Šolski center Celje
Srednja šola za strojništvo, mehatroniko in medije

NAPAD IN OBRAMBA V KIBERNETSKI VARNOSTI

Raziskovalna naloga

Področje: Računalništvo

Avtor:
Jan Zorc, M-4. e

Mentorja:
mag. Peter Arlič, univ. dipl. obl.
Žiga Pušelc, dipl. inž. el.

Celje, 2024

IZJAVA*

Mentorja mag. Peter Arlič in Žiga Pušelc v skladu z 20. členom Pravilnika o organizaciji mladinske raziskovalne dejavnosti »Mladi za Celje« Mestne občine Celje, zagotavljava, da je v raziskovalni nalogi z naslovom Napad in obramba v kibernetski varnosti, katere avtor je Jan Zorc:

- besedilo v tiskani in elektronski obliki istovetno,
- pri raziskovanju uporabljeno gradivo navedeno v seznamu uporabljene literature,
- da je za objavo fotografij v nalogi pridobljeno avtorjevo dovoljenje in je hranjeno v šolskem arhivu,
- da sme Osrednja knjižnica Celje objaviti raziskovalno nalogo v polnem besedilu na knjižničnih portalih z navedbo, da je raziskovalna naloga nastala v okviru projekta Mladi za Celje,
- da je raziskovalno nalogo dovoljeno uporabiti za izobraževalne in raziskovalne namene s povzemanjem misli, idej, konceptov oziroma besedil iz naloge ob upoštevanju avtorstva in korektnem citiranju,
- da smo seznanjeni z razpisni pogoji projekta Mladi za Celje.

Celje, 9. 4. 2024 žig šole Podpis mentorjev

Podpis odgovorne osebe

* POJASNILO

V skladu z 20. členom Pravilnika raziskovalne dejavnosti »Mladi za Celje« Mestne občine Celje je potrebno podpisano izjavo mentorja (-ice) in odgovorne osebe šole vključiti v izvod za knjižnico, dovoljenje za objavo avtorja (-ice) fotografskega gradiva, katerega ni avtor (-ica) raziskovalne naloge, pa hrani šola v svojem arhivu.

ZAHVALA

Hvaležen sem mentorjema za vso pomoč in usmerjanje v času, ko sem to najbolj potreboval. Prav tako bi se rad zahvalil vsem, ki so mi pri raziskovalni nalogi kakorkoli pomagali, tudi podjetjem in organizacijam v tujini, ki se ukvarjajo s kibernetsko varnostjo in odzivi ob kibernetskih incidentih. Navdihnili so me, da sam poskusim nekaj novega in pokažem svoje sposobnosti in razumevanje tega zelo kompleksnega področja. Posebna zahvala gre mentorju mag. Petru Arliču za strpnost in podporo ter za vodenje skozi temo, s katero sem se letos prvič srečal. Hvala tudi za vse lepe, prijazne in pozitivne komentarje s strani profesorjev in ostalih v šolskem kolektivu. Brez podpore bi ta projekt ostal le misel v moji glavi.

POVZETEK

V sodobnem času se vsakodnevno soočamo z grožnjami na internetu. Zaradi kibernetskih napadov na razna podjetja se moramo vedno znova prilagajati, tako v smislu osebne uporabe naprav, kot so računalniki, mobilni telefoni in podobno, kot tudi v smislu strežnikov v podjetjih in varnosti podatkov v oblaku. Velikokrat podjetja ne pretehtajo pomembnih dejavnikov za zaščito njihovih omrežij in njihovih korporativnih strežnikov in ukrepajo šele, ko je za to prepozno in je škoda že bila narejena. Šele potem kontaktirajo podjetja za odziv v incidentih, preko katerih poskušajo zaščititi svoj ugled in pomembne datoteke, ki bi jih lahko napadalci ukradli z uporabo izsiljevalske programske opreme ali pa preko kakšnih ranljivostih v kiber infrastrukturi določenega podjetja. Kraji podatkov iz omrežij korporacij in organizacij se je možno izogniti na mnogo različnih načinov. Najpomembnejši in tudi prvi korak je imeti varnostne kopije datotek, ki morajo biti shranjene posebej in neodvisno od naprav v omrežju. Najbolje na zunanjih diskih ali pogonih, ki niso povezani z napravami v korporacijah. Velikokrat pa tudi to ni dovolj. Kriminalci pogosto pri izsiljevalski programski opremi ustvarijo še komponento kradljivca podatkov, tako da je vse zaklenjeno, povrhu še ukradeno. Zato je zelo pomembno, da imamo tudi neke vrste zaščito na podlagi ugleda in protivirusni program, da se izognemo kraji ter razkrivanju podatkov na temni strani interneta.

Ključne besede: računalništvo, kibernetska varnost, zlonamerna programska oprema, vdori

ABSTRACT

In modern times, we are faced with daily threats on the internet. Due to cyber attacks on various companies, we constantly need to adapt, both in terms of personal device usage such as computers, mobile phones, and the like, as well as in terms of company servers and data security in the cloud. Often, companies do not consider important factors for protecting their networks and corporate servers until it is too late and damage has already been done. Only then do they contact incident response companies in an attempt to protect their reputation and important files that attackers could steal using ransomware or through vulnerabilities in a company's cyber infrastructure. Data breaches from corporate networks and organizations can be avoided in many different ways. The most important and first step is to have backups of files, which must be stored separately and independently from devices on the network. Ideally, on external drives or disks that are not connected to devices within the corporations. However, often this is not enough. Criminals often create a data theft component in ransomware, so everything is locked and stolen on top of it. Therefore, it is very important to also have some kind of reputation-based protection and antivirus program to avoid theft and disclosure of data on the dark side of the internet.

Keywords: computer science, cyber security, malware, hacking

KAZALO VSEBINE

1 UVOD 1
1.1 NAMEN 1
1.2 PROBLEM 1
1.3 CILJ 1
1.4 HIPOTEZE 2
1.5 METODE RAZISKOVANJA 2
2 TEORETIČNI DEL 3
2.1 OSNOVE O VDORIH 3
2.2 VARNOST V PODJETJIH 3
2.3 ZANESLJIVOST VARNOSTNIH KOPIJ 4
2.4 POVEZAVE MED GOSTITELJEM IN NAPADALCEM 5
2.5 IZSILJEVALSKA PROGRAMSKA OPREMA 7
2.6 RSA KRIPTOGRAFIJA 9
2.7 RANLJIVOSTI OMREŽIJ IN STREŽNIKOV 10
2.8 PODKUPOVANJE DELAVCEV V PODJETJIH 13
2.9 POMEMBNOST ZAŠČITE V REALNEM ČASU 13
2.10 PRIMERJAVA ZANESLJIVOSTI ANTIVIRUSOV 14
3 DEMONSTRACIJA KIBERNETSKEGA NAPADA 17
4 REZULTATI RAZISKAVE 29
5 ZAKLJUČEK 30
6 VIRI IN LITERATURA 31

SEZNAM SLIK

Slika 1: Amadey, ki je povezan preko strežnika Apache in MySQL, da ima popoln dostop do ogroženega sistema 6
Slika 2: Izsiljevalski program, ki prepiše zagonsko particijo diska 8
Slika 3: Izsiljevalski virus »WannaCry« in njegovo sporočilo o odkupnini 9
Slika 4: RSA Kriptografija 10
Slika 5: Ribarjenje z lažnim predstavljanjem podjetja Mimovrste 12
Slika 7: Comodo/Xcitium Client Security 12, osnovni uporabniški vmesnik s komponentami zaščite 14
Slika 8: Kaspersky Endpoint Security osnovni uporabniški vmesnik 15
Slika 9: Zlonamerno e-poštno sporočilo, poslano v e-poštni nabiralnik žrtve 17
Slika 10: Stran za prenos zlonamerne datoteke (MediaFire) 17
Slika 11: Zlonamerna datoteka, zakrinkana kot inštalacijski program za Google Chrome 18
Slika 12: Informacije o datoteki, klonirane iz legitimne inštalacijske datoteke za Google Chrome 18
Slika 13: Uspešna povezava do žrtvinega računalnika preko zlonamerne datoteke na istem omrežju 19
Slika 14: Datoteke za graditelj izsiljevalske programske opreme 19
Slika 15: Grajene datoteke z »Build« skriptom, ki se nahjajajo v mapi »Build« 20
Slika 16: Dešifrirni program, kupljen od kriminalcev 21
Slika 17: Način vstavljanja zlonamerne datoteke v pomnilnik žrtve 22
Slika 18: Zlonamerna datoteka izsiljevalske programske opreme, ki sem jo vstavil v žrtvin pomnilnik 22
Slika 19: Tik pred vstavitvijo izsiljevalskega virusa v naključen proces 23
Slika 20: Datoteka, ki je bila poslana v pomnilnik, uspešno okuži žrtvin računalnik 24
Slika 21: Poln dostop do žrtvine naprave v omrežju 25
Slika 22: Šifrirane datoteke 26
Slika 23: Pošiljanje dešifrirnega programa v sistem po plačilu 26
Slika 24: Dešifrirni program, ki obnovi vse datoteke 27
Slika 25: Konec napada, prekinitev povezave z žrtvijo 28

1 UVOD

V našem vsakdanu se pogosto zgodi, da imamo opravka s kibernetskimi grožnjami, proti katerimi pa je seveda zelo pomembno, da se dodobra zaščitimo. Izguba ali kraja naših osebnih podatkov ali podatkov podjetja je lahko resna nočna mora vsakega podjetnika ali pa tudi večje korporacije, ki je že dolgo na trgu.

1.1 NAMEN

Glavni namen raziskovalne naloge je povečanje zanimanja za možnosti protivirusne zaščite, predvsem pa povečati zavedanje, da je na internetu ogromno groženj, ki vseskozi prežijo na ranljivosti v našem omrežju ali podjetju. Pomembno je razumeti, da ni nobeno podjetje ali organizacija popolnoma varna pred socialnim inženiringom in da je velikokrat glavni razlog pohlep delavcev podjetja za hiter zaslužek, ko so za dostop podkupljeni s strani kriminalcev. To pa tudi povzroči največ gospodarske škode podjetju ali organizaciji, saj ne le da izgubi veliko zaupanja v svoj lasten kader, ampak tudi dostop do lastnih datotek, ki so velikokrat prodane na temni strani interneta.

1.2 PROBLEM

Glavni problem v raziskovalni nalogi je predvsem predstavljen okoli dejstva, da lastniki podjetij največkrat poskušajo zajeziti povzročeno škodo šele po kibernetskem napadu, kar pa velikokrat vrže analiste in najete bele klobuke precej iz tira.

Zato je predstavljena pomembnost varnostnih kopij in dobrih protivirusnih rešitev. Pojasnjeno je, kako velik vpliv lahko imajo celo minimalni varnostni protokoli proti podjetjem, ki nimajo nobenih varnostnih kopij in mislijo, da so dovolj majhni ter tako nekako imuni na vse grožnje z interneta.

1.3 CILJ

Cilj pri ustvarjanju te raziskovalne naloge je, da prepriča čim več ljudi, ki imajo svoja podjetja, da morajo vseskozi izobraževati sebe in svoj kader o varnosti na internetu. Tu ne govorim le o tistih zloglasnih zlonamernih elektronskih sporočilih z neznanimi priponkami in lažnimi PDF-datotekami, temveč tudi o izsiljevalski programski opremi, ki je trenutno najhitreje rastoča kibernetska grožnja na trgu.

