju kampanja Dridex-a od INDRIK SPIDER-a. Demontiranje ove mreže također se poklopilo s uhićenjem, a potom i zatvorom, zaposlenika jedne britanske banke koji je pomogao u postavljanju lažnih računa [27].

Možda je kao posljedica ovih prepreka INDRIK SPIDER promijenio svoje metode rada 2017. godine, provodeći manje distribucijske kampanje Dridex-a. U kolovozu 2017. grupa je predstavila BitPaymer ransomware i počela se usredotočivati na povećanje pristupa unutar organizacije žrtve kako bi zahtijevala visoku otkupninu.

Podrijetlo BitPaymera

CrowdStrike Intelligence, pratio je izvorni BitPaymer od kada je prvi put identificiran u kolovozu 2017. U svojoj prvoj iteraciji, bilješka o otkupnini BitPaymer-a uključivala je zahtjev za otkupninu i URL za portal za plaćanja temeljen na TOR-u. Portal za plaćanje sadržavao je naslov "Bit paymer" zajedno s referentnim ID-om, Bitcoin (BTC) novčanikom i e-adresom za kontakt. Primjer ovog portala prikazan je na slici 2.

Slika 2. Primjer Bit paymera [27]

Unutar prvog mjeseca rada iznos otkupnine je ispušten iz otkupnine. U srpnju 2018. uklonjen je i URL portala za plaćanje. Od srpnja 2018. do danas, otkupnina je uključivala samo dvije e-poruke za kontakt koje se koriste za pregovaranje o otkupnini.

Najnovija verzija BitPaymera

U studenom 2018. došlo je do značajnog ažuriranja BitPaymera. Bilješka o otkupnini ažurirana je tako da uključuje ime žrtve, a ekstenzija datoteke dodana šifriranim

datotekama također je prilagođena tako da koristi prikaz imena žrtve. Primjer nove otkupnine je prikazan ispod na slici 3.

Slika 3. Primjer otkupnine [27]

Uz ažuriranu napomenu o otkupnini i šifriranu ekstenziju datoteke, BitPaymer-ova rutina šifriranja datoteka ažurirana je tako da koristi 256-bitni AES u načinu lančanog bloka šifriranja (CBC) s nasumično generiranim ključem i vektorom NULL inicijalizacije. Prethodne verzije BitPaymer-a koristile su 128-bitni RC4 [27]

Budući da je AES blok-šifra, implementacija zahtijeva *„padding“* u slučajevima kada podaci nisu višekratnici veličine bloka. Obično se to provodi dodavanjem nula ili broja n bajtova za dodavanje n puta (također poznato kao PKCS#7). Međutim, INDRIK SPIDER odlučio je nasumično generirati n bajtova za dodavanje. Kao rezultat toga, programer zlonamjernog softvera morao je sačuvati nasumične bajtove za dodavanje kako bi ispravno dešifrirao posljednji podatkovni blok šifrirane datoteke. To se odražava u

bilješci o otkupnini BitPaymer-a s novim poljem TAIL-a, kao što je prikazano gore na slici 2, koje sadrži TAIL padding kodiran Base64 i šifrirani AES KEY [27].

Programeri BitPaymer-a implementirali su funkciju inicijalizacije enkripcije u kodu ransomware-a koja odabire jedan od tri željena algoritma za šifriranje. Algoritam se bira argumentom koji se kao cjelobrojni parametar prenosi funkciji. Podržane trenutne vrijednosti su 1, 2 i 3 za 128-bitni RC4, 128-bitni AES i 256-bitni AES. Novije verzije BitPaymer-a prenose tvrdo kodiranu vrijednost 3 za 256-bitnu AES enkripciju u funkciju, kao što je prikazano na slici 4.

```
if ( CryptoAlgorithm == 1 )
{
  crypto->CryptoAlgorithm = CALG_RC4;
}
else
{
  if ( CryptoAlgorithm != 2 )
  {
    if ( CryptoAlgorithm == 3 )
    {
      crypto->CryptoAlgorithm = CALG_AES_256;
      crypto->KeySize = 32;
    }
    else
    {
      crypto->CryptoAlgorithm = 0;
      crypto->KeySize = 0;
    }
    goto CRYPTO;
  }
  crypto->CryptoAlgorithm = CALG_AES_128;
}
crypto->KeySize = 16;
```

