**VISOKO UČILIŠTE ALGEBRA**

ZAVRŠNI RAD

# ZAŠTITA INFORMACIJSKOG SUSTAVA OD RANSOMWARE NAPADA

Žarko Vujanić

Zagreb, veljača 2018.

*„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada".*

*U Zagrebu, 9. travnja 2019.*

# Predgovor

S ovim radom dolazim do kraja svojeg trogodišnjeg puta prema nazivu stručni prvostupnik inženjer računarstva. Koristim priliku kako bih zahvalio osobama koje su mi pružile podršku i omogućili mi ovo putovanje.

Zahvaljujem se mentoru mr.sc. Draženu Praniću koji me je usmjeravao i pomagao mi u kreiranju ovoga rada. Hvala na pružanju nesebične pomoći i dijeljenju velikoga znanja.

Želim se zahvaliti i ostalim profesorima, asistentima i kolegama sa Visokog učilišta Algebra, koji su uvijek nesebično dijelili svoje znanje i pomoć.

I na kraju želim se zahvaliti svojoj obitelji i prijateljima koji su se trudili olakšati mi ovaj period života.

Algebra
visoko učilište

Visoko učilište Algebra I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 02412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2222 183 I info@algebra.digital I www.algebra.digital

**Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme završnog rada kojeg ste preuzeli u studentskoj referadi**.

# Sažetak

Sadržaj ovog rada prikazuje najveću informatičku sigurnosnu prijetnju današnjice zvana Ransomware. Svrha ovog rada je prikazati kako se korisnik može zaraziti od ovakve prijetnje, kako ova prijetnja funkcionira, što se očekuje od Ransomware-a u budućnosti i na kraju kako se zaštiti od ovakvoga napada. Praktični dio rada je prikazan sa nekoliko sigurnosnih politika koje se mogu upotrijebiti u većini informatičkih sustava. Svaki informatički sustav je jedinstven za sebe i ponekad nije moguće implementirati sve navedene sigurnosne politike, ali to ne znači da se ne može zaštiti već samo treba napraviti prilagodbu u implementiranju sigurnosnih politika.

**Ključne riječi:** Ransomware, prijetnja, budućnost, zaštita, implementacija sigurnosnih politika,

# Abstract

The content of this article shows the biggest security threat called Ransomware. The purpose of this paper is to show how a user can be infected with this threat, how this threat works, what is expected of Ransomware in the future and ultimately how to protect it from this attack. Practical part of the work is presented with several security policies that can be used in most IT systems. Each IT system is unique for itself and sometimes it is not possible to implement all of the security policies mentioned, but this does not mean that it can not be protected but needs only adaptation to the implementation of security policies.



**Key words:** Ransomware, threat, future, protection, implementation of security policies

# Sadržaj

# 1. Uvod

U današnjem ICT svijetu zbog velike konkurencije proizvođači imaju veći fokus kako nešto napraviti prvi nego kako se posvetiti sigurnosnom aspektu. Ovdje svoju priliku vide kibernetički (engl. *Cyber)* kriminalci sa svojim Ransomware napadima. Infiltracija jednog Ransomware-a dovodi sustav odnosno organizaciju do nedostupnosti svojih podataka, poslovnih ili financijskih izvještaja, nemogućnost rada organizacije… Jedan Ransomware može organizaciju dovesti do značajnih financijskih gubitaka do te mjere da odvede organizaciju u propast. Ransomware osim što radi financijsku štetu svojim djelovanjem može indirektno utjecati na čovjeka ili društvo. Jedan od primjera su nemogućnost rada javnog prijevoza nakon napada Ransomware-a i otkazivanje operacija u bolnicama zbog nedostupnosti podataka koji su kriptirani od strane Ransomware napada. Organizacija ili kompanija može umanjiti sigurnosne propuste koje stvaraju pojedini programi, protokoli…, ali za to je potrebno implementirati sigurnosne kontrole, politike i edukacije. Takva implementacija u početku zahtjeva veliku žrtvu financija, vremena i resursa. Da bi implementacija bila što uspješnija potrebno je razumjeti kako napadi rade i koje sigurnosne propuste maliciozni kodovi koriste.

# 2. Ransomware

Ransomware (ransom=otkupnina; ware=izvedenica od softvera) je naziv za skup malicioznih programa koji korisniku onemogućuju korištenje računala. Nakon zaraze, Ransomware može kriptirati datoteke ili onemogućiti korištenje na način da se pojavi početni ekran s određenom porukom koju nije moguće maknuti. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala. U zadnje vrijeme sve je više slučajeva u kojem se pojavljuje prvi navedeni slučaj u kojem maliciozni kod kriptira korisničke podatke i u zamjenu za njihovo dekriptiranje traži uplatu određenih novčanih sredstava[1]

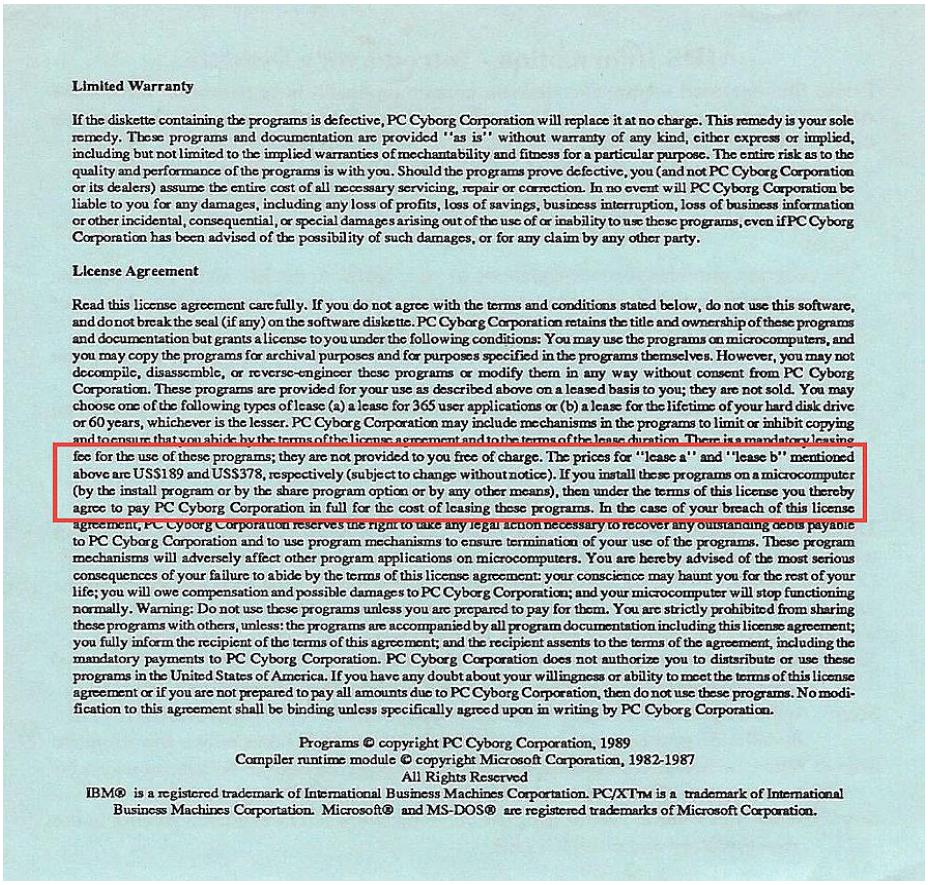
Postoje dva glavna oblika Ransomware programa: Prva je ona koja kriptira ometa ili zabranjuje pristup datotekama i druga je ona koja ograničavaju pristup ili zaključavaju korisnike izvan samih sustava.

Metoda napada i izvršenja se razlikuju ,ali cilj je uvijek isti a to je ucjena odnosno iznuđivanje.

## 2.1. Povijest

Prvi dokumentirani Ransomware u više različitih verzija iz 1989. godine se zvao AIDS Trojan, poznat i kao PC Cyborg virus ,a napravio ga je biolog Joseph Popp. Joseph Popp je zarazio 20000 disketa s upitnikom dali ste u opasnosti od zaraze AIDS-a, na kojima je bila naljepnica " Informacije o AIDS-u - Uvodne diskete " (engl. *AIDS Information - Introductory Diskettes*)! Diskete sa licenčnim ugovorom su bile podijeljene sudionicima Svjetske zdravstvene organizacije AIDS konferencije. U licenčnom ugovoru pisalo je: „…ako instalirate ovaj program na svoje računalo pristajete platiti PC Cyborg Corporation punu naknadu za ovaj proizvod…" Slika 2.1 Prikazuje licenčni ugovor koji su sudionici Svjetske zdravstvene organizacije AIDS konferencije dobivali uz diskete.

[1] http://www.cert.hr/Ransomware, 2018



**Limited Warranty**

If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of mechantability and fitness for a particular purpose. The entire risk as to the quality and performance of the programs is with you. Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, loss of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

**License Agreement**

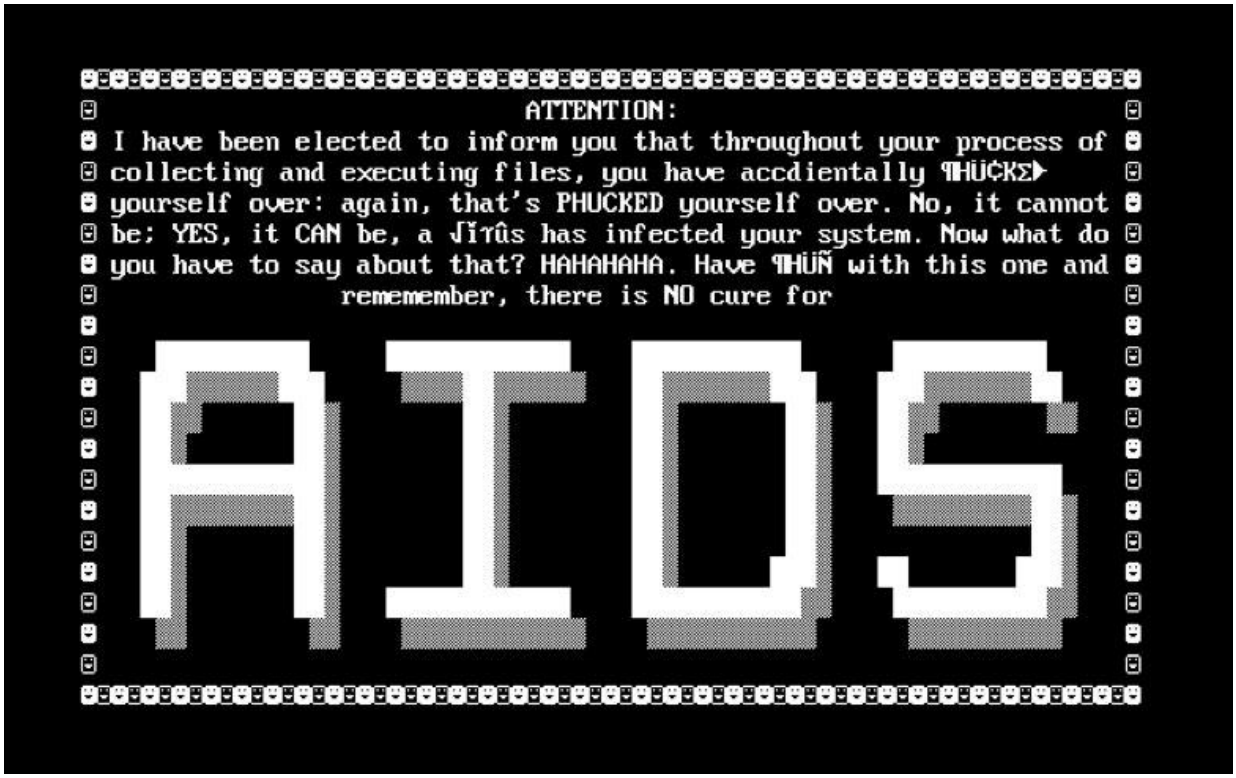
Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement; and the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation does not authorize you to distsribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

Programs © copyright PC Cyborg Corporation, 1989
Compiler runtime module © copyright Microsoft Corporation, 1982-1987
All Rights Reserved
IBM® is a registered trademark of International Business Machines Corportation. PC/XT™ is a trademark of International Business Machines Corportation. Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

Slika 2.1 Licenčni ugovor[2]

U jednoj od verzija bi nakon pokretanja virusa brojač počeo odbrojavati 90 podizanja sustava. Kada bi brojač došao do 90 pojavila bi se obavijest kako je sustav zaražen i korisnik više ne može pristupit svojim podatcima. Da bi korisnik opet dobio pristup svojim dokumentima morao je platiti $189 ili $378 (ovisno o verziji) PC Cyborg Corporation u Panami. Slika 2.2 Prikazuje kako je izgleda računalo nakon zaraze s AIDS malicioznim kodom.