1.4 HIPOTEZE

Predpostavljam, da bom z raziskavo potrdil naslednje hipoteze:

Hipoteza 1: Vdor v računalniško omrežje povprečnega, nezavarovanega podjetja je enostaven.

Hipoteza 2: Posamezna programska orodja nudijo različne vrste zaščit.

Hipoteza 3: Kraji podatkov in izsiljevanju se je mogoče izogniti.

1.5 METODE RAZISKOVANJA

Pregled literature

Raziskovalna naloga je nastala na podalagi osebnega pridobljenega znanja na izbrano temo in s pomočjo zanesljivih in kakovostnih virov z interneta. Literature v slovenščini je namreč na to specifično temo izredno malo, je pa kljub temu v raziskovalno nalogo vključenih nekaj pomembnih kontekstualnih izvlečkov tudi iz le-teh virov.

Poglobljeno raziskovanje

Po temeljitem pregledu znanj in literature sem se odločil, da je najbolje začeti z osnovnimi podatki, in sicer s pojasnili, kako sploh delujejo vdori v podjetja in kakšen vpliv imajo na posameznike, ki so bili žrtev tega.

2 TEORETIČNI DEL

2.1 OSNOVE O VDORIH

Zlonamerni vdor v omrežje ali infrastrukturo podjetja je operacija, pri kateri napadalec iz kateregakoli faktorja ranljivosti podjetja ali organizacije pridobi neodobren in nedovoljen dostop do baz podatkov, operacijskih sistemov, strežnikov ali omrežne infrastrukture za namen kraje podatkov, uničenja informacij ali izsiljevanja tarče. Največkrat so ti vdori povezani z uporabo orodij za vdiranje v računalniške sisteme, ki pa so z vsakim dnem učinkovitejša in tudi enostavnejša za uporabo – tako da lahko celo nek začetnik uspešno izvede kibernetski napad na ravni, ki so jo včasih izvajali profesionalci.

Niso pa vsi vdori vedno zlonamerni. Ob tem je pomembno, da razumemo ključno razliko med zlonamernim vdorom in testom penetracije. Slednji je odobren vdor v omrežje ali sistem in ga najpogosteje izvaja najeti analist ali heker. Cilj takega nadziranega testa je preizkusiti kibernetsko varnost in zagotoviti stabilnost kibernetske infrastrukture podjetja, da do zagona zlonamerne kode ali do naključnega napada ne bi prišlo.

Najpogosteje se vdori dogajajo, ko jih kader v podjetju najmanj pričakuje. Posledično se nanje ne morejo pripraviti in zajezitev škode je veliko težja.

Po vdoru lahko zlonamerni uporabnik bolj ali manj počne karkoli želi po okuženem računalniku. Lahko na primer uporabi črva, ki bo raznesel njegov virus po ostalih napravah v omrežju in jih tako povezal v sistem, imenovan »Botnet«. Zatem lahko napadalec upravlja z vsemi napravami v omrežju, do katerih ima dostop, in tako izvaja zlonamerne ukaze. Druga stvar, ki jo lahko naredi po uporabi črva, je, da raznese določen tovor po napravah v omrežju – najpogosteje po računalnikih, ki so med sebo že povezani. Tovor je najpogosteje izsiljevalska programska oprema, katere podrobnejši opis sledi.

2.2 VARNOST V PODJETJIH

Organizacija kibernetske varnosti podjetja je ključna za zaščito pred internetnimi grožnjami. Pogosto pomeni razliko med uničenimi datotekami in posledično velikimi stroški na eni strani ter med tistimi, ki so varnimi in zaščitenimi pred zlonamernimi dejanji.

Presenetljivo dajo podjetja, sploh v Republiki Sloveniji, precej malo na zaščito svoje lastne infrastrukture. Na tej točki je zelo dober primer napad na elektrarne skupine HSE, ki se je zgodil 25. 11. 2023. Kot pričakovano in potrjeno, je bil napad izveden s pomočjo izsiljevalske

programske opreme, ki je zaklenila (in verjetno tudi ukradla) datoteke. Podatek, ki potrjuje napad in krajo, kasneje pa tudi objavo dokumentov na temnem spletu, najdemo tudi na spletni Dnevnika z naslovom: ”Hekerji na spletu objavili del dokumentov iz kibernetskega napada na HSE”. [1]

Ta napad pa po podatkih s spletne strani zaenkrat ni povzročil večje materialne škode, prav tako pa so vodilni pojasnili, da poslovanje in delo poteka nemoteno še naprej.
Kot je že bilo omenjeno, je izrednega pomena, da se kader v podjetjih in organizacijah nenehno izobražuje o varnosti na internetu ter da imajo pogosto najavljene strokovnjake, ki lahko zagotovijo, da do napadov ne bo prišlo.
Slovenija beleži zelo majhno in skromno količino strokovnjakov na tem področju. Glede na to da nekega programa za izobraževanje (izrecno samo kiber forenzike in kibernetske varnosti) na naših tleh še ni, se je potrebno velikokrat posvetovati s profesionalci iz antivirusnih podjetij in organizacij za zaščito na internetu v tujini. Upam, da se bo to nekoč v prihodnosti spremenilo in da bo študij in srednješolski program obstajal tudi v tej izjemno specifični strokovni smeri.
Obstaja pa še eno pomembno načelo, na katerega ne smemo pozabiti, in sicer klasično pogojevanje. Pri tem je lahko na primer neka starejša oseba, ki je v podjetju zaposlena že dlje časa. Le-ta je navajena zaganjati razne datoteke, ki jih ne bi smela, in nalagati gonilnike preko CD diskov in podobno. Ti pogosto smatrajo, da so razne datoteke in URL-ji zaradi njihovih prejšnjih pozitivnih izkušenj v računalništvu preprosto varni. To je kot preprost instinktivni odziv, kar lahko podjetje močno ogrozi.

2.3 ZANESLJIVOST VARNOSTNIH KOPIJ

Ustvarjanje varnostnih kopij je za mnoga multinacionalna podjetja postal rutinski in izredno pomemben opravek, brez katerega so njihove datoteke nenehno v nevarnosti pred zlonamernimi aktivnostmi. Vsak profesionalec na tem področju bo govoril o pomembnosti hrambe varnostnih kopij ranljivih podatkov na zunanjih strežnikih in pogonih, ki niso povezani v glavna omrežja organizacije. Ti podatki so imena in priimki strank, njihovi rojstni podatki, podatki kadrovske zasedbe, podrobnosti o plačilnih informacijah strank, natančni opisi strank, algoritmi za raziskovanje interesov strank, baze podatkov o podjetju, informacije o prodaji izdelkov, računi in finance podjetja, občutljive recepture izdelkov podjetij in še mnogo več informacij, za katere resnično ne želimo, da bi jih odkrila konkurenca ali pa preprosto ena sama napačna oseba. Razumeti moramo tudi, da je kraja podatkov kadra in prodajanje le-teh brez zavedanja ali znanja podjetja hudo kršenje zasebnosti in kaznivo dejanje. Če je bila kateremu koli od delavcev

v kadru podjetja povzročena materialna ali kakršna koli škoda, zloraba osebnih podatkov in pa še kaj hujšega zaradi kraje, je to lahko podlaga za civilno tožbo zaradi vdora v zasebnost delavca kot zaščitenega posameznika, kar je pogosto tudi zagotovljeno v pogodbi. [5]

Kljub temu je pomembno izpostaviti, da čeprav imamo varnostne kopije, je napredno in novodobno izsiljevalsko programje oblikovano tako, da najprej krade vse informacije s pomočjo komponente za krajo podatkov, nato zaklene datoteke in šele zatem poišče preostale naprave, povezane v omrežje s pomočjo komponente črva. V takem primeru so obstoječe varnostne kopije sicer uporabne, a imajo kriminalci še vedno dostop do zgoraj opisanih informacij in jih, če seveda ne plačamo odkupnine, lahko še vedno prodajo konkurenci, kar bi imelo katastrofalne posledice za ugled in celo obstoj podjetja ali organizacije.

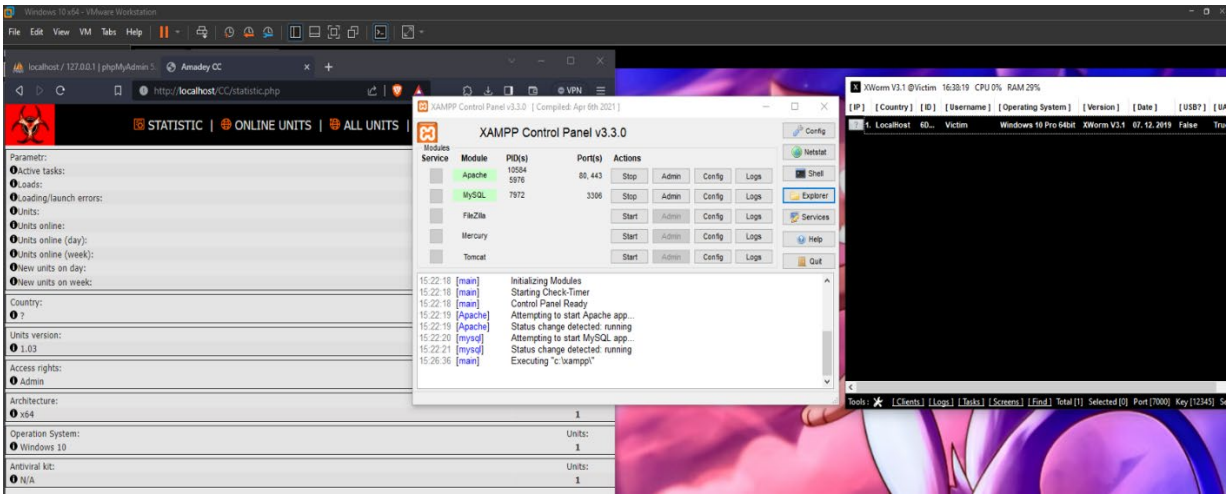
Zaradi konstantnega napredka v razvoju izsiljevalske programske opreme in tudi ostale zlonamerne programske opreme za namen kraje podatkov se na varnostne kopije preprosto več ne moramo popolnoma zanašati.

2.4 POVEZAVE MED GOSTITELJEM IN NAPADALCEM

Ob uspešnem kibernetskem napadu se vzpostavi posebna povezava med napadalcem in ranljivim sistemom. Povezava med dvema napravama je lahko preko SSH (Secure Shell Protocol), ki je kriptografski omrežni protokol, preko katerega prosto potujejo podatki in je izveden na nezaščitenem omrežju. Predhodnik SSH je bil izjemno znan in široko uporabljen omrežni protokol TELNET, ki pa je 7 (8)-bitni in na tej točki že precej star.

Telnet (Teletype Network) je povezava po načelu odjemalec/strežnik, ki pa nam omogoča preko našega lokalnega omrežja in domačih omrežnih vrat povezavo na oddaljen strežnik preko virtualnega terminala. Ta omrežna povezava se danes sicer še vedno uporablja za kibernetske napade, saj je dejansko možno ustvariti »Botnet« preko »telneta«. Žalostna novica za ta precej star protokol pa je, da se za ustvarjanje botnetov vedno pogosteje uporablja programski jezik PHP, ki je povezan s SSH in so podatki uvoženi v SQL baze podatkov (primer Amadey).