Slika 4. AES enkripcija [27]

Uz ažuriranu rutinu šifriranja datoteka, veličina RSA javnog ključa za žrtvu također je povećana sa 1.024-bitna na 4.096-bitna. Ovaj asimetrični ključ koristi se za šifriranje generiranih simetričnih ključeva za šifriranje datoteka. Ako je otkupnina plaćena, INDRIK SPIDER će osigurati alat za dešifriranje koji sadrži RSA privatni ključ odgovarajuće žrtve. INDRIK SPIDER prešao JE s RC4 na AES enkripciju, što je vjerojatno posljedica

zabrinutosti o relativnoj slabosti RC4 u usporedbi s AES -om. Povećanje veličine ključa RSA također uvelike povećava kriptografsku snagu štiteći ključeve za šifriranje datoteka. Međutim, nema dokaza da je prethodno ili trenutno šifriranje BitPaymer-a prekinuto [27].

Od ažuriranja u studenom 2018., INDRIK SPIDER aktivno je koristio najnoviju verziju BitPaymer-a u najmanje 15 potvrđenih napada ransomware-a. Ti su se napadi nastavili tijekom 2019., a više se incidenata dogodilo samo u lipnju i srpnju 2019. godine.

DoppelPaymer

Dok su prve poznate žrtve DoppelPaymera bile ciljane u lipnju 2019., uspjeli su se oporaviti ranije verzije zlonamjernog softvera koje datiraju iz travnja 2019. Tim ranijim verzijama nedostaju mnoge nove značajke koje se nalaze u kasnijim varijantama, pa nije jasno da li su bili raspoređeni žrtvama ili su jednostavno napravljeni za testiranje.

Do danas je identificirano osam različitih verzija zlonamjernog softvera i tri potvrđene žrtve s iznosima otkupnine od 2 BTC, 40 BTC i 100 BTC. Na temelju tečaja USD-a i BTC -a otkupnine variraju od približno 25.000 USD do preko 1.200.000 USD [27].

Bilješka o otkupnini koju koristi DoppelPaymer slična je onima koje je koristio izvorni BitPaymer u 2018. Bilješka ne uključuje iznos otkupnine; međutim, on sadrži URL za portal za plaćanja temeljen na TOR-u, a umjesto korištenja ključne riječi KEY za identifikaciju šifriranog ključa, bilješka koristi ključnu riječ DATA.

5. SLUČAJ NAPADA RANSOMWARE-A – NACIONALNI ZDRAVSTVENI SUSTAV U ENGLESKOJ

Jedan od najpoznatijih primjera napada ransomware-a koji je u proljeće 2017. pogodio tvrtke diljem svijeta bila je epidemija WannaCry, koja je zahvatila više od 200.000 računala u preko 150 zemalja. To je Englesku koštalo 92 milijuna funti i povećalo globalne troškove do nevjerojatnih 6 milijardi funti [28].

U ovom slučaju ransomware, poznat kao 'WannaCry', često se isporučuje putem e-pošte koja primatelja vara da otvori privitke i pusti zlonamjerni softver u svoj sustav u tehnici poznatoj kao *phishing*. Nakon što je računalo pogođeno, ono zaključava datoteke i šifrira ih na način da im više ne možete pristupiti. Zatim zahtijeva plaćanje u Bitcoinu kako bi se vratio pristup.

Kako je došlo do napada i na što je utjecalo?

Na datum 12. svibnja 2017., Nacionalni zdravstveni sustav (u daljnjem tekstu NZS), engl. *National Health Service* – NHS, je nekoliko dana bio u zastoju zbog pojave „WannaCry“ (slika 5.) koja je utjecala na bolnice i opće ordinacije diljem Engleske i Škotske. Iako NZS nije bio posebno ciljan, globalni kibernetički napad istaknuo je sigurnosne ranjivosti i rezultirao otkazivanjem tisuća zakazanih termina i operacija, zajedno s bjesomučnim preseljenjem hitnih pacijenata iz hitnih centara hitne pomoći. Osoblje je također bilo prisiljeno preći na olovku i papir te koristiti vlastite mobitele nakon što je napad utjecao na ključne sustave, uključujući telefone [28].