[2] https://www.gdatasoftware.com/blog/2017/04/29716-Ransomware-changed-my-life, 2018

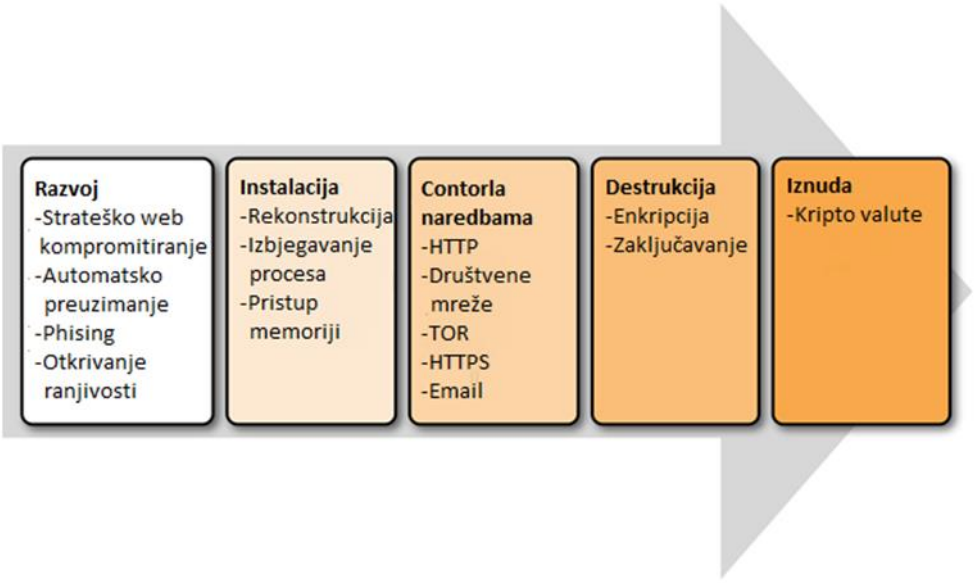



Slika 2.2 AIDS Ransomware[3]

## 2.2. Vrsta napada i kako funkcionira Ransomware

Ransomware napad se sastoji od pet faza: Razvoj, instalacija, kontrola naredbama, destrukcija i iznuda. Slika 2.3 prikazuje životni ciklus Ransomware napada u pet faza.

[3] http://theconversation.com/why-save-a-computer-virus-56967, 2018




Slika 2.3 Ciklus Ransomware napada[4]

### 2.2.1. Razvoj

U prvoj fazi instalira se komponenta na sustav žrtve koja se koristi kako bi inficirala, kriptirala ili zaključala sistem. Postoji nekoliko metoda koje opisuju kako na sustav žrtve ubaciti maliciozni kod.

- **Automatsko preuzimanje -** Pojavljuje se kada sistem automatski preuzme dio malicioznog koda bez znanja krajnjeg korisnika. Postavlja se na sistem kroz prevaru korisnika npr. kada korisnik posjeti neku Internet stranicu koja radi redirekciju ili otvara novi skočni prozor na drugu Internet stranicu koja inficira sistem malicioznim kodom.
- **Strateško web kompromitiranje (engl. *watering hole*) -** Kriminalci u ovom napadu nagađaju ili promatraju koju web stranicu žrtva često posjećuje te zaraze tu web stranicu malicioznim kodom i čekaju da ju žrtva otvori. Nakon što žrtva otvori kompromitiranu stranicu maliciozni kod se može infiltrirati u sustav žrtve.
- **Pecanje e-poštom (engl. *phishing emails*) -** Jako popularan način za kibernetičke kriminalce kako se infiltrirati u neki sustav. Meta može biti bilo tko odnosno kriminalac nema unaprijed definiranu ciljanu metu ili meta može biti ciljano neka

[4] Allan Liska and Timothy Gallo Ransomware. Defending Against Digital Extortion, studeni 2016.

osoba, organizacija… Kriminalac šalje žrtvi mail u kojoj je privitak ili link koji vodi do stranice s malicioznim kodom. Ako korisnik otvori primljeni privitak ili link kod će se pokušati infiltrirati u sustav. Kriminalci dolaze do mail adresa na način da kupe liste od nepoštenih email i internet servis pružatelja usluga, organizacija koja se bavi e-novostima … ili kupuju mail adrese ukradene od strane hakera. Neki koriste programe koji pretražuju Internet stranice i sve riječi koje odgovaraju opisu email adrese (npr. @) sakupljaju u listu.

- **Otkrivanje ranjivosti** - U ovoj metodi kibernetički kriminalac skenira mrežu odnosno traži sigurnosne propuste na sustavima koji su izloženi internetu te na taj način pokušava ubaciti svoj maliciozni kod. Jedan od napada je na računala s uključenim RDP-om, radi se najčešće o iskorištavanju slabih ili najčešćih lozinki. Napadač može pomoću raznih alata u kratko vrijeme detektirati da li se RDP na tome računalu koristi ,ako je odgovor potvrdan pokušava se spojiti isprobavajući lozinku po lozinku. Postoje i napadi na druge programe koji omogućuju spajanje preko interneta (npr. TeamViewer, VNC, ...).

### 2.2.2. Instalacija

Kada se maliciozni kod uspješno infiltrirao u sustav potencijalne žrtve on može početi obavljati svoju namjenu. Inficiranje sustava se može obaviti na različite načine, jedan od metoda instalacije je preuzimanje na kapaljku (engl. *download dropper methodology*). U ovoj metodi je u sustav infiltriran mali komad koda koji je dizajniran tako da izbjegne detekciju, a da istovremeno može komunicirati sa izvođačem napada. Kada je komunikacija uspješno uspostavljena dio koda započinje s preuzimanjem Ransomware-a. Nakon što se i sam Ransomware infiltrirao u sustav on započinje svoju instalaciju na sustav. U slučaju Windows sustava, Ransomware postavlja ključeve u registar sustava koji će osigurati da se maliciozni kod pokrene svaki put s računalom. Za ostale sustave iskoristit će prednosti nesigurnog app dućana (obično za uređaje Android) ili ukradene ili valjane certifikate za iOS. Kako bi napadač izbjegao otkrivanje AV skenera, Ransomware komponente se raščlanjuju u različite skripte, procese, batch datoteke i druge alate. U drugoj fazi Ransomware odlučuje dali je vrijedno zaraziti sustav. Ako je Ransomware odlučio zaraziti sustav započinje postupak koji često izgleda kao običan Windows proces. U tom trenutku maliciozni kod postaje jedinstven koristeći MD5 hash od imena računala ili nekog drugog

jedinstvenog identifikatora poput Mac adrese. Na taj način raspolaže s informacijama koliko i koja računala je zarazio. U ovoj fazi dropper pokreće nekoliko skripti koje isključuje sve Windows zaštite poput AV, kopiju sjenke (engl. *Shadow copy*), sistemskog oporavka (engl. *system recovery*)… Kada se Ransomware postavio kao Windows proces, započinje faza kontrola naredbama. [4]

### 2.2.3. Kontrola naredbama

Ransomware zahtjeva uspostavu nekakvog komunikacijskog kanala kako bi mogao provoditi kontrolu naredbama. Takav sistem se koristi za poduzimanje efektivnog slijedećeg koraka. Kada se maliciozni kod implementira i instalira na sustav, on će pokušavati doći do poslužitelja koji mu zadaje određene instrukcije. Te instrukcije su specifičnih zahtjeva kao što su: identifikacija dokumenata koje treba kriptirati, koliko treba čekati do pokretanja procesa… Neke verzije Ransomware-a će javiti ucjenjivaču koje domensko ime, koje verzije OS, web preglednika, AV… potencijalna žrtva koristi. Kanali koji se koriste za kontrolu naredbama ovise o verziji i familiji malicioznog koda. U nekim slučajevima to može biti jednostavno kao web komunikacija koja iskorištava ne kriptirani HTTP protokol prema kompliciranim sustavima koji iskorištavaju ugrađene TOR[5] usluge za povezivanje. Složeni sustavi poput TOR-a otežavaju u određivanju točne lokacije kriminalaca koji sudjeluju u iznuđivanju, a neke inačice Ransomware-a zapravo instaliraju TOR klijente na krajnje točke kako bi osigurali sigurnu komunikaciju. [4]

### 2.2.4. Destrukcija

U ovom trenutku ključ koji se koristi za enkripciju dokumenata ili zaključavanje sustava je aktivan i spreman. Svi dokumenti koji su identificirani u procesu kontrole naredbom biti će kriptirani. To uključuje sve Microsoft Office dokumente, slike, pdf-ove i još mnoge druge dokumente s poznatom ekstenzijom. Neke inačice ne samo da kriptiraju dokumente već i ime dokumenta kako bi korisnik na teži način saznao do kuda se Ransomware proširio i koje sve dokumente je korisnik izgubio. [4]

---

[5] https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-07-197.pdf, 2018

### 2.2.5. Iznuda

Nakon što su dokumenti kriptirani žrtvi se pojavljuje natpis na ekranu kako im je sustav ugrožen. Ucjenjivači imaju nekoliko metoda koji će potaknuti žrtvu na plaćanje. Neke verzije Ransomware-a omogućiti će svojim žrtvama besplatnu dekripciju jednog dokumenta kako bi ih uvjerio da postoji ključ pomoću kojeg će doći do svojih dokumenata. U nekim verzijama cijena otkupnine poskupljuje što korisnik duže čeka. Pojedine verzije postupno brišu dokumente sve dok korisnik ne uplati otkupninu ili dok ne obriše sve dokumente korisnika. Cijena otključavanja se u prosjeku kretala između 300 i 500 dolara ,ali u Bitcoin valuti. Za otključavanje dokumenata kompanije cijena se penjala i do nekoliko miliona dolara.

## 2.3. Platiti otkupninu ili ne

Prema istraživanju IBM Security-a više od pola ispitanika ne bi platilo otkupninu za vračanje podataka. Situacija je potpuno drugačija kada se radi o poslovnim subjektima odnosno o poslovnim korisnicima. 70% ispitanika je izjavilo da bi platili otkupninu samo kako bi vratili poslovna i financijska izvješća. [6]

U nekim slučajevima je „jeftinije i brže“ platiti otkupninu nego vraćati podatke iz rezervne kopije (engl. *Backup*), a to možemo procijeniti jako brzo računajući vrijeme vračanja podataka, vrijeme troška administratora koji vraća podatke, vrijeme koje cijela organizacija odnosno zaposlenici gube zato što nisu u mogućnosti raditi dok se podatci ne vrate i dok sustav nije siguran za rad. Prema navedenom računica je puno veća u odnosu na njenu otkupnu vrijednost, uz sve to opet postoje razlozi zašto ne platiti.

Plaćanje otkupnine se ne preporučuje. Ne postoje garancije da će napadač žrtvi vratiti podatke odnosno da će joj poslati ključ za dekriptiranje podataka nakon uplate.

Prema istraživanju Trend Micro-a oko 33% organizacija koje su platile otkupninu nisu nikada dobili ključ za dekriptiranje podataka.[7]

[6] https://www-03.ibm.com/press/us/en/pressrelease/51230.wss, 2018
[7] https://blog.trendmicro.com/paying-for-Ransomware-could-cost-you-more-than-just-the-ransom, 2018

Također uplatom žrtve potiču sve veći razvoj Ransomware-a. Uplatom žrtva ulazi u hakerovu listu onih koji su voljni platiti (engl. *want to pay*), te na taj način privlači još veću pažnju kibernetičkog kriminalca i zbog toga može postati opet potencijalna žrtva. Plaćanjem se potiče kibernetičke kriminalce na osmišljanje još više različitih virusa, povećava im se kreativnost i imaju veću želju za kreiranjem novih familija Ransomware virusa.