Za ustvarjanje same zlonamerne datoteke pa še vedno potrebujemo graditelja, ki pa je po navadi ločen od same PHP panele.



Slika 1: Amadey, ki je povezan preko strežnika Apache in MySQL, da ima popoln dostop do ogroženega sistema (Vir: Osebni arhiv)

Amadey je le eden izmed mnogih orodij za ustvarjanje tako imenovanih botnetov in ga dejansko ni tako zahtevno uporabljati. Potrebujemo pa nekaj predhodnega znanja na področju PHP in MySQL.

Omrežna vrata

Omrežna vrata ali po angleško »Network Ports« so vhodi in izhodi vmesnika omrežne infrastrukture naprav, ki skrbijo za pretok informacij med strežnikom in odjemalcem, med programi in strežniki ali pa tudi med različnimi napravami v omrežju.

Vrata ima vsak računalnik in naprava, sposobna komunikacije preko TCP in UDP. Število vrat je omejeno od 0 do 65535. Pri operacijskem sistemu Windows je velika možnost, da so vrata od 0 do 1024 že zasedena s strani sistemskih povezav, medtem ko pa so v programskem okolju Linux oziroma GNU vrata od 0 do 1024 dosledno rezervirana za obstoječe sistemske povezave in strežnike, kot so TELNET, HTTP, POP3, SMTP, FTP in še več. Ta vrata lahko na Linux programski opremi ureja in ponastavlja samo superuporabnik (ROOT), ki pa deluje precej podobno kot administrator v okolju Windows, le da na spremembe na sistemskem nivoju Windows administrator ne more vplivati. Prav tako ne more dostopati do datotek na sistemskem nivoju, saj spremembe sproti blokira uporabnik »TrustedInstaller«, ki pa deluje kot nek zaščitni mehanizem sistema pred nezaželenimi spremembami.

Pogosto že samo spreminjanje nastavitev vrat in požarnega zidu zahteva skrbniške pravice in običajni uporabniki v podjetju teh nastavitev ne morejo spreminjati. Tehniki in najeti strokovnjaki upravljajo z nastavitvami požarnega zidu in blokirajo vse nezaželene in škodljive povezave.

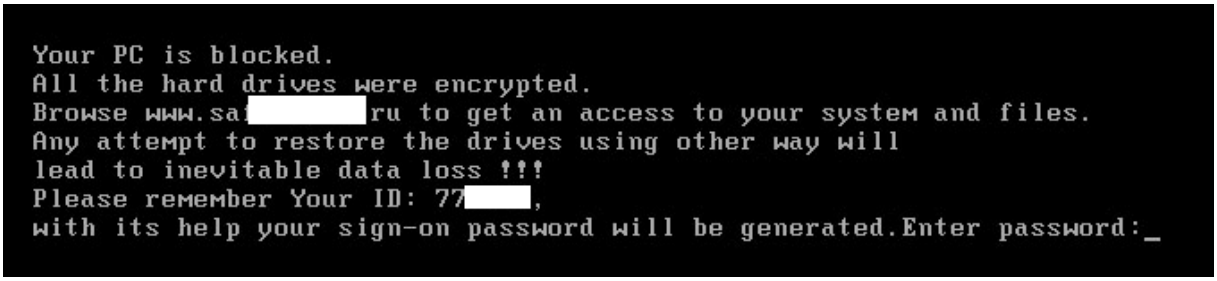
Preko omrežnih vrat lahko napadalec uspešno izvede eksfiltracijo podatkov in jih shrani na njegovo lokalno napravo ali pa na njegov strežnik.

2.5 IZSILJEVALSKA PROGRAMSKA OPREMA

Izsiljevalska programska oprema ali po angleško »Ransomware« je trenutno daleč največja in najbolj sofisticirana kibernetska grožnja na svetu. Deluje lahko na mnogo različnih načinov. Poznamo klasične, ki samo zaklenejo in kradejo datoteke, napravi pa pustijo polno funkcionalnost. Obstajajo pa tudi različice izsiljevalske programske opreme, ki blokirajo zaslon in miško, tako da lahko vidimo le sporočilo o odkupnini. Obstaja pa sicer še različica, ki prepiše informacije na tabeli prvega sektorja glavnega pogonskega zapisa na disku (MBR), kar popolnoma prepreči cel zagon operacijskega sistema. Namesto sistema se nam zato pokaže sporočilo o odkupnini in nič, razen popolno formatiranje diska, ne bo odstranilo te grožnje. S tem pa posledično odstrani tudi vse datoteke, pri čemer smo spet odvisni od varnostnih kopij.
Začetki te grožnje segajo v leto 1989, ko je bil ustvarjen in razširjen prvi izsiljevalski virus z imenom AIDS. Ta je bil izjemno enostaven v primerjavi z novejšimi tovrstnimi grožnjami. Zahteval je 189 ameriških dolarjev v zameno za dešifriranje datotek.
Od takrat naprej so kriminalci začeli ustvarjati boljše in naprednejše različice teh virusov. Že v letu 2010 se je začela nova doba izsiljevalskega programja, ki je prvič pokazala sposobnost prepisovanja zagonskih sektorjev diska s sporočili o odkupnini, ki so bila ustvarjena po meri. Ti so bili najprej najdeni, da izhajajo iz držav nekdanje Sovjetske zveze.
V letu 2013 je bila glavna zvezda šova izsiljevalske programske opreme, tako imenovani »Cryptolocker«, ki je bil prva večja in bolj problematična kibernetska grožnja po stari zlonamerni programski opremi med leti 1990 in 2006. Povzročil je precej veliko škode celo na gospodarskem nivoju, a ni bil niti blizu temu, kar se je zgodilo čez slaba štiri leta.
Leta 2017 se je zgodil največji kibernetski napad z uporabo izsiljevalske programske opreme v zgodovini. V napadu pa je bil uporabljen eden danes najbolj znanih izsiljevalskih virusov, ki se imenuje »WannaCry«.
Virus »WannaCry« je vseboval glavno komponento izsiljevalskega virusa. Prav tako pa je vseboval komponento črva, ki se je imenoval »DoublePulsar« Le-ta je bil ukraden od ameriške Agencije za nacionalno varnost (NSA) iz strani korejske skupine hekerjev. Kasneje je bil črv prodan na temnem spletu in uporabljen še v nekaj precej znanih izsiljevalskih programih, kot so »Petya«, » Mischa«, » Goldeneye« in kasneje še »NotPetya«, ki je bila imenovana tako, ker

je imela vse značilnosti virusa »Petya«, ampak povezave med tema dvema grožnjama ni bilo možno najti, so pa vizualno izgledali skoraj popolnoma enaki.

Po teh napadih so bila podjetja precej prestrašena, saj niso želela, da bi se tudi pri njih pojavil kakšen podoben scenarij. S tem se je povečalo tudi globalno povpraševanje po orodjih za dešifriranje in pomoč za odziv v incidentih.



Slika 2: Izsiljevalski program, ki prepiše zagonsko particijo diska

(Vir: https://securelist.com)

V današnjem času je za učinkovito zaščito pred izsiljevalskimi programi potrebno imeti:

- popolno varnostno kopijo vsakega sistema v podjetju, ki je tudi na oblaku;
- učinkovito ekipo za odziv ob napadih;
- dobro in sprotno izobražen ter za delo popolno sposoben kader;
- dobro rešitev proti virusom in izsiljevalski programski opremi;
- zaupanja vredne zunanje povezave, ki lahko pomagajo obnoviti datoteke.

Slika 3: Izsiljevalski virus »WannaCry« in njegovo sporočilo o odkupnini

(Vir: https://en.wikipedia.org)

2.6 RSA KRIPTOGRAFIJA

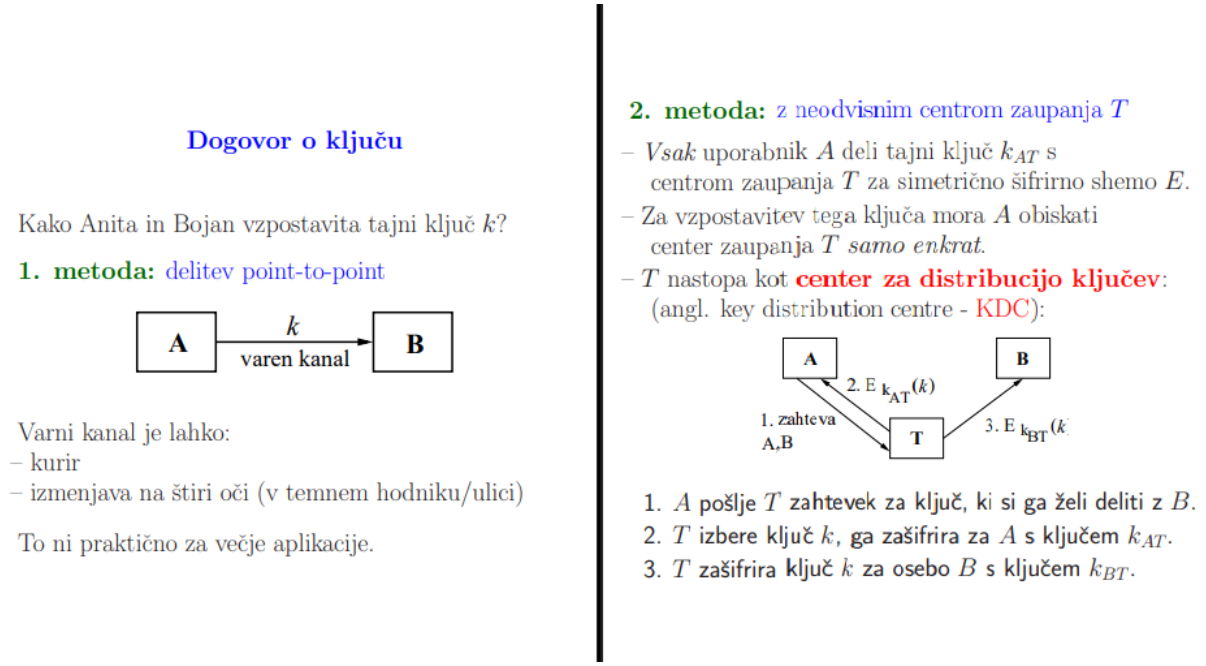
RSA je algoritem za šifriranje podatkov s pomočjo javnega in zasebnega ključa.

Največkrat se uporablja pri izsiljevalski programski opremi za šifriranje zasebnih datotek in uničevanje informacij, čeprav je bila sprva namenjena zaščiti informacij na raznih trdih diskih. Ta vrsta kriptografije je znana kot ena najbolj robustnih in varnih, tako da je dešifriranje brez zasebnega ključa lahko precej zahtevno.

Kot omenjeno, vsebuje dva ključa, zasebnega in javnega. Javni ključ lahko vidi kdorkoli in je vedno podan, saj je ta uporabljen za šifriranje. Zasebni ključ pa odklepa vse, kar je javni zaklenil, in samo lastnik zasebnega lahko vidi informacije, ki so zaklenjene s specifičnim javnim ključem.