Slika 5. WannaCry ransomware [29]

WannaCry ransomware otkrio je specifičnu ranjivost sustava Microsoft Windows, a ne napad na nepodržani softver. Utvrđeno je da je većina uređaja Nacionalnog zdravstvenog sustava zaraženih ransomware-om radila na podržanom, ali bez zakrpe, operacijskom sustavu Microsoft Windows 7, otuda i kibernetički napad. Ransomware se proširio i putem interneta, uključujući i putem mreže N3 (širokopojasna mreža koja povezuje sva web mjesta NZS u Engleskoj), ali na sreću nije bilo slučajeva širenja ransomware-a putem e-maila NZS.

Nacionalni zdravstveni sustav Engleske je izvijestio da je najmanje 80 od 236 ustanova bilo pogođeno uz 603 primarne zdravstvene zaštite i drugih organizacija NZS-a, uključujući 595 liječnika opće prakse. Ministarstvo, NZS Engleske i Nacionalna agencija za borbu protiv kriminala izvijestili su da nijedna NZS organizacija nije platila otkupninu, ali Odjel ne zna koliko su te smetnje u uslugama koštale NZS iako se procjenjuje da je ukupna šteta iznosila 92 milijuna funti. [28]

Tko je stajao iza napada?

U napadu je korišten EternalBlue, naziv za programsku ranjivost u Microsoftovom operacijskom sustavu Windows, koji funkcionira iskorištavanjem Microsoft Server MessageBlock 1.0. Blok poruka poslužitelja (SMB) mrežni je protokol za dijeljenje datoteka i omogućuje aplikacijama na računalu čitanje i pisanje u datoteke i traženje usluga koje su na istoj mreži [28].

Američka Agencija za nacionalnu sigurnost ga je razvila za iskorištavanje kibernetičkog napada. Iako je objavljeno da su znali za ranjivosti alata, Američka agencija za nacionalnu sigurnost na to nije skrenula pozornost Microsofta sve dok hakerska skupina pod nazivom Shadow Brokers nije pustila EternalBlue na opskurnu web stranicu [28].

Što je izazvalo napad?

U utorak, 14. ožujka 2017., Microsoft je izdao sigurnosni bilten u kojem je detaljno opisan nedostatak i objavljene su zakrpe za sve verzije sustava Windows koje su tada bile podržane. Ministarstvo zdravstva upozoreno je na rizike od cyber napada na NZS godinu dana prije WannaCryja, a iako je normalno funkcioniralo, formalno nije odgovorilo pisanim izvješćem do srpnja 2017. [28].

U vrijeme napada NZS je bio kritiziran zbog korištenja zastarjelih IT sustava, uključujući Windows XP, 17-godišnji operativni sustav koji bi mogao biti osjetljiv na kibernetičke napade. Neobičnim potezom, Microsoft je objavio zakrpu WannaCry za nepodržane sustave poput Windows XP koju je Microsoft prestao podržavati 2014. godine. NZS nije se pripremio za nacionalni kibernetički napad, nije odmah bilo jasno tko bi trebao voditi odgovor. Bilo je problema s komunikacijom jer su e-poruke ili zaražene ili zatvorene kako bi se spriječilo širenje ransomware-a. Jasno je da tadašnji plan oporavka od katastrofe nije uzimao u obzir kibernetički napad ovakvih razmjera, niti je bilo komunikacijskih nepredviđenih situacija ako je glavna mreža bila nedostupna. Prema ocjeni Povjerenstva za kvalitetu skrbi, nije postojala jasna veza između ustanova zaraženih WannaCryjem i kvalitete njihova vodstva [28].

Što je zaustavilo napad?

Kibernetički napad je zaustavljen prekidačem za slučajno suzbijanje koji je otkrio Marcus Hutchins, istraživač računalne sigurnosti, registrirajući domenu koju je ransomware programirao za provjeru. U tjedan dana nakon toga taj prekidač postao je meta moćnih botneta koji su željeli isključiti domenu izvan mreže i izazvati još jednu epidemiju.