# 3. Zašto ne smijemo zanemarivati Ransomware napad

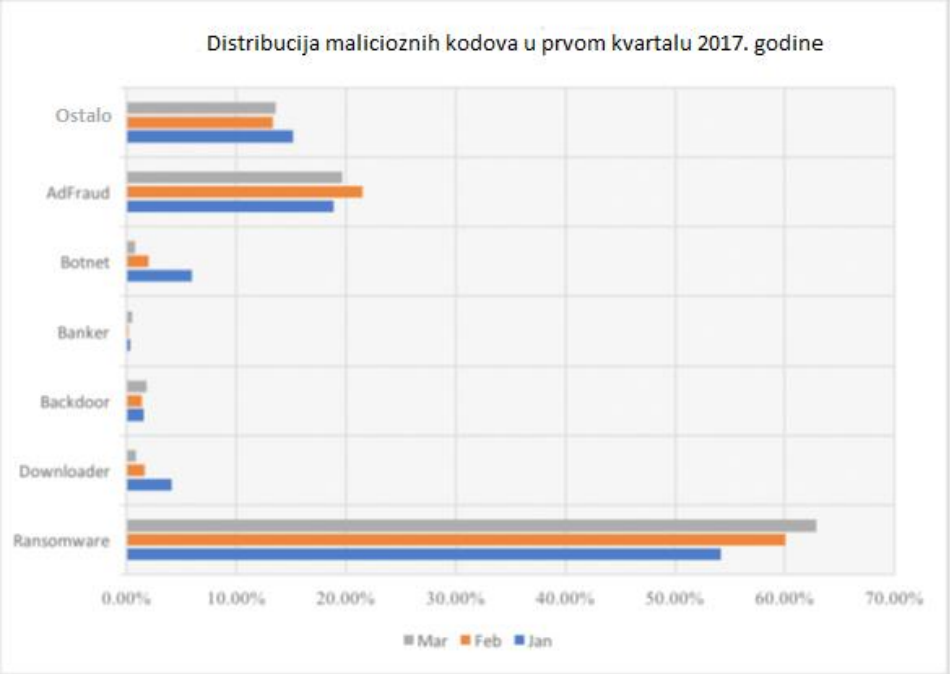
Nakon prvog zabilježenog Ransomware-a slijedi dugačka pauza od 1989. pa sve do 2006. Kada se pojavljuje Trojan.Gpcoder. Pojava novijih verzija Ransomware događa se jako sporo oko jedna verzija kvartalno, a ponekad jedna verzija godišnje.

Sredinom 2014. Godine Ransomware doživljava svoju revoluciju i u samo pola godine pojavljuje se sedam "obiteljskih" verzija Ransomware-a i od tada rapidno raste napad različitih Ransomware-a.

Prema istraživanju Kaspersky-og u prvom kvartalu 2016. Godine učestalost napad na korisnika je bio svakih dvadeset sekundi u trećem kvartalu on je iznosio svakih deset sekundi. Kod poslovnih klijenata učestalost napad bio je 2 minute u prvom kvartalu 2016. da bi se u trećem kvartalu on povećao na svakih četrdeset sekundi. [8]

U prvom kvartalu 2017. Godine Ransomware je zauzeo najveći postotak oko 60% napada u odnosu na sve ostale maliciozne napade. Slika 3.1 Prikazuje statistiku distribucije malicioznih kodova u prvom kvartalu 2017. godine. Na slici je je vidljivo kako se distribucija Ransomware kodova za dva mjeseca povećala za deset posto.

[8]https://www.kaspersky.com/about/press-releases/2016_attacks-on-business-now-equal-one-every-40-seconds, 2018




Slika 3.1 Statistika distribucije malicioznih kodova[9]

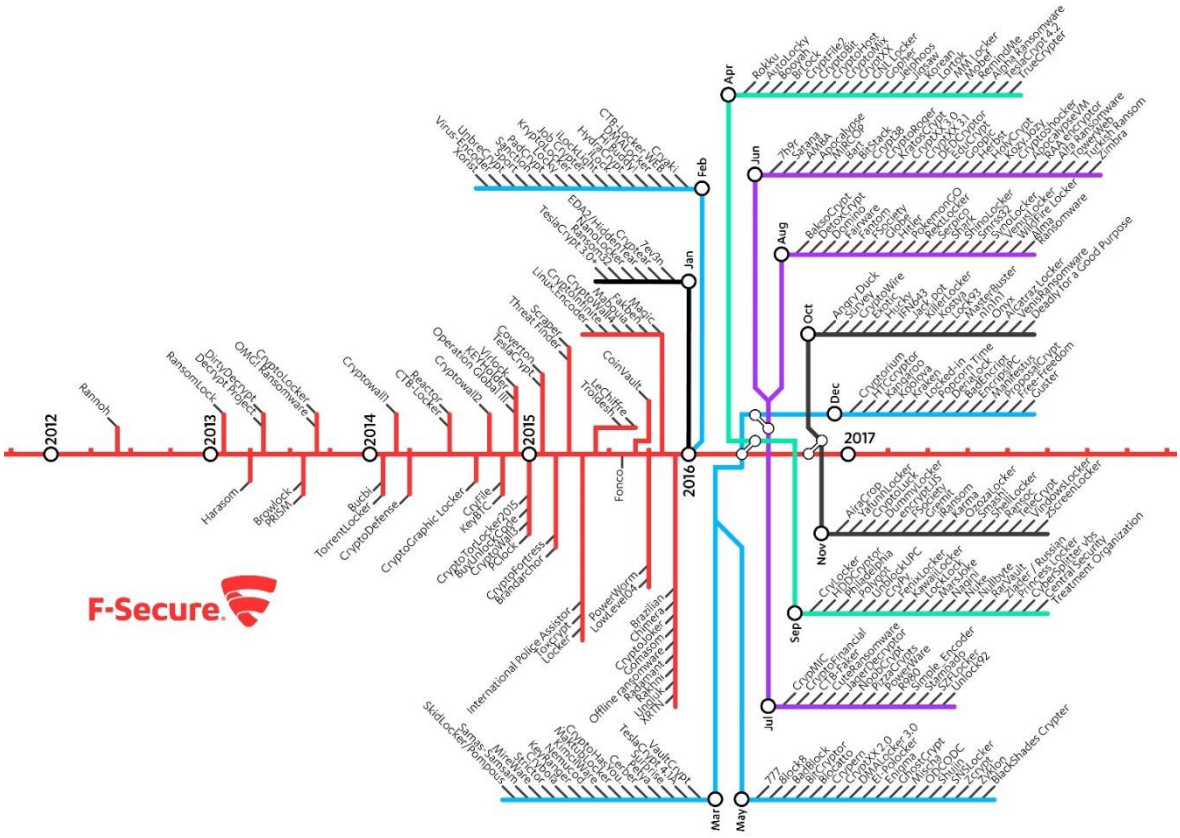
## 3.1. Jučer, danas i sutra

Gledajući životnu crtu Ransomware-a Slika 3.2 koja pokazuje njegovo razvijanje od 2012. godine pa do kraja 2016. godine otprilike možemo znati što nas očekuje u budućnosti.

Forrester-ovo istraživanje pokazuje da bi 2018. godine kibernetički kriminalci svoju zaradu mogli tražiti na IOT uređajima i instaliranju Ransomware-a na POS uređajima.[10]

Preciznije gledano sve što je umreženo je pod prijetnjom kao npr. televizori, pametne kuće, frižideri, veš mašine pa čak i automobili.

[9] https://blog.barkly.com/Ransomware-statistics-2017, 2018
[10] https://www.infosecurity-magazine.com/news/forrester-expect-pos-Ransomware/, 2018




Slika 3.2 Životna linija novih verzija Ransomware-a kroz pet godina [11]

### 3.1.1. Najznačajnije Ransomware familije

Da bi Ransomware napad bio što učinkovitiji on osim kriptiranja koristi i određene alate. Alati koje koriste najpoznatije Ransomware familije: EternalBlue exploit za Windows-e koju je razvila Američki NSA, EternalBlue iskorištava sigurnosni propust SMBv1 protokola. Microsoft je 14. ožujka 2017 objavio sigurnosnu zakrpu MS17-010 za propust na SMBv1 protokolu za sve sustave koji nisu ažurirani, pa čak i za one koje ne postoji podrška duže vrijeme kao što su Windows XP ili Windows Server 2003. Mimikatz je alat koji se koristi za izvlačenje korisničkog imena i lozinke iz memorije računala. PsExec omogućuje pokretanje procesa na udaljenim sustavima. WMIC je alat komandne linije koja služi za administriranje računala.

[11] https://safeandsavvy.f-secure.com/2017/02/21/why-Ransomware-is-so-good-at-ripping-you-off/, 2018

Evo kratkog pregleda najvažnijih i najaktualnijih familija:

- **WannaCry -** Najintenzivniji period napada bio je od 12.5.2017 – 15.5.2017. pri čemu je napao preko 200.000 Windows sistema širom svijeta. Svi sustavi na kojima nije bila instalirana sigurnosna zakrpa MS17-010 postali su potencijalna žrtva. Da bi maliciozni kod zarazio računalo nije mu potrebna interakcija korisnika. Kada se pokrenuo ovaj maliciozni kod širio bi se putem SMB protokola koristeći EternalBlue. WannaCry je onesposobio svu bolničku infrastrukturu širom UK, a ugrozio je i njihovu nacionalnu sigurnosnu agenciju.

  Najpoznatiji zaražene organizacije su: Telefonica iz Španjolske, Renault iz Francuske, Njemačke željeznice, FedEx
- **NotPetya -** Radi se o izuzetno sofisticiranom malicioznom kodu koji koristi različite načine širenja, kombinirajući različite alate.: PsExec, WMIC, Mimikatz i EternalBlue. S obzirom da je ovaj maliciozni kod koristio EternalBlue i za njega je vrijedila sigurnosna zakrpa MS17-010. NotPetya je distribuiran ukrajinskim računovodstvenim softver-om zvan MeDoc, koji se koristi za podnošenje prijave poreza u Ukrajini. MeDoc je imao u sebi stražnje ulaze (engl. *Backdoor*) kojeg je iskoristio ovaj maliciozni kod i proširio se pomoću automatskog ažuriranja sistema. Ako maliciozni kod nije pokrenut na domenskom kontroleru i nema pristup DHCP-u prvo će pokrenuti skeniranje mreže i saznati što se sve nalazi na mreži. Kada ima administratorska prava i kada se može slobodno kretati po mreži pokreće alate PsExec i WMIC te na taj način inficira računala i kriptira podatke. Nakon kriptiranja dokumenata NotPetya postavlja zadatak ponovnog pokretanja računala i uz taj zadatak postavljene su još neke metode pokretanja u slučaju da jedna od njih zakaže. Pri ponovnom pokretanju računala pojavljuje se CHKDSK ekran koji se pojavljuje nakon pada sistema, ali u ovom slučaju računalo ne radi CHKDSK nego NotPetya vrši enkripciju tablicu glavnih datoteka (engl. *Master file table*). Kada je enkripcija gotova prikazuje se poruka o otkupnini te računalo postaje beskorisno, jedino što se može je upisati ključ za dekripciju ili formatirati računalo. NotPetya je bio destruktor njegova namjena nije bila da se kibernetički kriminalci obogate. Namjena mu je bila destrukcija što više računala i sustava.

  Najpoznatiji zaražene organizacije su: A.P. Moller-Maersk, Fedex, Beiersdorf: Nivea

- **GoldenEye -** Prvi napad je primijećen u Ukrajini gdje je pogođena nacionalna banka i najveća Kijevska zračna luka. Ovaj maliciozni kod je kombinacija Petya i Mischa malicioznog koda. Koji se isto kao i WannaCry širi putem SMB protokola koristeći EternalBlue. Za razliku od Petya-e, GoldenEye osim što kriptira podatke on sprječava računalu da se podigne i na taj način onemogućuje korisniku povrat podataka. Nakon enkripcije i ponovnog pokretanja računala korisnik jedino što može vidjeti na ekranu je mrtvačka glava sa zahtjevima gdje i koliko uplatiti.
  Najpoznatiji zaražene organizacije su: Englesko zdravstvo, Ukrajinska nacionalna banka

## 3.2. Kako se financira

Najveći problem kriminalaca u cijelom procesu od izrade Ransomware-a do naplate otkupnine je kako sredstva od otkupnine imati u svojim rukama. Za svaku bankovnu transakciju koju osoba ili organizacija napravi postoji trag. To je jedan od glavnih razloga zašto Ransomware napada nije bilo od 1989. do 2012. godine kada se pojavljuju kripto valute. Kripto valute osiguravaju anonimnost te zbog toga predstavljaju idealno sredstvo plaćanja za kriminalce.