Najboljši primer je izsiljevalska programska oprema, ki z javnim ključem, ki je sproti generiran za vsako individualno tarčo, napade in zaklene datoteke na računalnikih nekega podjetja. Na tej točki lahko datoteke dobimo nazaj samo, če kupimo dostop do zasebnega ključa, ki ga ima v lasti napadalec in ga moramo kupiti kot odkupnino. [6]

Proces sestavlja mnogo matematičnih operacij, a je najbolje prikazan in ponazorjen z dejansko demonstracijo kibernetskega napada z izsiljevalsko programsko opremo.



Slika 4: RSA Kriptografija

(Vir: http://lkrv.fri.uni-lj.si)

2.7 RANLJIVOSTI OMREŽIJ IN STREŽNIKOV

Omrežja in strežniki pogosto potrebujejo ogromno zaščite in vzdrževanja, da lahko uspešno in varno shranjujejo podatke. Kljub temu pogosto pride do nezaželenih aktivnosti in vdorov, ki pa so v večini primerov popolnoma preprečljivi.

Zastarela programska in strojna oprema

Pogosto je razlog za kibernetski napad programska oprema za omrežje, kot je na primer zastarela in neposodobljena programska oprema za brezžični usmerjevalnik ter slaba gesla za dostop. Prav tako je velik dejavnik in razlog za napad slaba zaščita omrežja.

Zlonamerni izmenljivi diski

Če se naprave, kot so USB-ji, CD-ji ali pa ostale pomnilniške kartice, priključujejo v računalnike in ostale naprave konstantno za prenos in shranjevanje informacij, je pomembno, da so skenirane in preverjene iz strani zadolženih za kibernetsko varnost v podjetju. V nasprotnem primeru lahko tvegamo napad ali pa eskfiltracijo podatkov preko omrežja.

Šibka gesla za dostop v omrežje

Če so gesla za dostop v omrežje res slaba, jih lahko napadalci uganejo s pomočjo programov, ki pošljejo na tisoče gesel na strežnik, v upanju, da bi eno delovalo (t. i. »Brute force« napadi). Najboljša rešitev je preveriti moč gesla in predstaviti dolgoročno rešitev za zaščito gesel, kot je na primer upravljalnik gesel, ki jih shrani in zašifrira, tako da nima nobena nepooblaščena oseba dostopa.

Problemi z overitvijo

Overitev za občutljive podatke bi morala v vsakem podjetju potekati v dveh ali več korakih.
Najbolj varen način overjanja je varnostni ključ, ki pa v Republiki Sloveniji še ni tako zelo razširjen. Varnostni ključ je zelo uporaben in učinkovit, saj ima dostop do podatkov, ki so šifrirani, z njim pa opravlja ena ali več oseb, ki ima ta isti ključ.

Slaba konfiguracija požarnega zidu

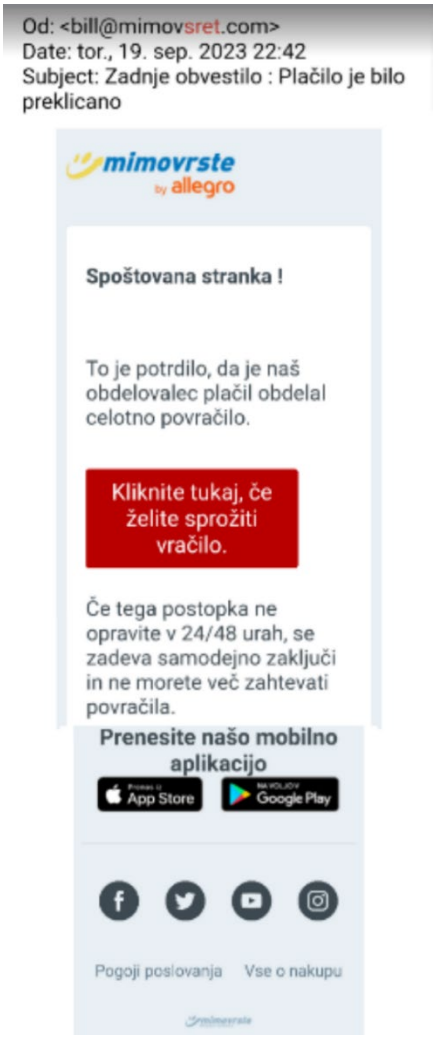
Po znanih podatkih je slaba konfiguracija požarnih zidov razlog za več kot 9 % vdorov v omrežja.
Pomembno je, da je konfiguriran pravilno in da blokira vse nezaželene povezave, za katere nadrejeni ali kader ne more potrditi, da so popolnoma varne.
Že en sam napačen parameter v nastavitvah omrežnih vrat požarnega zidu je lahko precej nevaren in prisotna je ranljivost, ki kar čaka, da jo nekdo izkoristi za neodobren dostop.

Napad z lažnim predstavljanjem (»Phishing«)

Lažno predstavljanje ali ribarjenje, tudi imenovano zvabljanje, je način socialnega inžineringa, pri katerem je glavna šibka točka nevednost delavca v podjetju. [7]
Najpogosteje je prikazano in izvedeno preko elektronske pošte ali pa redkeje preko sporočil na mobilnem telefonu.
Velikokrat kriminalci in tatovi izvajajo te napade tako, da se izdajajo za neko podjetje (najpogosteje Pošta Slovenije, DPD, Aliexpress ipd.) in nas namesto na uradno stran teh podjetij hiperpovezava preusmeri na stran, ki je v lasti kibernetskih tatov. Ti poskrbijo, da izgleda stran za prijavo popolnoma takšna, kot je legitimna. Povprečen človek tako ne opazi razlike in izpolni vsa polja ter jih na koncu tudi potrdil. S tem pride do kraje informacij.
Pomembno je, da ob odprtju take strani preverimo, kakšno hiperpovezavo ima dejanska uradna spletna stran storitve.

Če se strani popolnoma razlikujejo po hiperpovezavi, potem je stran lažna in poskuša zlonamerno krasti osebne podatke ali podatke podjetja.

V podjetjih je prek elektronske pošte pomembno preveriti, ali je elektronski naslov legitimen in ni samo neka različica naslova legitimnega podjetja. Na sliki 5 je na primer »mimovsret«, namesto »mimovrste«.



Slika 5: Ribarjenje z lažnim predstavljanjem podjetja Mimovrste

(Vir: https://sl.wikipedia.org)

Obstaja še mnogo raznovrstnih načinov, kako je možno vdreti v omrežja podjetij.

2.8 PODKUPOVANJE DELAVCEV V PODJETJIH

Do podkupovanja delavcev pride takrat, ko želijo ustvarjalci zlonamerne programske opreme hiter in zanesljiv dostop do celotne omrežne infrastrukture napadenega podjetja in tako razširiti zlonamerno programsko opremo po ostalih napravah, pa čeprav nimajo popolnoma nič s tem.
Najpogosteje izbirajo kriminalci šibkejše člene v kadru, da bi čim hitreje in varneje prišli do informacij.
Vsi se moramo zavedati, da ima v poslu vse svojo ceno in da je izjemno zahtevno pridobiti delavce, ki se ne bodo prodali najboljši ponudbi iz strani kibernetske mafije. Je pa res, da dejavniki, kot so na primer nizke plače, slabi delovni pogoji, nezadostni dodatki in še več, močno vplivajo na to, kako bo določen uslužbenec na tako ponudbo reagiral.
Do podkupovanja lahko pride tudi s spletnimi prevarami ali manipulacijo, saj kot je že bilo omenjeno, ima vsako podjetje nekje šibko točko. [2]

2.9 POMEMBNOST ZAŠČITE V REALNEM ČASU

Zaščita v realnem času je znan mehanizem, ki je implementiran v antivirusne programe in omogoča zaznavanje groženj pred ali med okužbo.
Je verjetno najpomembnejši sestavni del mehanizma protivirusnih programov in zato tudi čista osnova.
V občutljivih okoljih je pomembno, da posodabljamo, preverjamo in konstantno popravljamo konfiguracijo naših protivirusnih programov. Tako poskrbimo, da so naši sistemi in korporativna omrežja varna pred najnovejšimi grožnjami in pa tudi ranljivostmi, ki bi lahko ogrozila našo ali integriteto podjetja.
Obstaja mnogo načinov, kako nas protivirusni programi zaščitijo v resničnem času. Od zaščite na osnovi ugleda do tehnologije HIPS (Host Intrusion Prevention System), ki deluje po točno določenih pravilih, da blokira vse zlonamerne dejavnosti, ki jih kateri koli program izvaja.
To vključuje skripte (VBS, JS, PowerShell (ps1, ps, cmd, ipd.), BAT in še več). Programe, funkcije, DLL (Dynamic Link Library) datoteke, datoteke ohranjevalnikov zaslona (SCR) in še mnogo ostalih datotek, ki nam lahko na kakršen koli način ob zagonu povzročijo škodo.

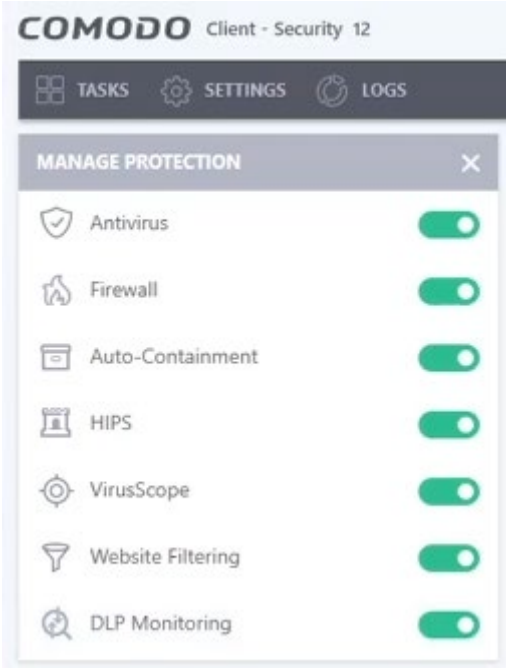
2.10 PRIMERJAVA ZANESLJIVOSTI ANTIVIRUSOV

Pri primerjavi protivirusne opreme je potrebno biti pozoren na več raznovrstnih dejavnikov. Eden izmed njih je izbor komponent, ki so na voljo v specifičnih programih, drugi pa, kako ga je možno zliti v nam najbolj ustreznega.

Izjemno pogosto ali pa celo vedno se bodo vsa podjetja osredotočila na oglaševanje komponent, ki jih njihova protivirusna oprema ponuja, na druge pa ne, kar bi pomagalo pri prodaji in zanimanju iz strani podjetij ali pa fizičnih oseb, ki želijo okrepiti svojo kibernetsko varnost ter integriteto naprav in celotnega podjetja.

V nadaljevanju je predstavljenih nekaj podjetij, ki ponujajo protivirusno zaščito za podjetja.

Xcitium (prej Comodo) Client Security suite



Slika 6: Comodo/Xcitium Client Security 12, osnovni uporabniški vmesnik s komponentami zaščite (Vir: Osebni arhiv)

Xcitium ponuja mnogo zanimivih funkcij. Najbolj zanimiva pa je zagotovo tako imenovana »Auto-Containment«, pri kateri protivirusni program popolnoma izolira program od sistema z ustvarjanjem popolne kopije map na našem sistemskem disku ter nato zažene virus v tistem okolju, kjer ima protivirusni program tudi čas, da reagira na vsa dejanja in ustrezno ukrepa. S tem imitira nekakšen peskovnik, kjer zlonamerne datoteke nimajo dostopa do naših sistemskih datotek in ostalih potencialno občutljivih informacij.