Zaključak kibernetičkog napada na NZS

Prema Nacionalnoj agenciji za kriminal (NCA), ransomware ostaje najčešća metoda cyber iznude u Velikoj Britaniji, dok se tehnička vještina potrebna za vršenje cyber napada nastavlja smanjivati. Izvješće koje se temelji na zahtjevu FOI-a SolarWindsa otkrilo je da se smanjio ukupni postotak ispitanika javnog sektora u Velikoj Britaniji koji su doživjeli cyber napad u 2018. u odnosu na 2017. (38% nije doživjelo cyber napade u 2018., dok 30% nije doživjelo nijedan u 2017.), bilo je i više organizacija koje su doživjele preko 1.000 cyber -napada - 18% u 2018. u odnosu na 14% u 2017. godini.

Sigurnosni stručnjaci upozorili su da cyber kriminalci zdravstveni sektor vide kao posebno unosnu metu zbog zdravstvenih kartona koje ima u količinama deset puta većima od ostalih podataka, poput primjerice bankovnih podataka. Devet mjeseci nakon napada, "NHS Digital" je otkrio da niti jedan od 200 NZS-ovih ustanova nije prošao inspekciju ranjivosti u cyber sigurnosti. Većina grešaka odnosila se na zakrpe.

Nedovoljno financiranje istaknuto je kao glavni razlog zašto NZS još uvijek koristi sustave podrške i nije dostigao standarde kibernetičke sigurnosti. U prosincu 2015. Nacionalni revizorski ured (engl. *National Audit Office*, NAO) je zaključio da kontinuirano pogoršanje financijskog poslovanja nije održivo te da su financijski problemi u NZS-u endemični. Napad WannaCry pokrenuo je poticanje ulaganja vlade u cyber sigurnost u NZS-u. Ovo je klasičan primjer kako nedostatak razumijevanja o rizicima vezanim uz ranjivosti kibernetičke sigurnosti nije jamčio dovoljnu razinu financiranja za podmirivanje rastućih potreba velikih javnih institucija poput NZS -a.

Postoje daljnji dokazi da se razumijevanje kibernetičke sigurnosti od strane višeg rukovodstva u javnom sektoru Velike Britanije mora poboljšati. U nedavnom istraživanju Sophosa, zabrinjavajućih 55% IT čelnika javnog sektora vjeruje da su digitalni podaci njihove organizacije manje vrijedni od podataka privatnog sektora. 36% IT čelnika kaže da je zapošljavanje i zadržavanje stručnjaka za kibernetičku sigurnost najveći izazov, dok se čini da IT stručnjaci na prvoj liniji nemaju dovoljno resursa, a samo 14% njih zabrinuto je

zbog nedostatka takvih vještina. Jasno je da postoji komunikacijski most koji treba propustiti [28].

Očekuje se da će tehnologija "transformirati" NZS. Inovacije poput povećane uporabe umjetne inteligencije, računalstva u oblaku i povezanih uređaja mogu podržati učinkovitiju skrb. No, kako se zdravstvena zaštita više oslanja na tehnologiju, rizik od cyber poremećaja također će se značajno povećati, osim ako se ne poduzmu odgovarajuće mjere.

6. ZAKLJUČAK

Računalnim kriminalom krši se privatnost pojedinaca i sigurnost njihovih podataka, osobito hakiranjem, zlonamjernim softverom, krađom identiteta, financijskim prijevarama, medicinskim prijevarama i određenim prekršajima protiv osoba koji uključuju otkrivanje osobnih podataka, poruka, slika i video i audio zapisa.

Podaci igraju integralnu ulogu u počinjenju mnogih kibernetičkih zločina i ranjivosti na kibernetički kriminal. Iako podaci korisnicima (pojedincima, privatnim tvrtkama, organizacijama i vladama) pružaju nebrojene mogućnosti, neki ih mogu (a neki i jesu) iskoristiti u kriminalne svrhe. Konkretno, prikupljanje, pohrana, analiza i razmjena podataka omogućuju mnoge kibernetičke zločine i ogromno prikupljanje, pohranu, upotrebu i distribuciju podataka bez pristanka i izbora korisnika te potrebne pravne i sigurnosne zaštite. Štoviše, skupljanje, analiza i prijenos podataka događaju se u razmjerima za koje vlade i organizacije nisu spremne, stvarajući niz rizika kibernetičke sigurnosti. Privatnost, zaštita podataka i sigurnost sustava, mreža i podataka međusobno su ovisni. S obzirom na to, za zaštitu od kibernetičkog kriminala potrebne su sigurnosne mjere koje su osmišljene za zaštitu podataka i privatnosti korisnika.