## 3.3. Najveće zabilježene štete

Najveća svjetska istraživačka i izdavačka organizacija koja piše o globalnoj kibernetičkoj ekonomiji Cyberysecurity Venturees tvrdi da je 2015. godine šteta od Ransomware napada iznosila 325 miliona dolara. Cyberysecurity Venturees predviđa da će se šteta 2017. popesti za 350% i ona će iznositi oko 5 milijardi dolara. [12]

Štetu možemo podijeliti u više kategorija: Gubitak produktivnosti, gubitak podataka, financijska šteta koju je kompanija pretrpjela pri otkupnini Ransomware-a, trošak vremena i financija za povrat podatka… Kompanije obično ne izlaze s podatcima o šteti koju su pretrpjele tako da je teško sa 100% sigurnošću reći koliko ona iznosi.

[12] https://cybersecurityventures.com/Ransomware-damage-report-2017-5-billion/, 2018

Najveća zabilježena šteta koju je pretrpjela jedna organizacija je Danska transportna i logistička organizacija Maersk. Procijenjena šteta je 300 milijuna dolara. A.P. Moller-Maersk bio je jedan od mnogih globalnih tvrtki koji je pogođen zlonamjernim softverom kasnije poznat kao NotPetya. Prema neslužbenim informacijama napad je imao utjecaj na cijelu Windows okolinu, točnije kriptirao je sve podatke organizacije A.P. Moller-Maersk. Ovaj kibernetički napad bio je do tada nevidljiva vrsta zlonamjernog softvera za Windows sustave i antivirusne programe i tada nisu postojale zakrpe i ažuriranja koja bi spriječila ovakav napad.

Najveći „platiša“ Južno Korejski web hosting pružatelj usluga Nayana sa prvotnih 550 Bitcoin-a (oko 1,62 miliona dolara) uspjeli su ispregovarati cijenu od 397,6 Bitcoin-a (oko milion dolara). Napad se dogodio 10. lipnja. Nakon toga je krenuo dugotrajan pregovarački proces i prikupljanje financijskih sredstava.

Prilikom ovog napada koristio se Erebus Ransomware koji je zarazio i kriptirao 153 Linux servera pri čemu je to utjecalo na 3400 klijenata. Ransomware je iskoristio sigurnosne propuste na sustavima iz 2006. i 2008. godine.

# 4. Zaštita sustava

Zaštita sustava se ne smije bazirati samo na jedno sigurnosno pravilo, ona se mora sastojati od više različitih instrukcija, pravila i politika. Australska vlada je u travnju 2013. izdala obvezu za sve vladine organizacije „Top 4 strategije o umanjenju kibernetičkog upada“ (engl. *Top 4 Strategies to Mitigate Targeted Cyber Intrusions).* Na taj način je smanjeno preko 85% upada u informacijski sustav. Ovo su odlični sigurnosni temelji svakog komunikacijsko informacijskog sustava. Iskorištavanjem navedenih strategija može se sa samo malo uloženih sredstava, vremena i resursa riješiti većinu sigurnosnih problema i propusta. U nastavku biti će prikazano koje sve korake treba poduzeti kako bi umanjili ili potpuno uklonili opasnost od Ransomware napada.

## 4.1. Ažuriranje sustava

Operacijski sustav je „srce“ informatičkog okruženja i oko njega se gradi cijela informatička infrastruktura. Novija ažuriranja za OS sadrže zaštite od malicioznog ponašanja u više razina. Ona mogu biti na način da je proizvođač napravio zakrpu za sigurnosni problem te je na taj način umanjio sigurnosni propust ili na način da je onemogućio određeni protokol ili aplikaciju i na taj način zaštitio sustav od određenog napada. Nadogradnja i ažuriranje operativnog sustava mora biti najvećeg prioriteta. Operacijski sustavi koji više nemaju sigurnosnu podršku nije preporučljivo koristiti.

## 4.2. Ograničavanje admin prava krajnjim korisnicima

Administrativna prava su kreirana tako da omogućuju jedino povjerljivim osobama konfiguriranje, administriranje i nadgledanje sustava. Administrator na jednom sustavu može doći do bilo kakve informacije i može napraviti bilo kakvu promjenu na takvom sustavu i iz tog razloga pristup korisničkom računu sa administrativnim ovlastima imaju samo povjerljive i ovlaštene osobe koje mogu konfigurirati, administrirati i nadzirati informatički sustav.

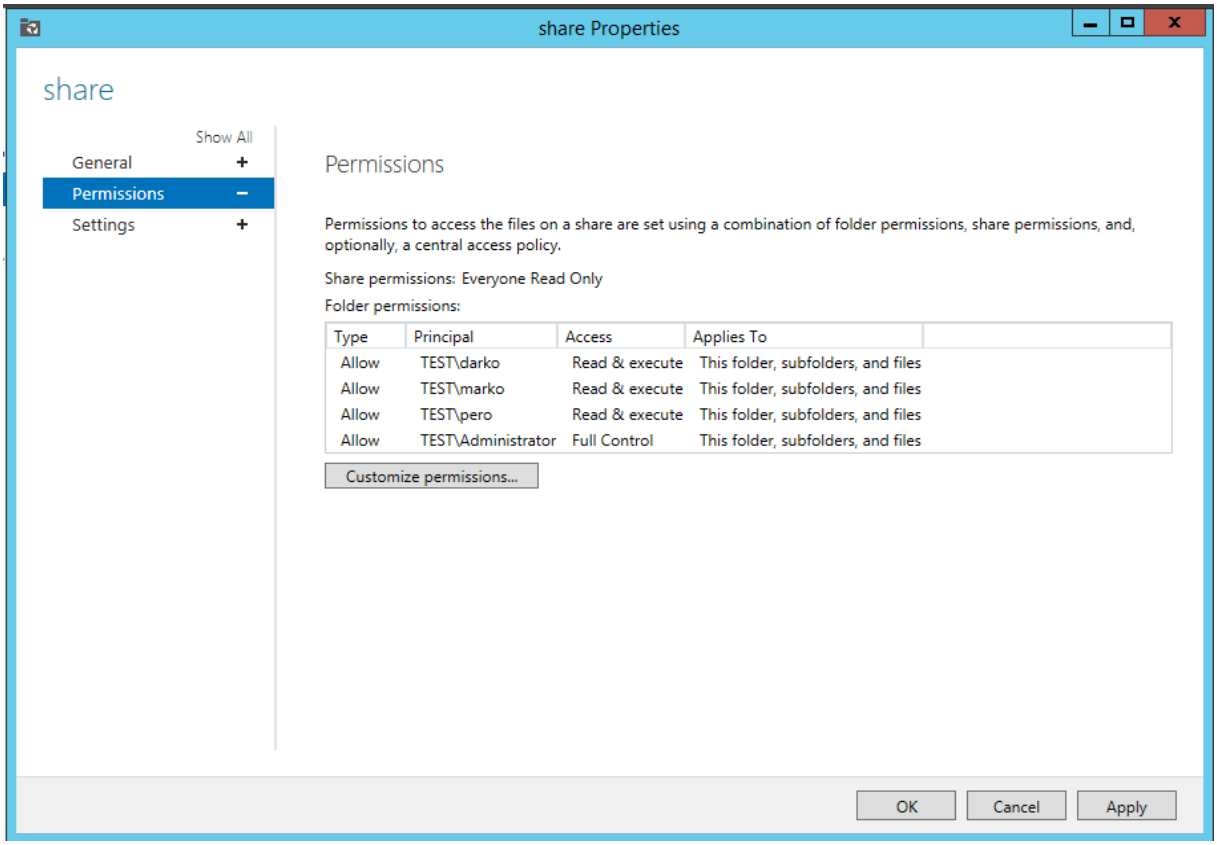
Lokalni administratori ne mogu raditi izmjene u AD-u, ali svejedno mogu priuštiti dovoljno problema i sa svojih računala. Lokalni administrator može izbaciti računalo iz domene ili

instalirati hrpu nepotrebnih (i potencijalno opasnih) aplikacija. Idealan scenarij je onaj u kojem prava lokalnog administratora imaju samo djelatnici IT odjela. Ograničavanje prava se može regulirati na razini računala ili na razini domene odnosno na razini informatičkog sustava. [13]

## 4.3. Reguliranje dozvolama pristupa na dijeljenim dokumentima

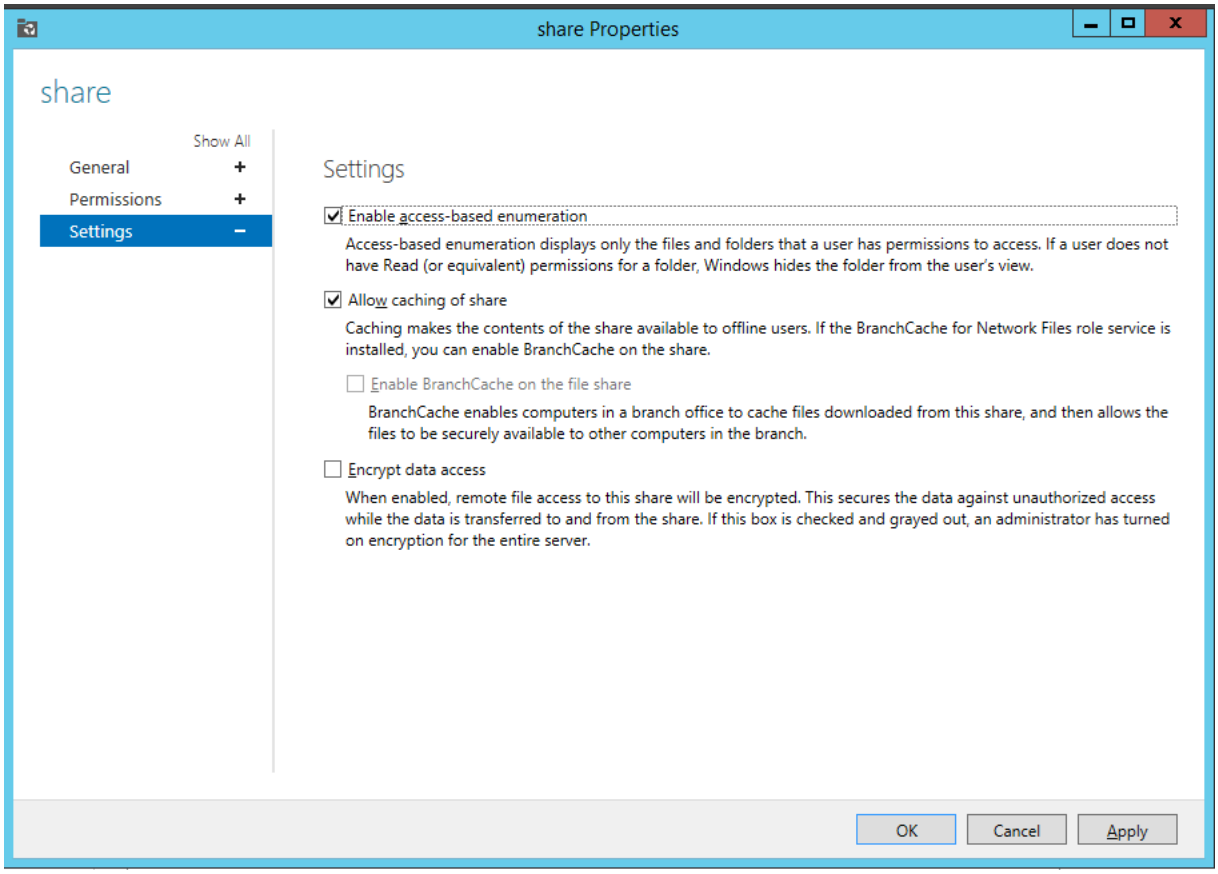
Dozvole pristupa određuju razinu mogućnosti koju korisnik ima na nekom resursu, primjerice mapi ili datoteci. Pravilno podešenim dozvolama pristupa na dijeljenim dokumentima onemogućuje se pretraživanje i mijenjanje dokumenata na kojima pojedini korisnik nema pravo. Preporuka je da se ovakva pravila koriste i da se nikome ne daju maksimalna prava. Za one korisnike koji smiju imati prava čitanja, zapisivanja i mijenjanja, daju se prava čitanja (engl. *Read*),pisanja (engl. *Write*) i modificiranja (engl. *Modify*). Za one korisnike koju imaju samo pravo čitanja dodjeljuju se samo read prava, za korisnike koji ne smiju pristupati određenim dokumentima ne daju se nikakva prava. Slika 4.1 Prikazuje kako podesiti pravila pristupa na dijeljenim dokumentima preko Server Manager-a

[13] Medić, G. (2014) Administracija operacijskih sustava, Lab 11 Konfiguracija kroz Group Policy -1. dio-, 2014




Slika 4.1 Server Manager i određivanje prava pristupa

Slika 4.2 Prikazuje kako podesiti ABE. Opciju ABE treba naknadno uključiti ona se ne kreira automatski, a omogućujemo postavljanjem kvačice kraj opcije „Enable access-based enumeration“. Ova opcija omogućuje administratorima „skrivanje“ onih dokumenata na kojima korisnici nemaju prava.