Ta program je izjemno priljubljen v visoko ogroženih okoljih in tistih, ki morajo imeti vseskozi zelo dobro urejene varnostne protokole na tem področju. [8]

Kaspersky Endpoint Security

Slika 7: Kaspersky Endpoint Security osnovni uporabniški vmesnik
(Vir: Osebni arhiv)

Kaspersky je znan po ogromnem naboru različnih orodij, ki so zelo uporabna, prav tako pa tudi zanimiva za analizo.

Osnovne komponente zaščite za podjetja so deljene na tri dele: osnovna zaščita, kontrolorji za varnost in napredna zaščita. Vse imajo določen pomen in pripomorejo k boljši zaščiti sistemov. Protivirusna zaščita tega izdelka je zelo znana po izredno dobri integraciji različnih komponent zaščite do točke, da lahko vsaka deluje popolnoma spontano in ima svoja pravila, kar je bilo dokazano že v mnogih videoposnetkih in reportažah po internetu.

To prav tako pomeni, da teoretično ne potrebujemo modula »File Threat Protection«, saj tudi če bi ne bil aktiven, bi grožnjo blokirala katerakoli druga komponenta, na primer »Application Control« ali pa »System Watcher«.

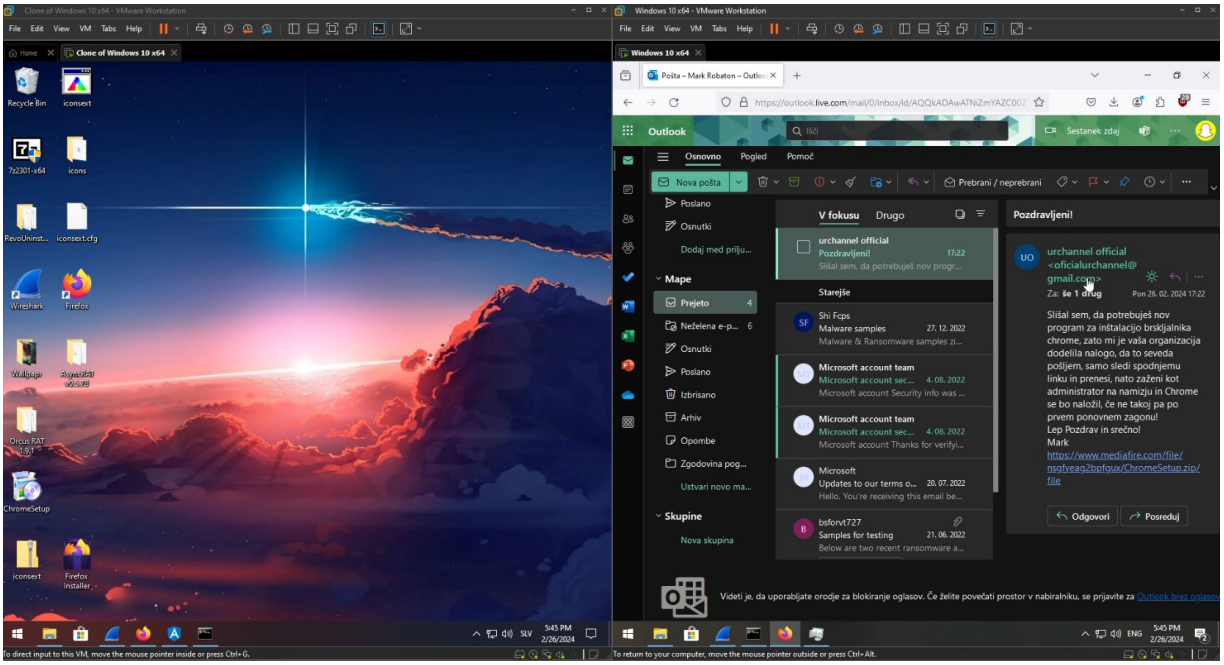
Seveda so tu v igri tudi »Behavior Detection«, »Host Intrusion Prevention – HIPS«, »Device Control« in »Remediation Engine«.

Preprosto preveč komponent je, ki delujejo skupaj, da bi kakršna koli zlonamerna programska oprema prišla enostavno skozi.

Seveda pa tudi ta, kot mnogi drugi protivirusni programi, ni popoln in je bil pod močnimi kritikami, saj je zaradi ruske vpletenosti v vojno v Ukrajini podjetje padlo pod precej slabo luč. Ljudi je skrbelo, da podjetje zbira podatke iz zahodnih držav, kot so Združene države Amerike, Velike Britanije idr. Ti podatki naj bi bili celo tajne in državne skrivnosti. Pomembno je

razumeti, da je velika verjetnost, da temu ni tako, čeprav velikokrat slišimo, da protivirusna podjetja zbirajo sumljive informacije o uporabnikih in jih shranjujejo na strežnike ali pa prodajajo naprej za namen oglaševanja. [4]

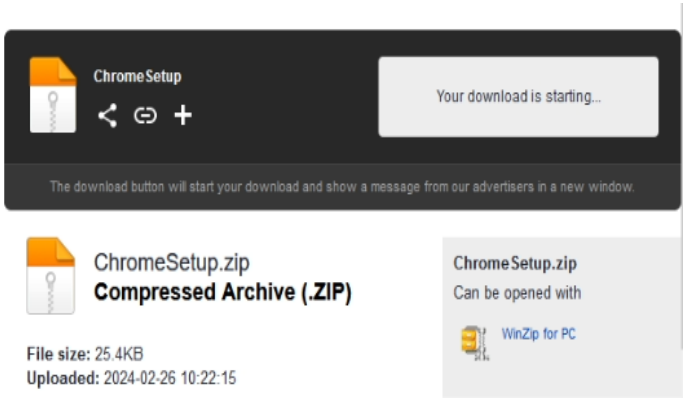
3 DEMONSTRACIJA KIBERNETSKEGA NAPADA



Slika 8: Zlonamerno e-poštno sporočilo, poslano v e-poštni nabiralnik žrtve

(Vir: Osebni arhiv)

Zamislil sem si dva virtualna računalniška sistema v okolju Vmware. Levi je bil napadalec, desni pa tarča v nekem podjetju. Pripravil sem elektronsko sporočilo, s katerim bi žrtev prepričal, da datoteka ni zlonamerna in je bila poslana zaradi na videz legitimne prošnje iz vrha podjetja. Priložen je bil tudi URL, ki je predstavljal brskljanik Google Chrome.



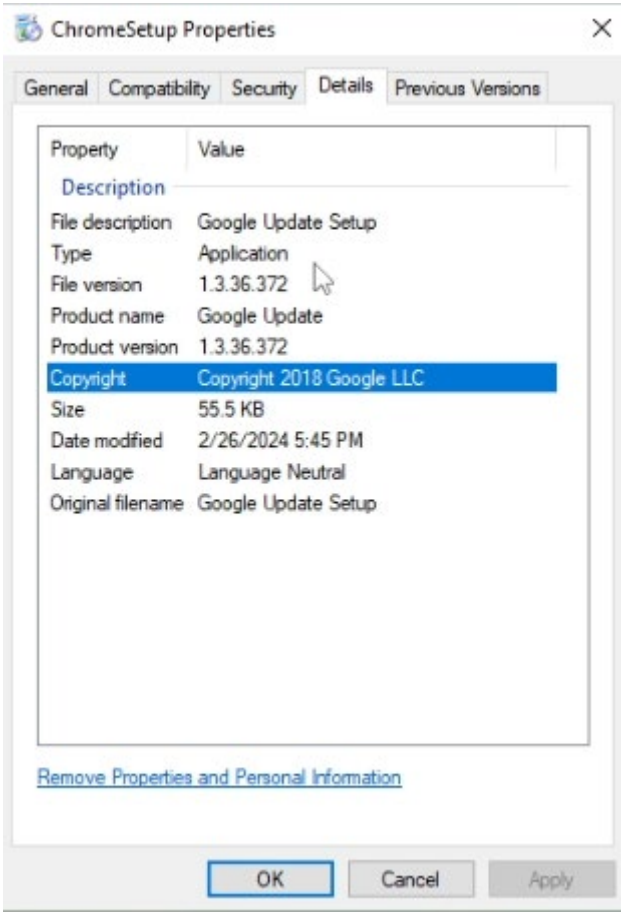
Slika 9: Stran za prenos zlonamerne datoteke (MediaFire)

(Vir: Osebni arhiv)

Ko je žrtev uspešno sledila URL-ju, je prišla na spletno stran MediaFire, ki je namenjena deljenju datotek in programov. Zatem je žrtev preprosto pritisnila gumb za prenos in s tem je bil trojanec za oddaljen dostop uspešno prenesen.

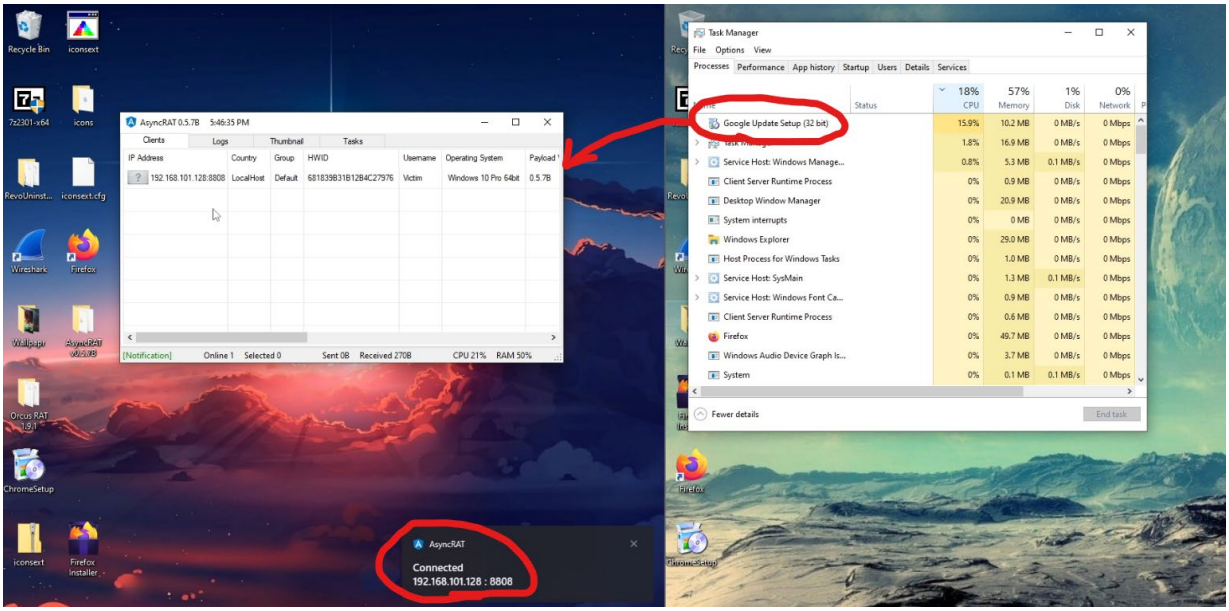
Slika 10: Zlonamerna datoteka, zakrinkana kot inštalacijski program za Google Chrome
(Vir: Osebni arhiv)

Prenešena datoteka je izgledala popolnoma enako kot dejanski inštalacijski program za brskljalnik Google Chrome. S tem žrtev ne bi mogla posumiti, da nekaj ni prav. Edina razlika je zagotovo velikost, saj ima legitimni inštalacijski program nekaj več kot 1 MB podatkov.