Ransomware je jedan od najvećih sigurnosnih problema na internetu i jedan od najvećih oblika kibernetičkog kriminala s kojim se organizacije danas suočavaju. On šifrira datoteke i dokumente na bilo čemu od jednog računala pa sve do cijele mreže, uključujući poslužitelje. Žrtvama se često može ostaviti malo izbora; mogu ili vratiti pristup svojoj šifriranoj mreži plaćanjem otkupnine kriminalcima koji stoje iza ransomware-a, vratiti ih iz sigurnosnih kopija ili se nadati da postoji ključ za dešifriranje koji je dostupan.

Kibernetički napad koji je zahvatio više od 60 ustanova unutar Nacionalne zdravstvene službe Engleske proširio se na više od 200.000 računalnih sustava u 150 zemalja, WannaCry ransomware počeo je utjecati na desetke ustanova NZS-a. Na kraju je pogođeno više od 60 ustanova NZS-a. Mnoge ustanove nisu mogle pristupiti evidenciji pacijenata, što

je dovelo do kašnjenja operacija koje nisu hitne i otkazivanja pregleda pacijenata. Neke bolnice morale su preusmjeravati vozila hitne pomoći u druge ustanove.

Temeljni problem koji je prouzročio ovaj napad je propuštanje ulaganja u tehnologiju koja je mogla spriječiti napad. Iako se čini da NZS nije bio posebno ciljan od strane onih koji stoje iza WannaCry ransomwarea, bio je osjetljiv na napade, jer su neki od njegovih operativnih sustava Windows stari više od 15 godina i Microsoft ih više nije ažurirao niti podržavao.

Kibernetički kriminal napreduje iz dana u dan na sve većem nivou što nije ni čudno s obzirom na današnje okolnosti u kojima informatika postaje dio svakodnevnog života. Tijekom godina broj kibernetičkog kriminala sve više raste te je potrebna adekvatna zaštita. Osnovne stvari zaštite računala su antivirusni programi koji imaju i besplatnu verziju koja može pružiti dovoljno dobru sigurnost i zaštitu na internetu. Vrlo je važno obratiti pažnju na ispravnost rada antivirusnog programa, odnosno pravovremeno ga ažurirati. Uz antivirusne programe i redovito ažuriranje operativnog sustava na računalu, ne smijemo zanemariti ni ono osnovno – (ne)otvaranje email poruke od nepoznatog pošiljatelja, naročito ako ta ista ima privitak, blokirati skočne prozore u Internet pregledniku, koristit vatrozid (engl. *firewall*) te koristit postavke privatnosti u internetskom pregledniku.

POPIS LITERATURE

[1]Baća, M., Ćosić, J. Prevencija računalnog kriminaliteta, Policijska sigurnost, god, 22, br.1, 2013.

[2]Naughton, J. A BriefHistoryofthe Future: TheOriginsofthe Internet. Phoenix,London 1999.

[3]Grabosky, P. Computer Crime: A CriminologicalOverview. V: Forum on CrimeandSociety, United Nations Publications, New York, Vol.1., No.1, 2001., p. 35–53.

[4]Aghatise, J. Cybercrimedefinition, Computer Research Centre. dostupno na: http://www.crime-research.org/articles/joseph06/2, (10.kolovoza 2021.)

[5]Wall D.S. Crimeandthe Internet. Routledge, London, 2001., p. 44-58.

[6] Wall, D. S. , Cybercrime: TheTrasformationofCrimeintheInformation Age. Polity Press, Cambridge, Malden, 2007.

[7] Broadhurst, R., Alazab, M. Trends&issuesincrimeandcriminaljustice, Australian Institute ofCriminology, No. 526 December 2016.

[8]Računalna forenzika, dostupno na:

http://racfor.zesoi.fer.hr/doku.php?id=racfor_wiki:email:gmail_phishing, (12.kolovoza 2021.)