Slika 4.2 Uključivanje ABE

## 4.4. Pričuvna pohrana podataka

Pričuvna pohrana podataka (engl. *Backup*) jedna od najvažnijih stavki u svijetu informacijskih tehnologija, to je proces u računarstvu koji se odnosi na izradu kopije podataka i sistema originalnog izvora za slučaj da se originalni izvor podataka ošteti ili izgubi. Podaci mogu biti datoteke ili/i programi. Pričuvni podaci se obično trebaju držati na više mjesta radi bolje sigurnosti, također moguće je držati podatke na nekom udaljenom Internet serveru.[14] Za kućnog korisnika sa manjim financijskim sredstvima sigurnosnu kopiju je moguće napraviti na CD-u, DVD-u, usb, tvrdom disku… Za velike sustave takav način pričuvne pohrane podataka nije primjeren. Tvrtke pri tome mogu koristiti različite mehanizme, tehnologije pričuvne pohrane kao što su magnetne trake, sustave za pohranu podataka (engl. storage), korištenje tehnologije u oblaku… Kada korisnik ili organizacija

[14] https://bs.wikipedia.org/wiki/Backup, 2018

ima riješenu potrebnu proceduru za pričuvnu pohranu podataka potrebno je istu zaštiti od Ransomware ili drugih napada. Zaštita može biti:

- Pričuvna pohrana podataka čuva se na medijima koji su odvojeni fizički ili mrežno od produkcijskog sustava
- Spremanje na oblaku (engl. Cloud)
- Posebno korisničko ime sa jedinstvenim vjerodajnicama koji ima jedini pristup i pravo na pohranu i izmjenu pričuvnih podataka
- Korištenje drugih protokola za pričuvnu pohranu podataka

Za određene organizacije duljina čuvanja pričuvnih podataka određeno je zakonom. Za korisnike i organizacije kojima nije zakonski određeno koliko dugo moraju čuvati pričuvnu pohranu podataka, preporuka je što duže koliko resursi i financije mogu to podnijeti.

### 4.4.1. Mogući izazovi

Pričuvna pohrana podataka  jedino što traži je prostor i to zna stvarati korisnicima velikih problema, drugi problem je valjanost pričuvne pohrane podataka. Ponekad se zna dogoditi da korisnik radi pričuvnu pohranu podataka određenih dokumenata, sistema… ali ti pričuvni podatci nisu ispravni odnosno pohrana pričuvnih podataka se izvrši ali iz određenih razlog povrat podataka nije moguće uspješno izvršiti zato se preporučuje raditi provjeru pričuvnih podataka. Ukoliko pričuvna pohrana nije ispravna potrebno je provjeriti gdje se događa greška, ukloniti grešku, pokrenuti ponovno kopiranje pričuvnih podataka i nakon toga testirati dali je sve u redu. Problemi zbog koji se ne mogu vratiti pričuvni podatci znaju biti ako određeni dokument iznosi više od 256 znakova, medij sa kojeg korisnik vraća podatke može biti oštećen…

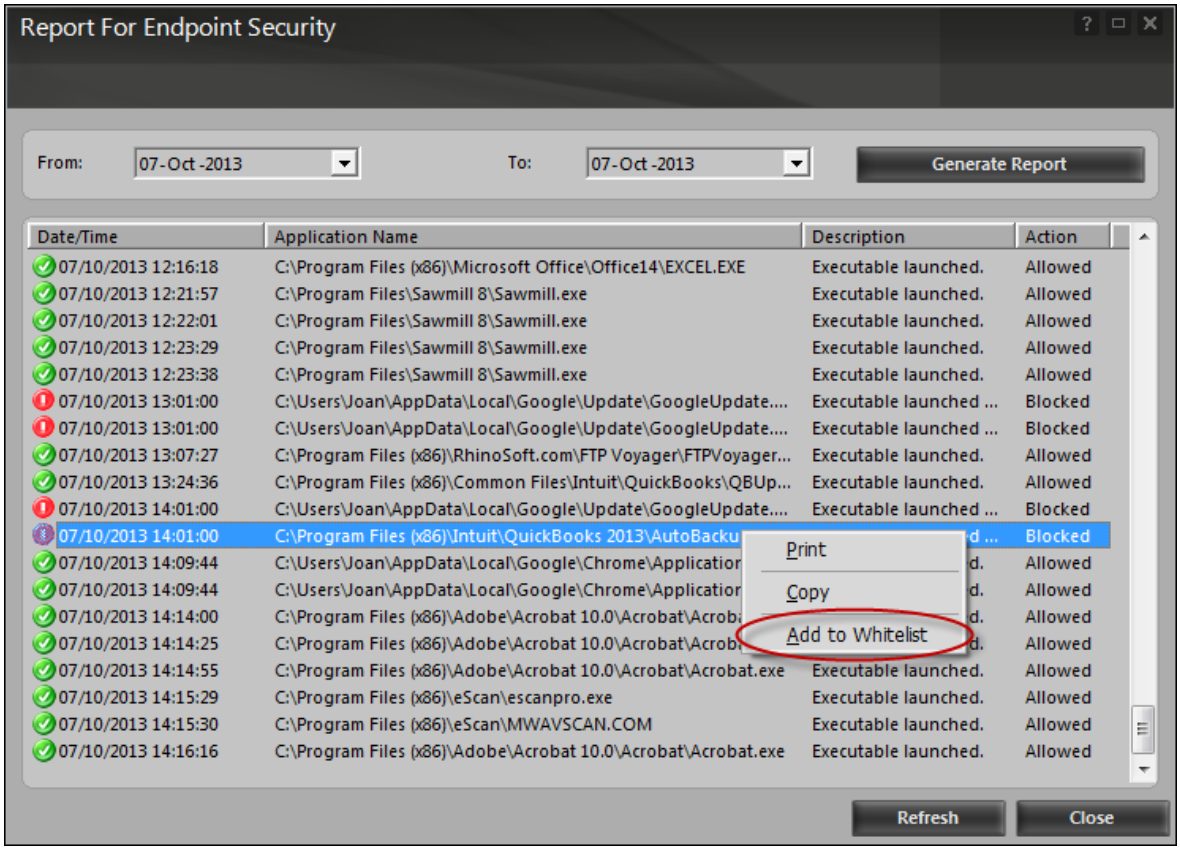
## 4.5. Popis dopuštenih aplikacija

Popis dopuštenih aplikacija (engl. Application whitelisting) ako je ispravno implementiran može biti od velike pomoći u sigurnosti, stabilnosti i konzistentnosti u računalnom okruženju. Nažalost ovaj način zaštite je jako često krivo shvaćen ili je loše implementiran pri čemu korisnika zavara da je sustav sigurniji nego što je. AWL je tehnologija osmišljena kako bi očuvala sustav od pokretanja neželjenog software-a i malicioznog koda. AWL kontrolira software koji ima dopušteno pokretanje na računalima, a zabranjuje pokretanje

svim ostalim aplikacijama koje nisu navedene u popisu dopuštenih aplikacija. S druge strane postoji sličan način zaštite, a on se zove popis blokiranih aplikacija (engl. Application blacklisting). ABL radi po principu da blokira sve aplikacije koje se nalaze na zabranjenoj listi, a sve ostale aplikacije ili ekstenzije propušta. AWL radi kao vatrozid odnosno u samom početku blokira sve aplikacije ili ekstenzije ,a korisnik bira što želi propustiti. Sa sigurnosnog aspekta AWL se smatra sigurnijim baš zato što će spriječiti bilo koju aplikaciju koja nije na listi, a to može biti i napad koji koristi „nulti dan“ (engl. *Zero day*) exploit, dok će ABL takve exploit-e propustiti i napad će se moći izvršiti.

### 4.5.1. Mogući izazovi

Izazov za implementaciju AWL za jedan sustav i korisnika su što u samom startu treba saznati sve ekstenzije koje dopuštene aplikacije koriste. Prilikom ažuriranja određene aplikacije mogu dobiti novu ekstenziju ili dodatne mogućnosti koje također treba propustiti. Slika 4.3 prikazuje kako izgleda izvješće u Escan okolini gdje je podešen popis dopuštenih aplikacija, te kako propustiti određenu ekstenziju.




Slika 4.3 Escan izvješće

## 4.6. Edukacija korisnika

Većina problema polazi od krajnjeg korisnika odnosno od njegovog ne znanja. Od samog ne znanja rada za računalom pa do ne znanja za surfanjem na internetu što klijent smije otvarati što ne smije kakve se sve prijetnje nalaze na internetu i kakve sve prijetnje mogu dobiti putem mail-a. Kako bi se umanjili takvi problemi potrebno je educirati ljude objasniti kakve prijetnje postoje putem mail-a, društvenih mreža, interneta… Potrebno je objasniti da svoje pristupne podatke ne smiju nikome davat i da trebaju takve stvari shvatiti jednako kao i podatke o bankovnim karticama i osobnoj kartici. Zbog samo jednog trenutka ne pažnje i ne znanja napadač može doći do svih podataka korisnika i podataka organizacije za koju korisnik radi.

## 4.7. Onemogućavanje SMB 1.0 protokola

SMB Protokol je protokol kreiran 1980. godine koji se koristi za komunikaciju klijent-poslužitelj. Ovaj protokol omogućuje aplikaciji ili klijentu da pristupi dokumentima, printerima i nekim drugim resursima na mreži. 2006. godine je predstavljena verzija SMB 2.0 s izlaskom Windows Viste. Izlaskom Windows 8 i server 2012 izlazi i novija verzija SMB 3.0. Danas nakon što je prošlo više od 30 godina od kako je kreiran SMB protokol i kako je izašlo nekoliko novijih verzija pojedine kompanije i dalje koriste zastarjelu 1.0 verziju. U tom sigurnosnom propustu napadači vide svoju priliku. Većina poznatih Ransomware-a se oslanja na sigurnosne propuste koje ima verzija 1.0 i iz tog razloga se preporučuje onemogućavanje verzije 1.0 i prelazak na noviju. Korisnik može provjeriti dali je SMBv1 omogućen putem PowerShell-a sa linijskom naredbom Get-WindowsOptionalFeature –Online –FeatureName SMB1Protocol. Ako je protokol onemogućen pisat će „State : Disabled“ u protivnom će pisati „State : Enabled“. Onemogućavanje verzije 1.0 moguće je putem pravilnika grupe, PowerShell-a, upravitelja poslužitelja… Onemogućavanje SMBv1 putem pravilnika grupe moguće je napraviti na slijedeći način: U konzoli za upravljanjem pravilnikom grupe potrebno je kreirati novu stavku registra na putanji „konfiguracija računala\preference\postavke sustava Windows\ registar“ sa slijedećim svojstvima registra

- Akcija: Create
- Košnica: HKEY_LOCAL_MACHINE

- Put ključa: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
- Naziv vrijednosti: SMB1
- Vrsta vrijednosti: REG_DWORD
- Vrijednost podatka: 0