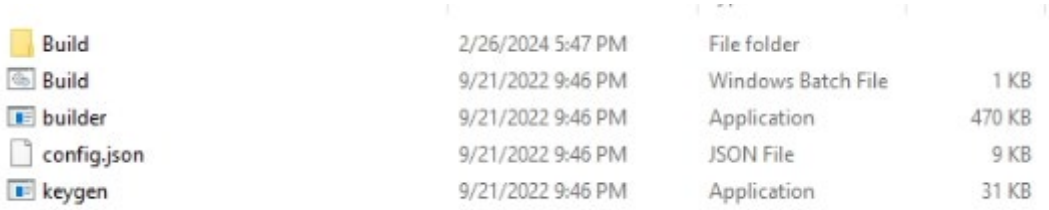
Slika 11: Informacije o datoteki, klonirane iz legitimne inštalacijske datoteke za Google Chrome
(Vir: Osebni arhiv)

Na sliki 11 so informacije o datoteki trojanca za oddaljeni dostop, ki ga je žrtev prenesla s strani MediaFire. Edina razlika je, kot že omenjeno, velikost, kar pa veliko ljudi sploh ne zanima oziroma na to niso preveč pozorni. Najbolj razvidna razlika na tej točki je, da ima legitimni inštalacijski program Googlov digitalni podpis, ki pa ga ta datoteka nima (seveda pa bi se ga dalo pridobit tudi na nelegalen način).



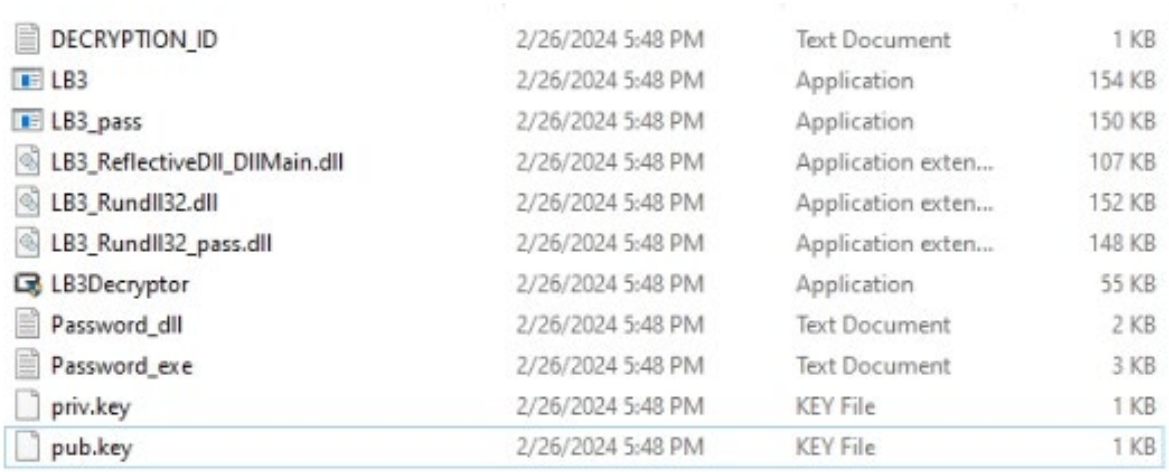
Slika 12: Uspešna povezava do žrtvinega računalnika preko zlonamerne datoteke na istem omrežju
(Vir: Osebni arhiv)

Po uspešnem zagonu trojanca je vidno, da se je iz napadalčevega sistema vzpostavila povezava preko omrežja v računalnik žrtve. Tako ima napadalec zdaj popoln dostop do žrtvine naprave.



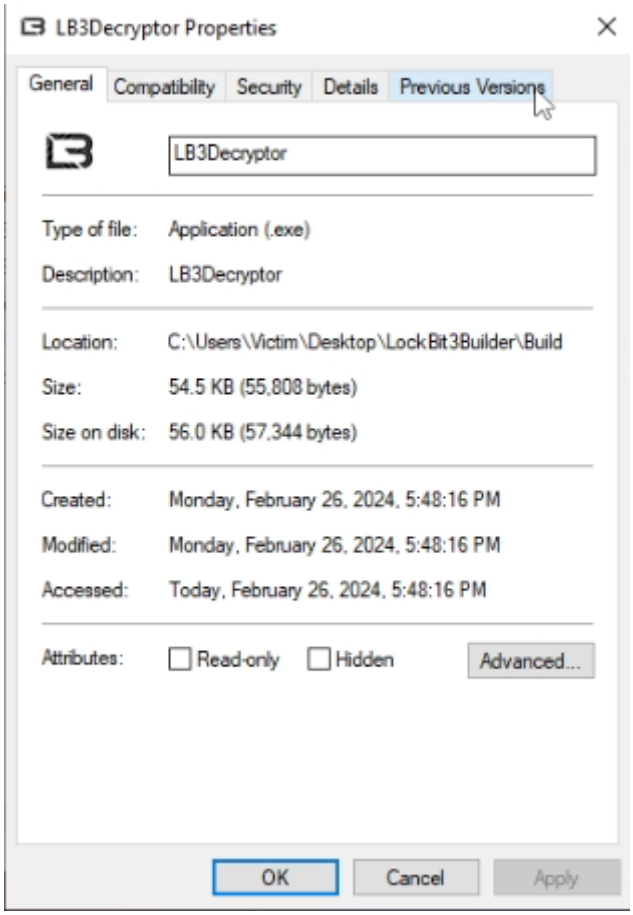
Slika 13: Datoteke za graditelj izsiljevalske programske opreme
(Vir: Osebni arhiv)

Po prvem koraku pridobivanja nedovoljenega dostopa imamo vse možnosti, da ta sistem okužimo še s čim drugim. Na primer z izsiljevalsko programsko opremo, ki sem jo s pomočjo programa, ki je uporabljen za grajenje teh zlonamernih programov, tudi ustvaril specifično za ta napad.



Slika 14: Grajene datoteke z »Build« skriptom, ki se nahjajajo v mapi »Build«
(Vir: Osebni arhiv)

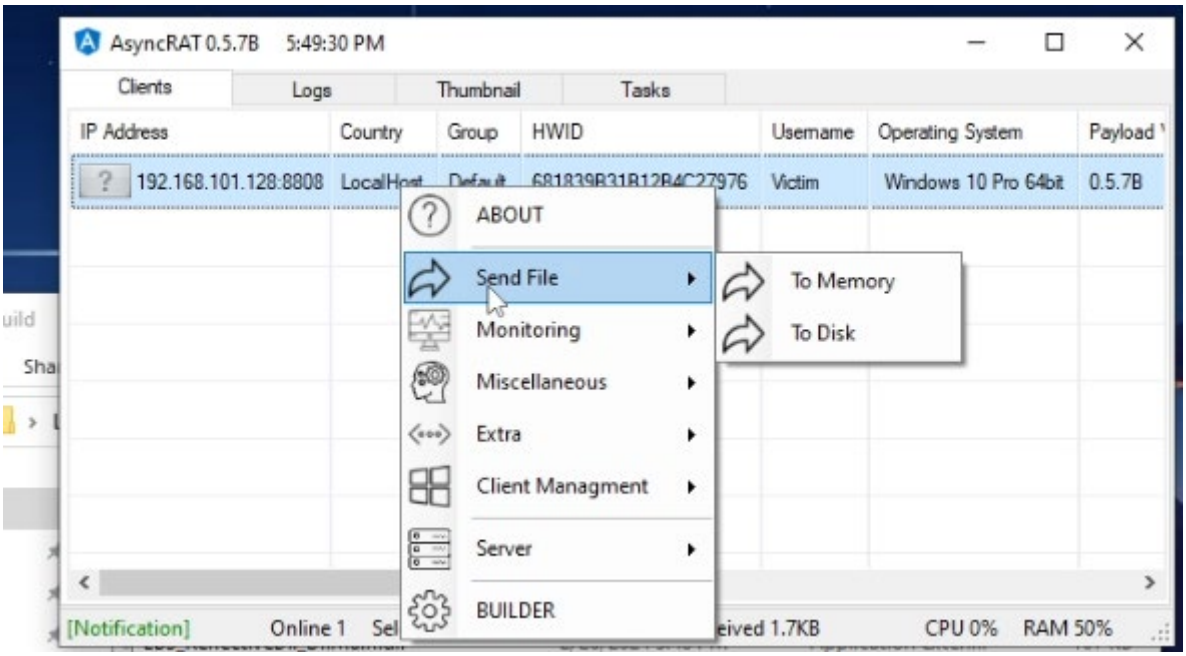
Po zagonu skripta lahko vidimo, da so v mapi »Build« nastale nove datoteke, ki so potrebne za uspešen napad. Prva datoteka je ID napada, druga je dejanski izsiljevalski virus, tretja je virus z geslom, četrta, peta in šesta so gonilniki, ki so potrebni za delovanje samega zlonamernega programa, sedmi je program za dešifriranje, osma in deveta sta za pomoč, deseta in enajsta pa zasebni in javni ključ RSA kriptografije.



Slika 15: Dešifrirni program, kupljen pri kriminalcih

(Vir: Osebni arhiv)

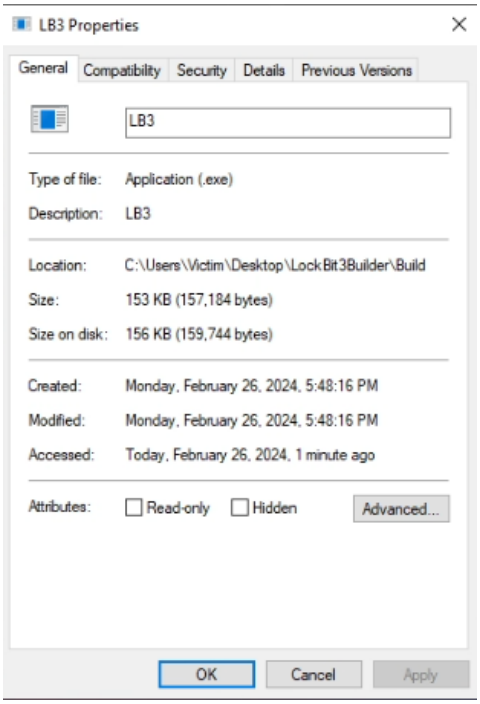
Na sliki 15 so osnovni podatki o dešifrirnem programu. Datoteka je precej majhna, ampak pošlje zasebni ključ na sistem, ki nato povzroči, da se datoteke dešifrirajo in so nazaj, kot so bile pred napadom.



Slika 16: Način vstavljanja zlonamerne datoteke v pomnilnik žrtve

(Vir: Osebni arhiv)

Na sliki 16 je vidna sposobnost trojanca za oddaljeni dostop, da pošljem virus v votli proces.