[9] Sharma, U.:Phishing-An Analysis on theTypes, Causes, Preventive MeasuresandCaseStudiesintheCurrentSituation, Conference: National Conference on AdvancesinEngineering, Technology & Management (AETM'15)Volume: IOSR Journal of Computer Engineering (IOSR-JCE),January 2015, p. 1-8

[10]Sharma, U. Phishing-An Analysis on theTypes, Causes, Preventive MeasuresandCaseStudiesintheCurrentSituation, Conference: National Conference on

AdvancesinEngineering, Technology & Management (AETM'15)Volume: IOSR Journal of Computer Engineering (IOSR-JCE) January 2015, p. 1-8

[11]Palmer, D. : Whatisphishing? Everythingyouneed to know to protectyourselffromscamemailsand more, dostupno na: https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more/, (20 kolovoza 2021.)

[12]Pauli, J. TheBasicsof Web HackingToolsandTechniques to Attackthe Web 2013, Elsevier, UK, 2013., p.105-123

[13]2020 PhishingTrendsWith PDF Files, https://unit42.paloaltonetworks.com/phishing-trends-with-pdf-files/, (12.kolovoza 2021.)

[14]Yar, M. CybercrimeandSociety. Sage PublicationLtd, London., 2006., str.23

[15]Jahankhani, H., Al-Nemrat, A., Hosseinian-Far, A. Cyber Crimeand Cyber TerrorismInvestigator'sHandbookChapter: 12Publisher: Elsevier Science, November 2014., pp.149-164.

[16]CIFAS, TheUK'sFraudPrevention Service, 2012., dostupno na: http://www.cifas.org.uk/, (11.kolovoza 2021).

[17]Deo, S. And M. FarikInformation Security - RecentAttacks In Fiji. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME, 2016. 5(12): p. 218-220.

[18]Gazet, A. "Comparativeanalysisofvariousransomwarevirii," Journal in Computer Virology, vol. 6, 2010., p. 77-90,

[19]Andronio, N. Zanero,S. Maggi, F. "HELDROID: Dissectinganddetectingmobileransomware," in 18th International Symposium on Research

inAttacks, Intrusions, andDefenses, RAID 2015 vol. 9404, H. Bos, G. Blanc, and F. Monrose, Eds., ed: Springer Verlag, 2015, pp. 382-404.

[20]Bartock, M. :Guide For Cybersecurity Event Recovery.NIST, USA, 2016,.

[21]Brewer, R.: Ransomwareattacks: detection, preventionand cure, Network Security, vol. 2016, 2016., pp. 5-9

[22]Kansagra,J. Kuhmar,HandJha,D.: Ransomware: A threat to Cyber-Security, CS Journals, vol. 7, 2016

[23]Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda: Cuttingthegordianknot: A lookunderthehoodofransomwareattacks, International Conference on DetectionofIntrusionsandMalware, andVulnerabilityAssessment, 2015, pp. 3-24

[24]Shah, N., Farik,M. Ransomware - Threats, VulnerabilitiesAndRecommendations, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 6, ISSUE 06, JUNE 2017, p. 307-309.

[25]Pathak, D.P., Nanded, Y. M.: A dangerous trend ofcybercrime: ransomwaregrowingchallenge, International Journal of Advanced Research in Computer Engineering& Technology (IJARCET), vol. 5, 2016.

[26]Zavarsky, Lindskog,D.: ExperimentalAnalysisofRansomware on Windows and Android Platforms: EvolutionandCharacterization,Procedia Computer Science, vol. 94, 2016.,pp. 465-472,

[27]Stone-Gross,B., Frankoff, S., Hartley, B.: BitPaymerSourceCodeFork: MeetDoppelPaymerRansomwareandDridex 2.0, dostupno na: https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/, (27. kolovoza 2021.)

[28]The NHS cyber attack, dostupno na: https://www.acronis.com/en-us/articles/nhs-cyber-attack/, (29.kolovoza 2021.)

[29] Digital TransformationWeekly: WannaCry cyber attackcost NHS £92m, dostupno na: https://zaizi.com/our-thinking/digital-transformation-weekly-wannacry-cyber-attack-cost-nhs-ps92m, (29.8.2021.)

POPIS SLIKA

POPIS TABLICA