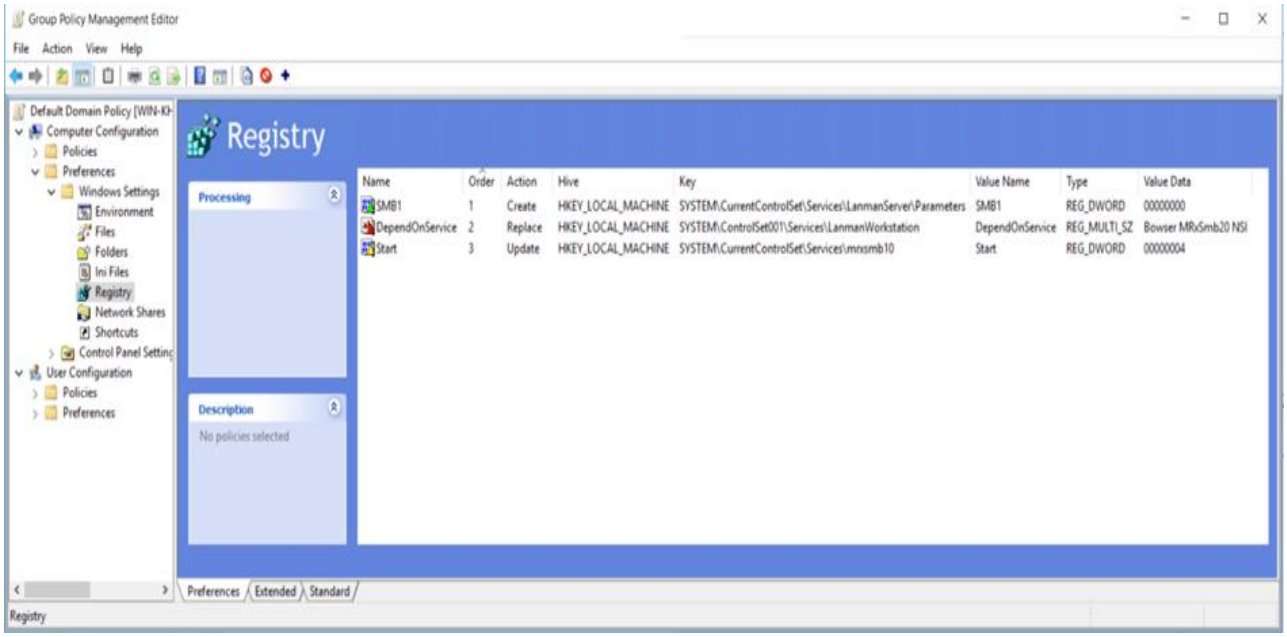
Kada je prvi registar gotov potrebno je ponoviti proceduru sa slijedećim svojstvima registra:

- Akcija: Update
- Košnica: HKEY_LOCAL_MACHINE
- Put ključa: SYSTEM\CurrentControlSet\services\mrxsmb10
- Naziv vrijednosti: Start
- Vrsta vrijednosti: REG_DWORD
- Vrijednost podatka: 4

Kada je drugi registar gotov potrebno je ponoviti proceduru sa slijedećim svojstvima registra:

- Akcija: Replace
- Košnica: HKEY_LOCAL_MACHINE
- Put ključa: SYSTEM\CurrentControlSet\Services\LanmanWorkstation
- Naziv vrijednosti: DependOnService
- Vrsta vrijednosti: REG_MULTI_SZ
- Podaci o vrijednosti:
    - Bowser
    - MRxSmb20
    - NSI

Slika 4.4Slika 4.4 GP **Pogreška! Izvor reference nije pronađen.** prikazuje kako izgleda pravilnik grupe nakon dodavanja novih stavaka registra.




Slika 4.4 GP Management Editor

### 4.7.1. Mogući izazovi

Kao najveći problem zašto kompanije ne mogu prijeći na noviju verziju je taj što koriste aplikaciju koja komunicira koristeći SMB 1.0 protokol i jednostavno ne smiju onemogućiti tu opciju.

## 4.8. Multi faktorska autentikacija

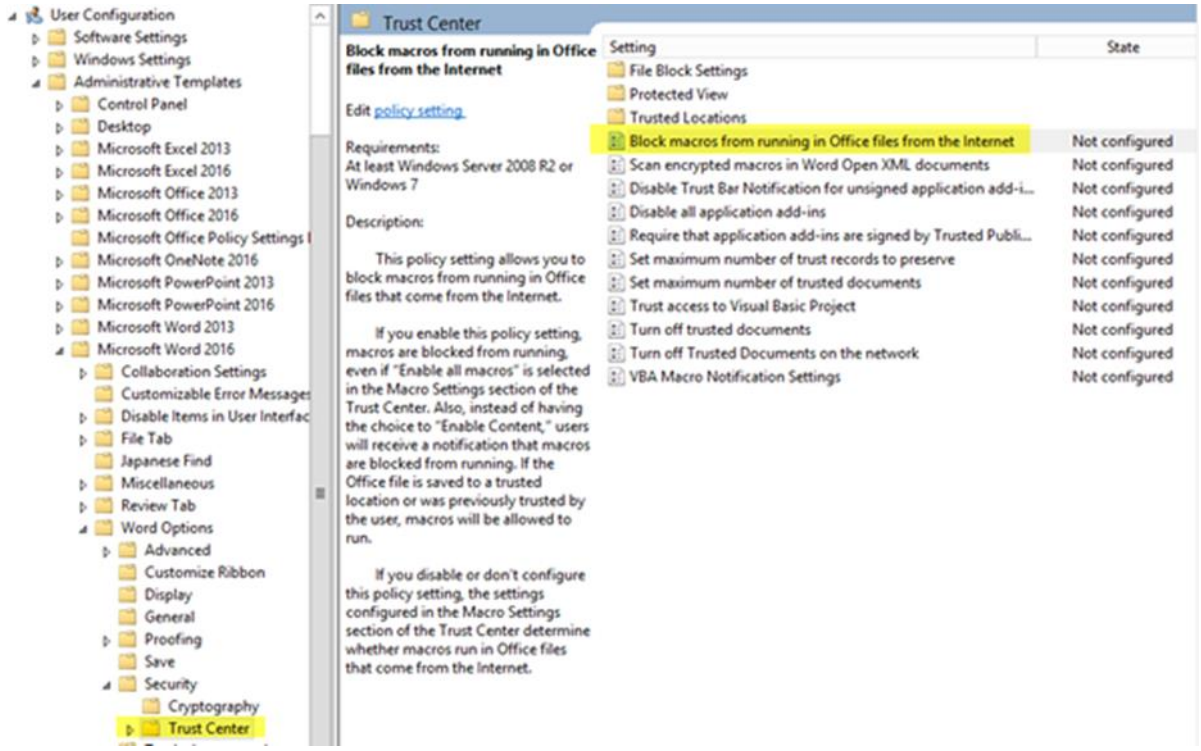
MFA je metoda utvrđivanja identiteta korisnika koji se želi prijaviti na sustav pomoću dva ili više različitih dokaza, a ona se može sastojati od više faktora:

- Nešto što samo korisnik zna (pin, lozinka..),
- Nešto što samo korisnik ima (broj mobitela, osobna..)
- Nešto što korisnik je (otisak prsta…).

Ovakav način prijavljivanja u sustav postavlja sigurnost na visoku razinu. U slučaju da napadač na neki način dođe u posjed administrator vjerodajnicama, njegov napad se neće moći izvršiti u potpunosti jer mu nedostaje drugi faktor autentikacije. Da bi napadač došao do drugih faktora autentikacije mora se infiltrirati u njegov mobitel ili imati njegov otisak prsta ili njegovu osobnu… ovisno koji drugi način autentikacije je administrator odabrao.

## 4.9. Ograničavanje korištenja makro naredbi

Skrivanje malicioznih kodova unutar Microsoft Office makroa postao je popularan način kriminalcima kako pokrenuti njihov napad. Makroi su mali programi ugrađeni u drugi program kako bi automatski ponavljali određene zadatke, npr. Korisnik može napraviti makro u Excel tablici koja će mu automatski povući podatke s vanjske baze. Ako su makroi dopušteni, prilikom otvaranja dokumenta skripta se pokreće automatski što predstavlja sigurnosni propust. Svoju priliku ovdje vide kibernetički kriminalci i unutar makroa ubacuju svoju skriptu ili program. Zaštita od ovakvog propusta je: Stavljanjem na AWL samo one makroe koji imaju digitalni potpis, onemogućavanje makroa putem GP. Slika 4.5 prikazuje kako blokirati makroe na računalima putem GP.




Slika 4.5 Blokiranje makroa putem GP[15]

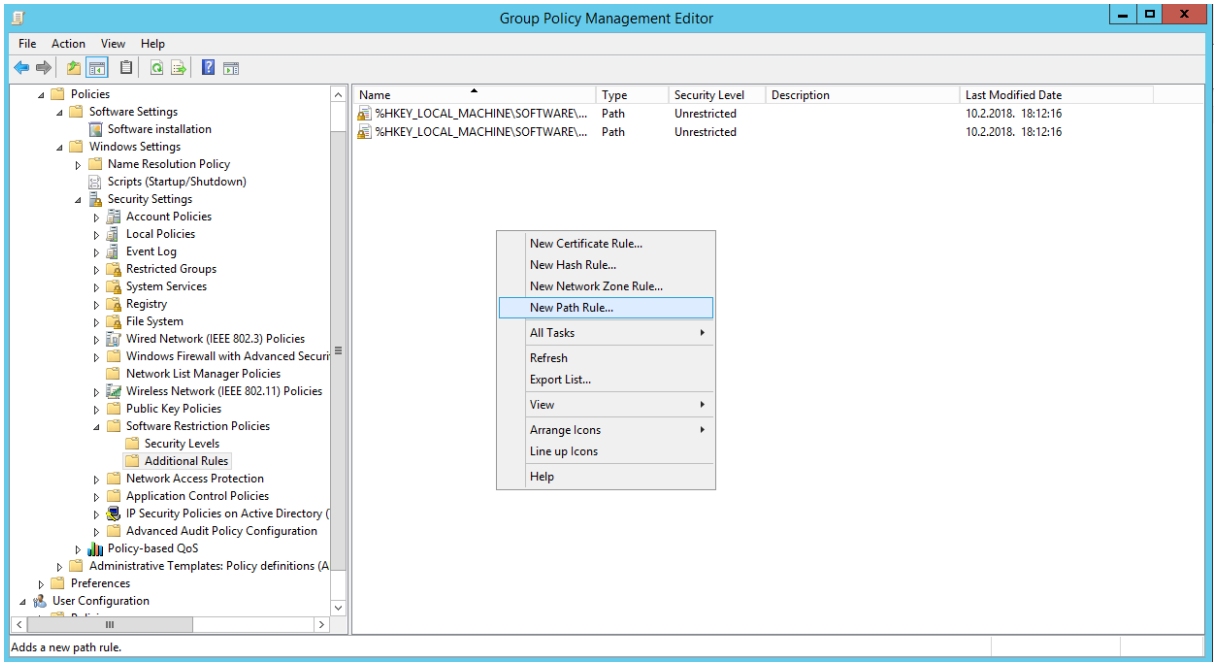
[15] http://www.thewindowsclub.com/block-macro-malware-microsoft-office, 2018

## 4.10. Ažuriranje aplikacija

Nakon deset godina istraživanja, znanstvenici su otkrili da su sigurnosni propusti u Adobe i Java programima odgovorni za iskorištavanje 66 posto svih sigurnosnih rupa u Windows sustavu. Proizvođači za programe izdaju zakrpe što je brže moguće, no njihov trud neće biti od pomoći ako korisnici ne ažuriraju svoje programe s najnovijim nadogradnjama. U izvješću se navodi da preglednici sudjeluju u najvećem broju zlonamjernog iskorištavanja. Web stranice mogu uputiti upit preglednicima za bilo koju informaciju, kao što su informacije o točnoj verziji preglednika, operativnog sustava, Flash i Java dodataka. Svrha ovog mehanizma je generiranje stranice koja će korisniku pružiti najbolje korisničko iskustvo. Međutim, taj mehanizam može biti zlouporabljen od strane zlonamjernih web stranica čiji se napadi temelje na povratnim informacijama koje šalju preglednici. Neki od napada idu kroz ranjive dijelove preglednika, ali još veći broj napada odvija se putem propusta u obradi pojedinih tipova datoteka. Prema izvješću, za prijenos malicioznog koda na računala putem propusta najviše se koristi PDF format datoteka. Posljednjih godina povećana je svjesnost IT sigurnosti među korisnicima i kompanija  no i dalje najveću sigurnosnu prijetnju predstavljaju aplikacije. U 2015. godini web aplikacije koje su testirane u prosjeku su imali četiri ranjivosti. 2016. godine ranjivost se smanjuje za 25% oko tri ranjivosti. To je i dalje visoka ranjivost pogotovo zato što je polovica tih ranjivosti kritična. Nakon ovakvih statistika vidljivo je da su ažuriranje i nadogradnja aplikacija jednako važni kao i ažuriranje OS. Za aplikacije koje više ne postoji podrška nije preporučljivo koristiti te ih je potrebno zamijeniti novijim verzijama.