Slika 17: Zlonamerna datoteka izsiljevalske programske opreme, ki sem jo vstavil v žrtvin pomnilnik

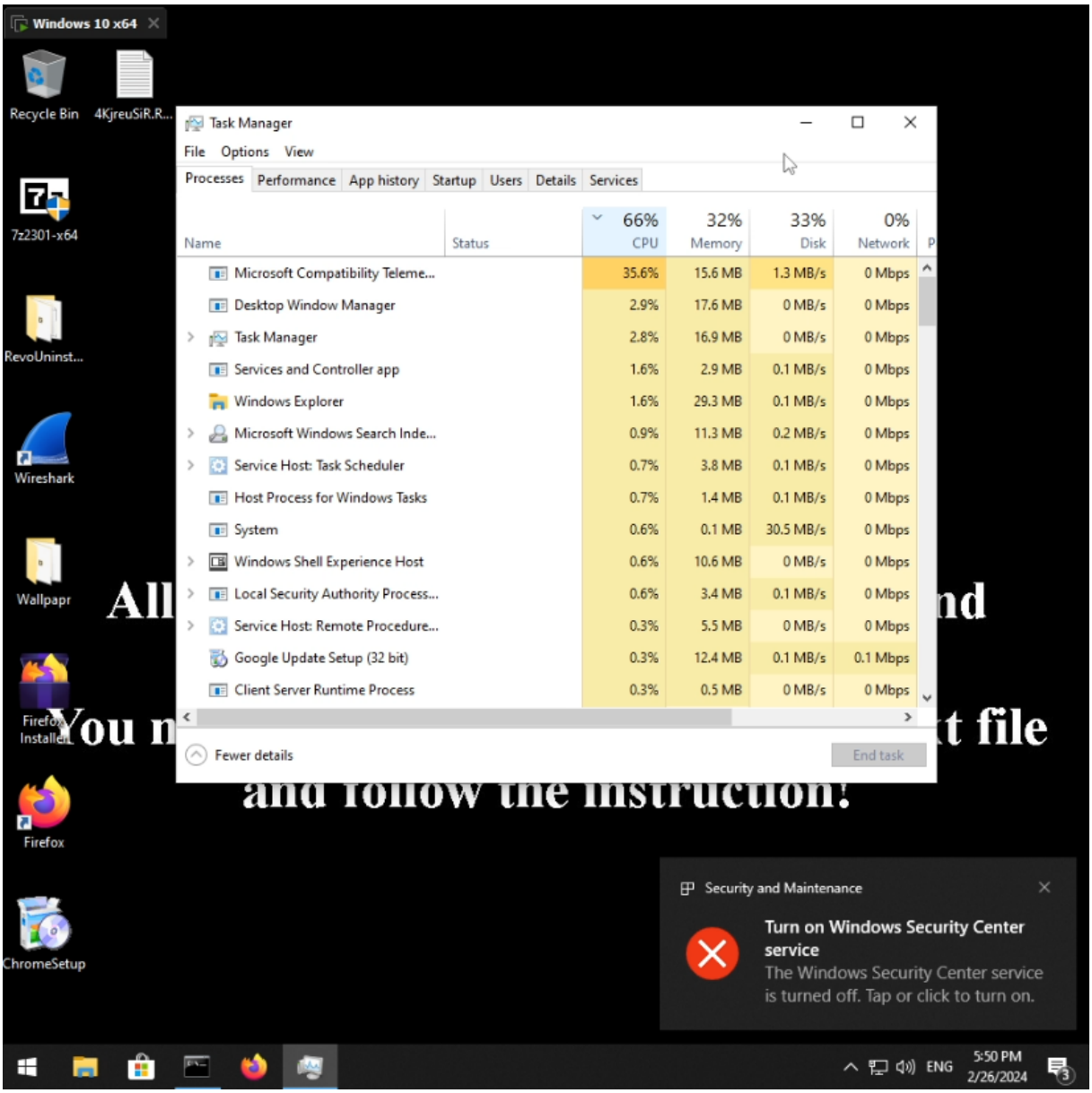
(Vir: Osebni arhiv)

Na sliki 18 je približen izgled uporabljenega izsiljevalskega virusa in njegovi osnovni podatki.

Slika 18: Tik pred vstavitvijo izsiljevalskega virusa v naključen proces
(Vir: Osebni arhiv)

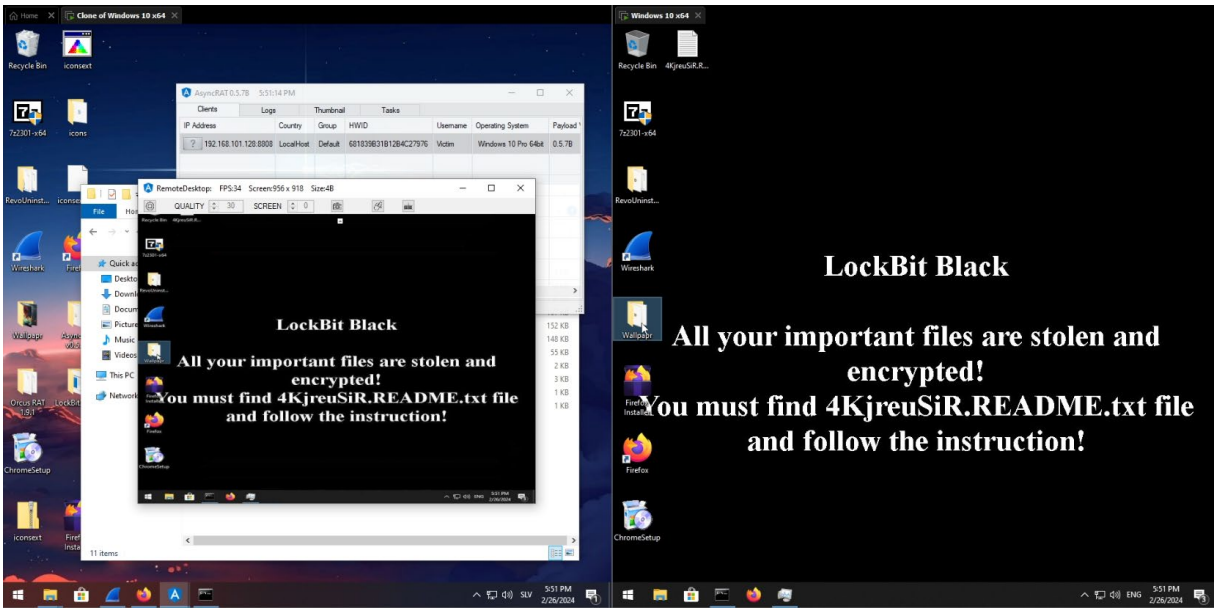
Na tej točki sem preprosto moral le še vstaviti izsiljevalski program v določen sistemski proces in s tem pričeti kibernetski napad.

Za votli proces sem izbral datoteko »RegAsm.exe«, ki je v osnovi orodje registra za potrjevanje določenih vrst datotek, s to funkcijo pa je postala glavni proces za uspešen zagon zlonamerne kode na žrtvini napravi. Votli proces je sistemski proces, ki ga pogosto uporablja programska oprema in v katerega lahko vstavimo zlonamerno kodo, da bi se izognili potencialni zaznavi iz strani protivirusnih programov. Zato je to še vedno zelo priljubljena metoda za okužbo sistemov.



Slika 19: Datoteka, ki je bila poslana v pomnilnik, uspešno okuži žrtvin računalnik
(Vir: Osebni arhiv)

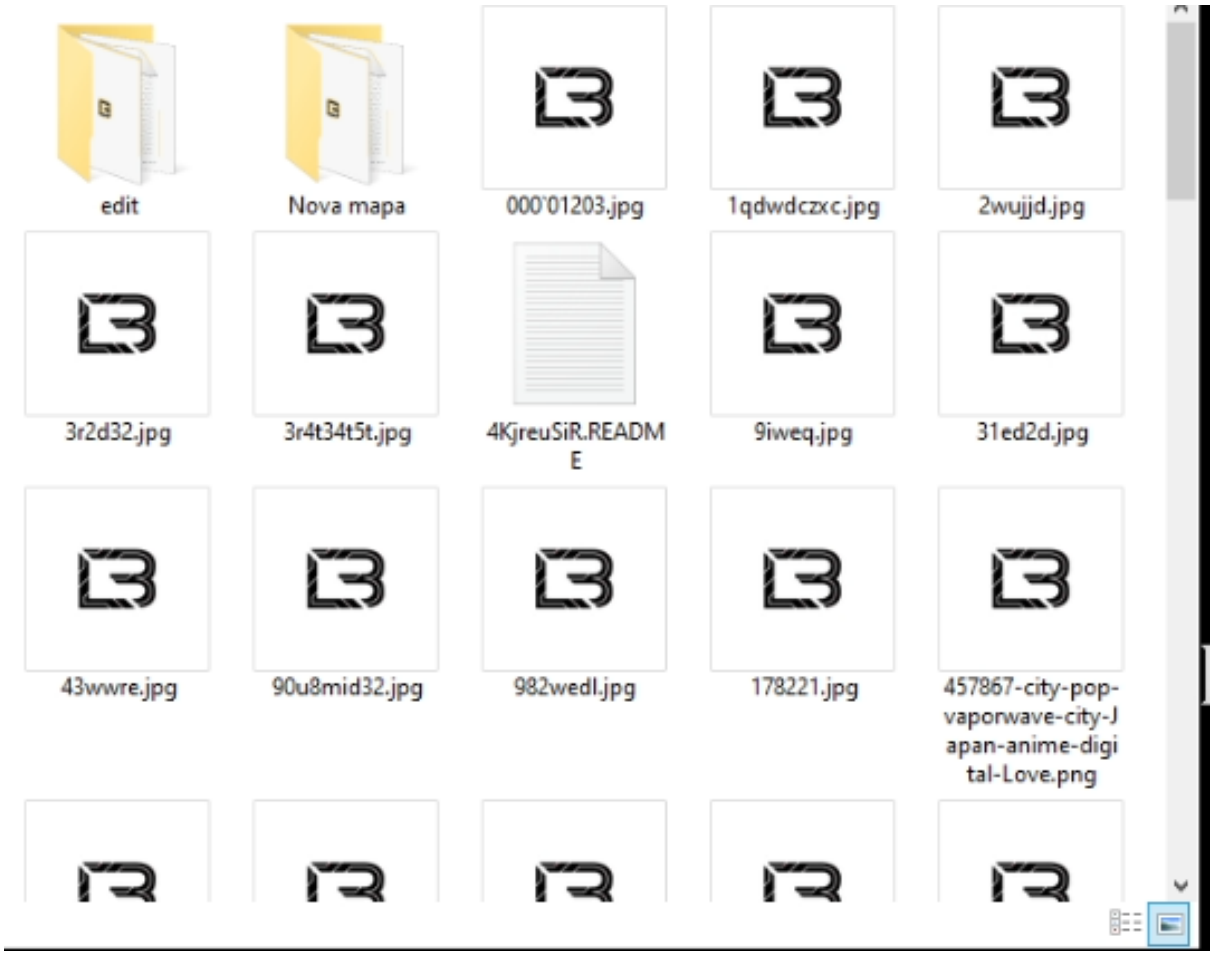
Po uspešni namestitvi zlonamerne kode v votli proces lahko vidimo, da je izsiljevalski program zelo hitro prevzel žrtvin sistem. Po tem je kibernetski napad uspešen, saj so žrtvine datoteke šifrirane in napadalec ima popoln dostop do naprave. Tega si seveda ne želi noben uporabnik.