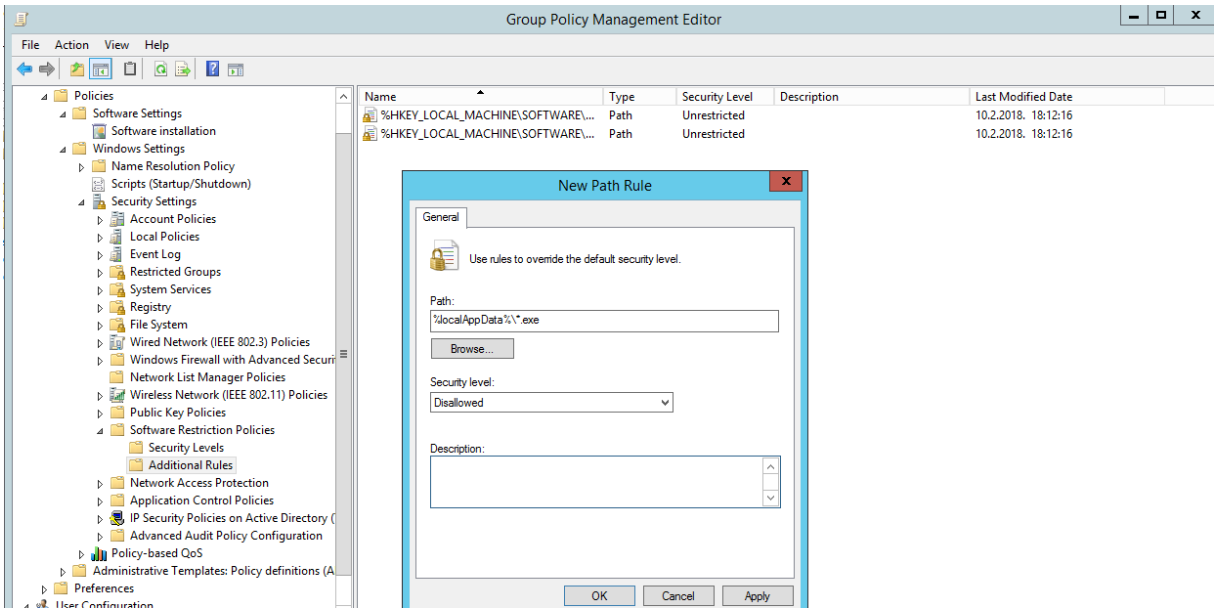
## 4.11. Onemogućavanje pokretanje programa

Mape iz kojih se pokreću maliciozni kodovi su Appdata, Preuzimanja, Radne površine… Jedan od besplatnih načina kojim se Windows okolina može obraniti su postavljanje određenih pravila na GP-u. Korisnik pomoću GP može postaviti dodatnu zaštitu od pokretanja određenih ekstenzija sa određenih mapa. Slika 4.6 Prikazuje kako na GP dodati novo pravilo.



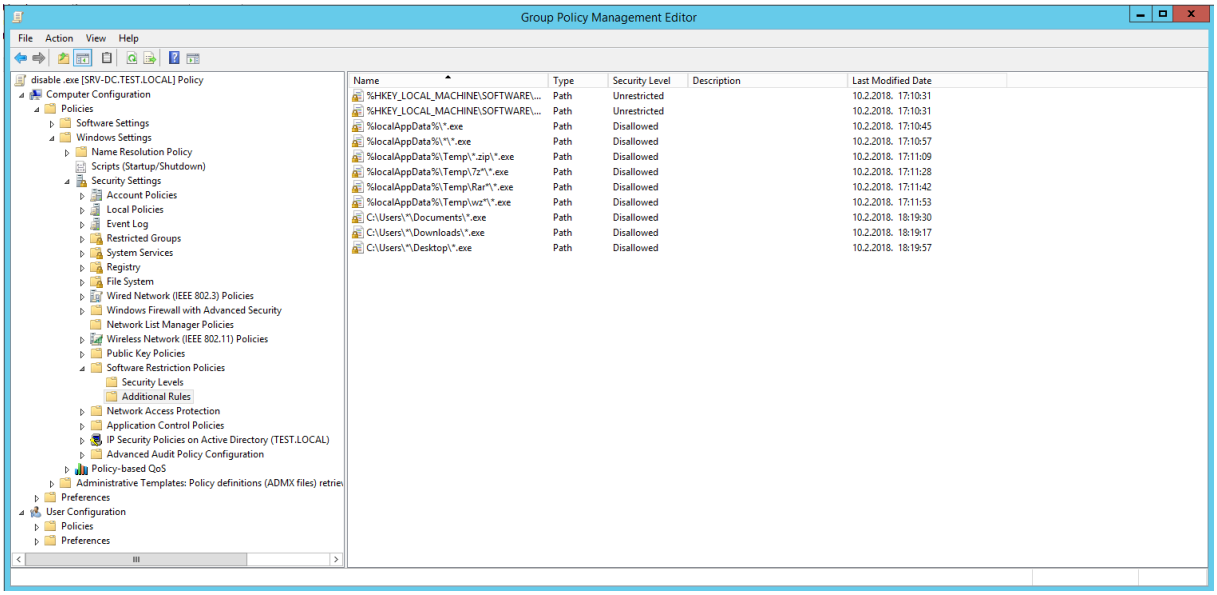

Slika 4.6 Dodavanje novog pravila

Slika 4.7 prikazuje kako dodati putanju novom pravilu i kako ga regulirati




Slika 4.7 Postavljanje putanje novom pravilu

Slika 4.8 Ilustrira kako izgleda nakon dodavanja određenih pravila




Slika 4.8 Prikaz svih postavljenih pravila

## 4.12. Antivirusna rješenja

Antivirusni softver, antivirusni program ili antivirus je računalni softver koji se koristi za zaštitu, identifikaciju i uklanjanje računalnih virusa, kao i drugih štetnih programa koji mogu uzrokovati probleme u korištenju računala ili oštetiti podatke. Postoji nekoliko metoda koje antivirusni program koristi za identifikaciju štetnih programa. Ovisno od programa može se koristiti i više metoda. Detekcija bazirana na uzorcima - najčešće korištena metoda za identifikaciju štetnih programa. Da bi pronašao virus ili neki drugi zlonamjerni program, softver uspoređuje sadržaj datoteka sa sadržajem kataloga uzorka virusa. S obzirom da virus može biti ugniježden u samu datoteku, provjerava se i njezin sadržaj, kao i sadržaj svih njenih sastavnih dijelova, ako se radi o složenoj ili komprimiranoj datoteci. Heuristička metoda - ova metoda se može koristiti kod novih i nepoznatih virusa. Može se koristiti na dva načina: analiza datoteka i emulacija datoteka. Analiza datoteka je proces traganja za sumnjivim programskim zapovijedima u datotekama. Slabost ove metode je to što ona može znatno usporiti računalni sustav provjeravajući veliki broj datoteka. Emulacija datoteka je metoda koja izvršava program u virtualnom okruženju i bilježi sve akcije koje on izvrši. Analizom zabilježenih akcija može se utvrditi može li program ugroziti računalni sustav.[16]

[16] https://hr.wikipedia.org/wiki/Antivirusni_program, 2018

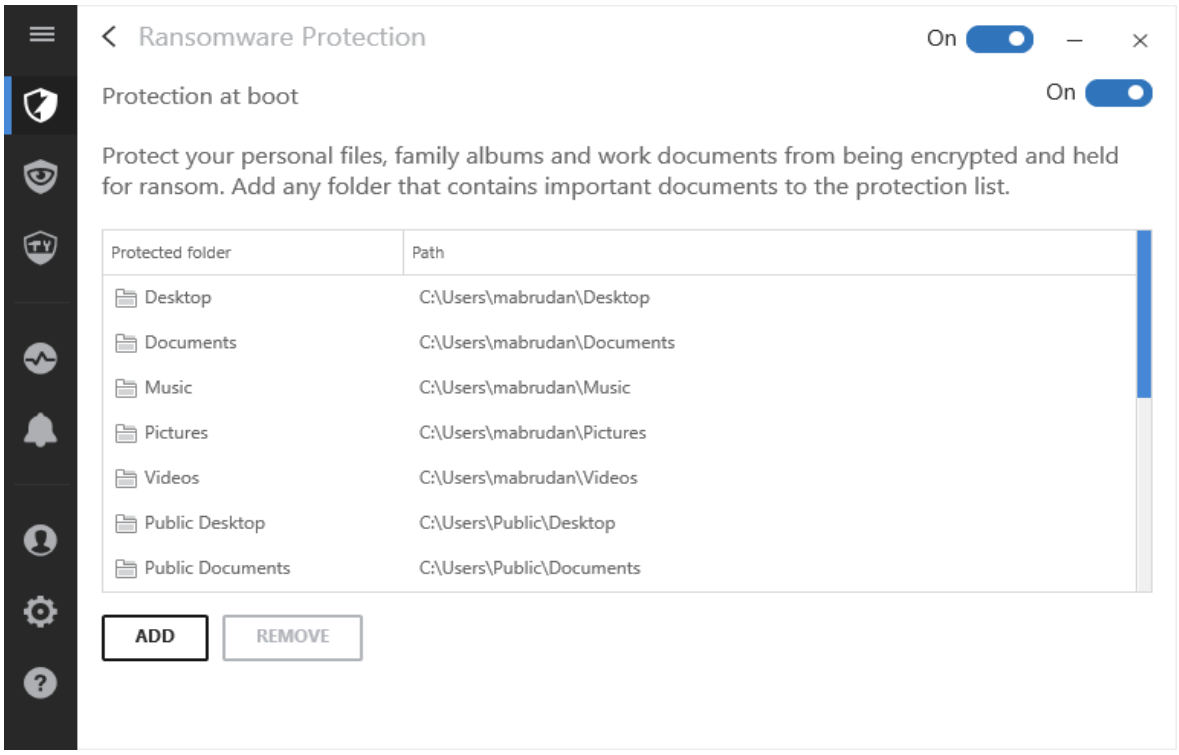
### 4.12.1. Usporedba načina zaštite 3 top AV rješenja

Za usporedbu prikazati će se tri najbolja Business Windows antivirusna rješenja iz prosinca 2017. godine prema AV-TEST nezavisnom IT sigurnosnom institutu koji provodi ovakva istraživanja zadnjih petnaest godina. Pri odabiru najboljeg antivirusa institut je radio testove u tri kategorije, a to su: zaštita, performanse i iskoristivost gdje su u svakoj kategoriji morali zadovoljiti s nekoliko različitih kriterija. Konvencionalni proizvođači AV programa oslanjaju se na metode zaštite poput anti-maliciozni potpis (engl. anti-malware signature) i katalog uzorka virusa (engl. code fingerprint), no s obzirom da se svaki dan proizvede oko 400.000 novih malicioznih kodova/Ransomware-a, ove metode nisu dovoljno učinkovite u borbi protiv tolikih izazova. U daljnjoj usporedbi prikazat će se način zaštite sustava koju koriste top tri anti virusna rješenja i mogu li se današnja anti virusna rješenja nositi s današnjim izazovima. Sva niže navedena AV rješenja se temelje na nekim dinamičkim analizama ponašanja pokrenutih procesa gdje se po određenim algoritmima zaključuje dali je proces maliciozan i terminira se. Krajnji uređaji (engl. Endpoint) mogu se povezati sa pješčanikom (engl. sandbox appliance), na način da mu šalju nepoznate datoteke na analizu i dobivaju povratnu informaciju, jednom kad pješčanik otkrije maliciozni kod u datoteci, šalje instant poruku svim krajnjim uređajima koji automatski brišu dokument ili ga blokiraju na neki drugi način. Pješčanik (engl. sandbox appliance) je izolirano i sigurno okruženje koje oponaša cijeli računalni sustav. U pješčaniku se pokreću sumnjivi programi kako bi se pratilo njihovo ponašanje i kako bi se shvatile njihove namjere. Kada je program u pješčaniku on nikako ne može ugroziti sustav organizacije.

#### 4.12.1.1 Bitdefender Endpoint Security 6.2

Ovaj antivirus u borbi protiv Ransomware-a i ostalih malicioznih kodova koristi nekoliko metoda jedan od njih su: strojno učenje (engl. machine learning) – metoda koja pomoću algoritma strojnog učenja na temelju iskustva i analiziranju miliona malicioznih kodova predviđa i uvježbava se kako bi otkrio nove ili nepoznate prijetnje koje imaju sličnosti sa već poznatim prijetnjama. Kada god se pojavi sumnjiv uzorak na krajnjem računalu on se šalje na Bitdefender-ov oblak pri čemu se on automatski analizira. Ukoliko je pronađen Ransomware dodjeljuje mu se potpis i objavljuje se za manje od 30 minuta. Nakon što je objavljen potpis propagacija putem ažuriranja na sva krajnja računala bi trebala biti oko 3 sata. Ako je kod pokrenut unutar perioda kad se obavlja ažuriranje on će biti blokiran i neće

se moći pokrenuti. Jedan od načina zaštite protiv Ransomware-a je Ransomware Protection koji omogućuje promjenu podataka samo aplikacijama koje imaju digitalni potpis, sve ostale aplikacije koje nemaju digitalni potpis bit će postavljeni kao blokirane aplikacije, ako korisnik vjeruje određenoj aplikaciji on ju može postaviti u „Trusted applications“ listu. Po zadanim postavkama zaštićene mape su Radna površina, Dokumenti, Muzika, Slike, Video, Oblak mape. Slika 4.9 Prikazuje kako izgleda Ransomware zaštita kod Bitdefendera i kako novi dokument.