Slika 20: Poln dostop do žrtvine naprave v omrežju

(Vir: Osebni arhiv)

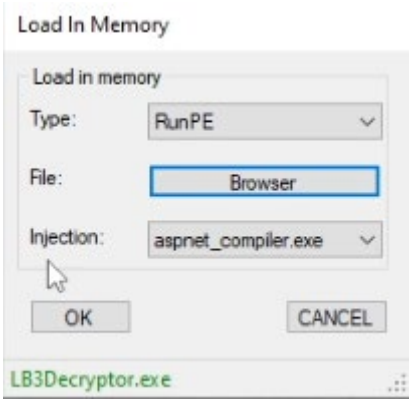
S pomočjo orodja za oddaljeni dostop lahko vidimo tudi monitor, kamero in slišimo mikrofon žrtve, ki smo jo napadli, kar je razvidno iz slike 20.



Slika 21: Šifrirane datoteke

(Vir: Osebni arhiv)

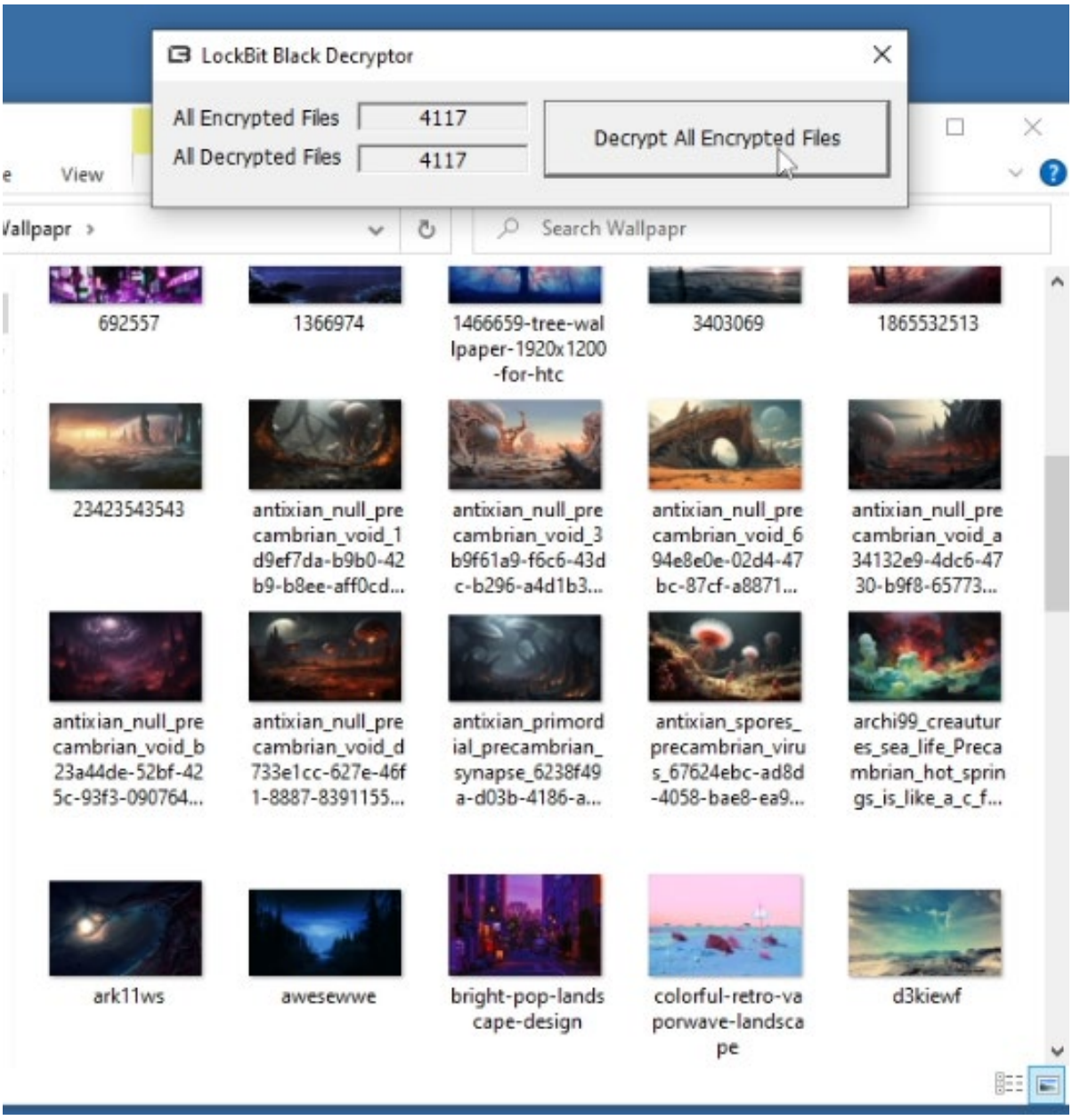
Na sliki 22 vidimo, da so datoteke šifrirane z datotečno pripono »4KkreuSir«. Samo en dešifrirni program lahko datoteke dešifrira in to je tisti, ki ga ima napadalec, ki je v osnovi napadel sistem.



Slika 22: Pošiljanje dešifrirnega programa v sistem po plačilu

(Vir: Osebni arhiv)

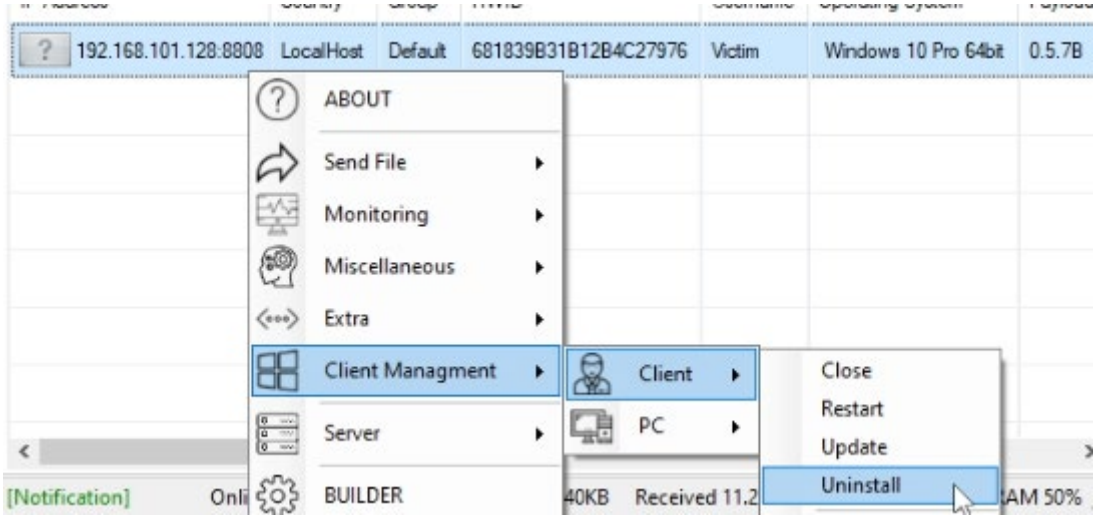
Potem ko je žrtev opravila plačilo, lahko napadalec v še en, tokrat drug votli proces, vstavi kodo programa za dešifriranje, ki pa bo datoteke tudi obnovil. Ta proces je viden na sliki 22. Uporabljen je popolnoma isti način kot za dejanski napad.



Slika 23: Dešifrirni program, ki obnovi vse datoteke

(Vir: Osebni arhiv)

Na tej točki je kibernetski napad zaključen. Vse zaklenjene datoteke so obnovljene na stanje pred napadom in so ponovno berljive.



Slika 24: Konec napada, prekinitev povezave z žrtvijo

(Vir: Osebni arhiv)

Ko napadalec zaključi, je spodobno, da za sabo tudi počisti. To naredi tako, da preprosto zbriše program za oddaljeni dostop in s tem je povezava med napadalcem in žrtvijo dokončno prekinjena.

4 REZULTATI RAZISKAVE

Hipoteza 1: Vdor v računalniško omrežje povprečnega, nezavarovanega podjetja je enostaven. Z demonstracijo napada na nezavorovan sistem sem to hipotezo potrdil. Z avtorskim videoposnetkom na platformi YouTube sem prikazal postopek napada in možnosti kraje podatkov z izsiljevalsko programsko opremo. Prikazan je tudi način dešifriranja datotek po uspešnem napadu. [3]

Hipoteza 2: Posamezna programska orodja nudijo različne vrste zaščit.
V poglavju 2.10 te naloge sem primerjal dva različna ponudnika protivirusne zaščite. Primerjava je pokazala razliko v zaščitnih modulih. S tem sem hipotezo potrdil.

Hipoteza 3: Kraji podatkov in izsiljevanju se je mogoče izogniti.
V podjetjih je pomembno izobraževanje kadrov in ozaveščanje o nevarnostih interneta. Pred zagonom neznanih datotek je potrebno pridobiti mnenje strokovno usposobljenega kadra. Tudi ta hipoza je potrjena.

5 ZAKLJUČEK

Po tej demonstraciji je zelo pomembno uvideti in razumeti, kako zelo enostavno je vdreti v sistem nezavarovanega podjetja že samo z dostopom do njihovega omrežja.

Z raziskovalno nalogo sem želel na preprost način pojasniti mnogo tem okoli kibernetske varnosti. Želim si, da bi bili podjetniki, kadrovske zasedbe podjetij in tehniki čimbolj ozaveščeni, kar se tiče njihove lastne varnosti in varnosti informacij v podjetjih in organizacijah. Zaradi vseh novih groženj in ranljivosti, ki se ponavljajo vsakodnevno, pa je gotovo, da se bo tudi v prihodnosti izvajala velika količina raziskav na tem specifičnem področju.

6 VIRI IN LITERATURA

[1] *Hekerji na spletu objavili del dokumentov iz kibernetskega napada na HSE.* (online). 2024. (citirano 16. 2. 2024). Dostopno na: https://www.dnevnik.si/1043039905**.**

[2] *Industrialcybersecuritypulse.* (online). 2024. (citirano 20.2.2024). Dostopno na: https://www.industrialcybersecuritypulse.com/strategies/insider-threat-how-ransomware-hackers-are-trying-to-bribe-your-trusted-employees.

[3] *Raziskovalna Jan Zorc.* (online). 2024. (citirano 25. 3. 2024). Dostopno na: https://www.youtube.com/watch?v=T62ZxHmaZcg.

[4] *Securelist.* (online). 2024. (citirano 17. 2. 2024). Dostopno na: https://securelist.com/and-now-an-mbr-ransomware/30626/ (zadnja sprememba 30. 11. 2010).

[5] *Varstvo o delovnih razmerjih.* 2024. (online). (citirano 17. 2. 2024). Dostopno na: https://www.iprs.si/fileadmin/user_upload/Pdf/smernice/Smernice_Varstvo_OP_v_delovnih_razmerjih_verzija_1.1_koncna.pdf.

[6] *Wikipedia.* (online). 2024. (citirano 17. 2. 2024). Dostopno na: https://sl.wikipedia.org/wiki/RSA (zadnja sprememba 26. 9. 2022).

[7] *Wikipedia.* (online). 2024. (citirano 19. 2. 2024). Dostopno na: https://sl.wikipedia.org/wiki/La%C5%BEno_predstavljanje (zadnja sprememba 19. 12. 2023).

[8] *Xcitium.* (online). 2024. (citirano 17. 2. 2024). Dostopno na: https://www.xcitium.com/history-of-ransomware.