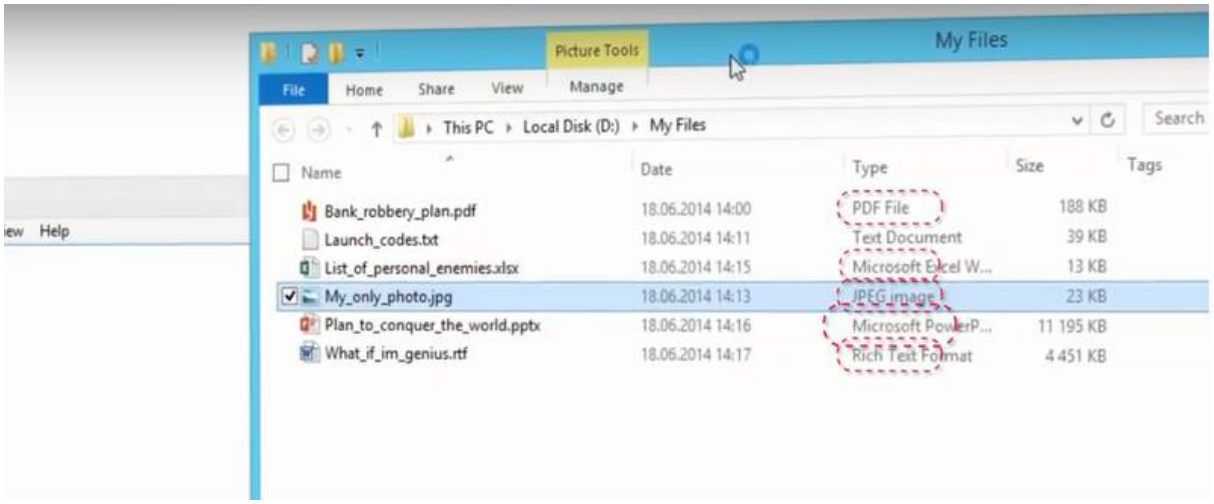

Slika 4.9 Bitdefender Ransomware Protection[17]

#### 4.12.1.2 Kaspersky Lab Endpoint Security 10.3

Kaspersky omogućuje opciju poput povrat podataka nakon kriptiranja istih bez dozvole korisnika. Kada Kaspersky uoči nekakvu stranu aktivnost nad privatnim dokumentima, podacima poput izmjene ili enkripcije on automatski napravi svježu kopiju svih podataka. Maliciozni kod odradi svoj „posao“ kriptira podatke, a Kaspersky nakon toga briše taj maliciozni kod i vraća podatke iz backup-a koje je napravio prije nego što je započela

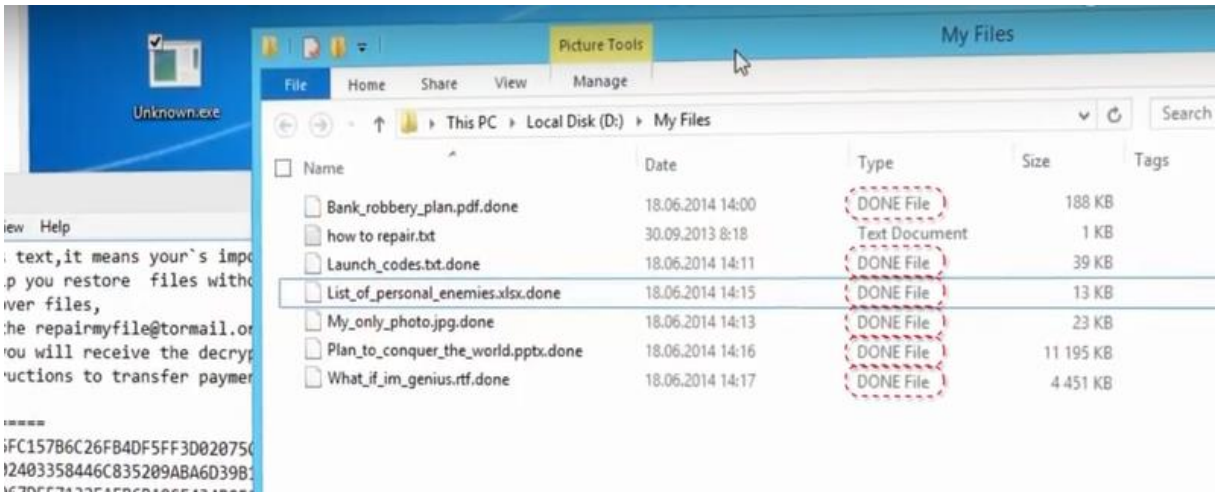
[17] https://www.bitdefender.com/support/how-Ransomware-protection-works-in-bitdefender-2017-1733.html, 2018

enkripcija. Slika 4.10 Prikazuje kako dokumenti izgledaju dok nisu kriptirani i koje su ekstenzije.



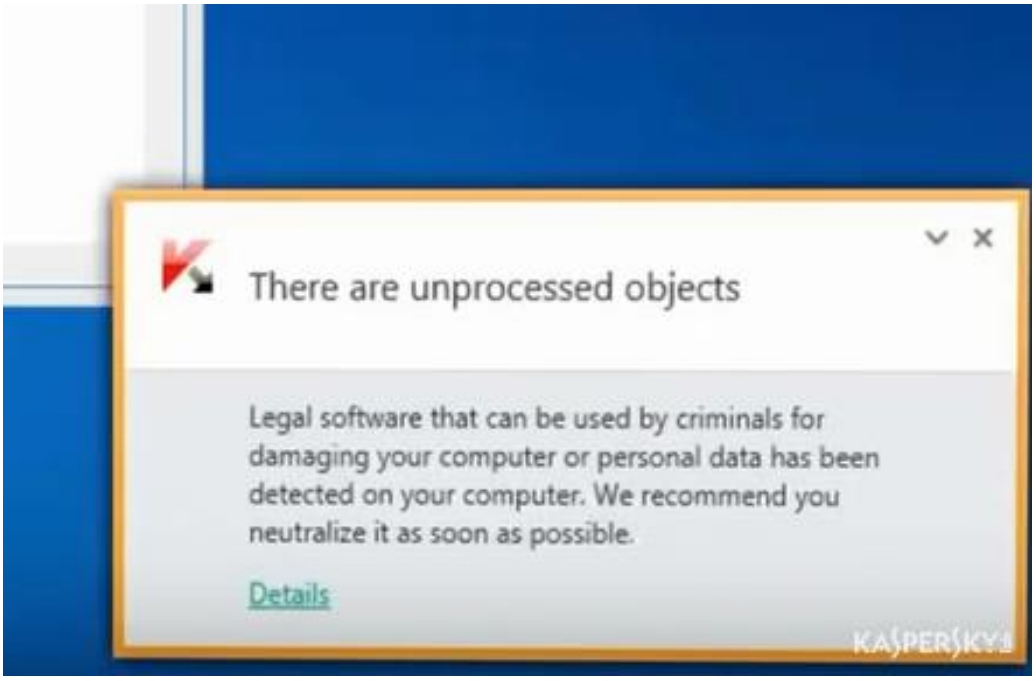

Slika 4.10 Prikaz ne kriptiranih dokumenata

Slika 4.11 prikazuje kako dokumenti izgledaju nakon zaraze Ransomware-a, te kako izgledaju njihove ekstenzije

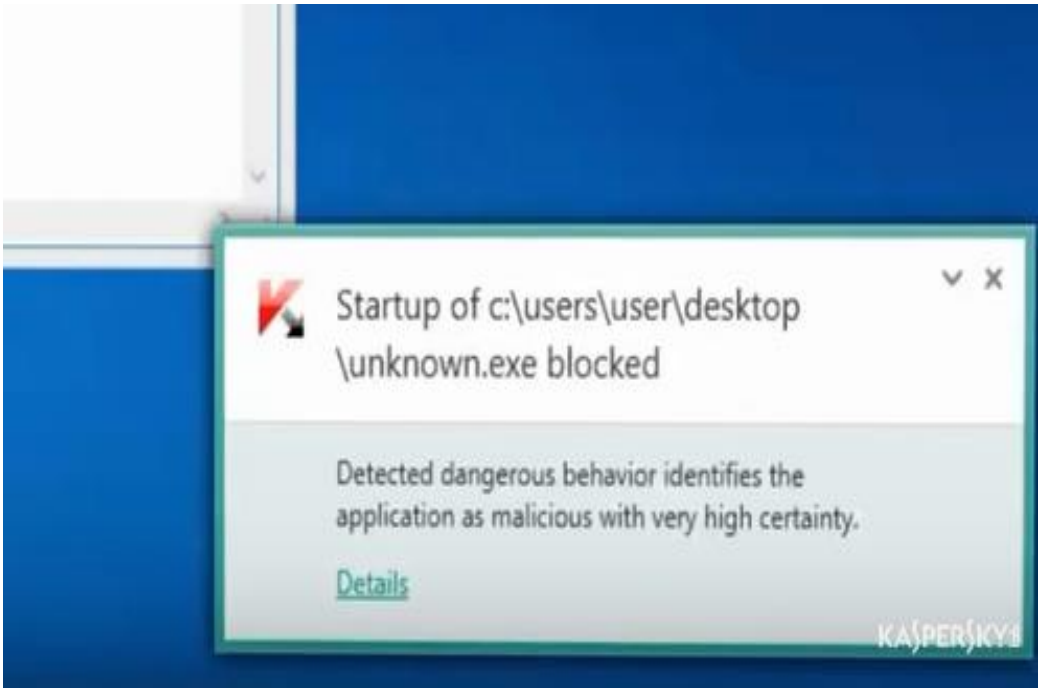



Slika 4.11 Prikaz kriptiranih dokumenata

Slika 4.12 i Slika 4.13 Prikazuje reakciju Kaspersky AV nakon enkriptiranja podataka

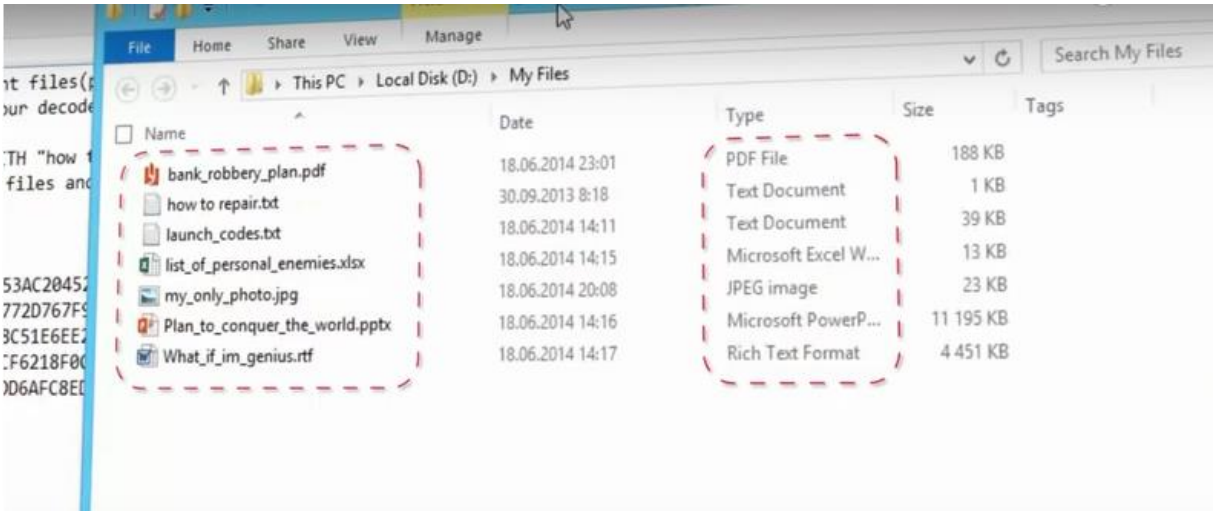



Slika 4.12  Kaspersky intervencija




Slika 4.13 Kaspersky intervencija

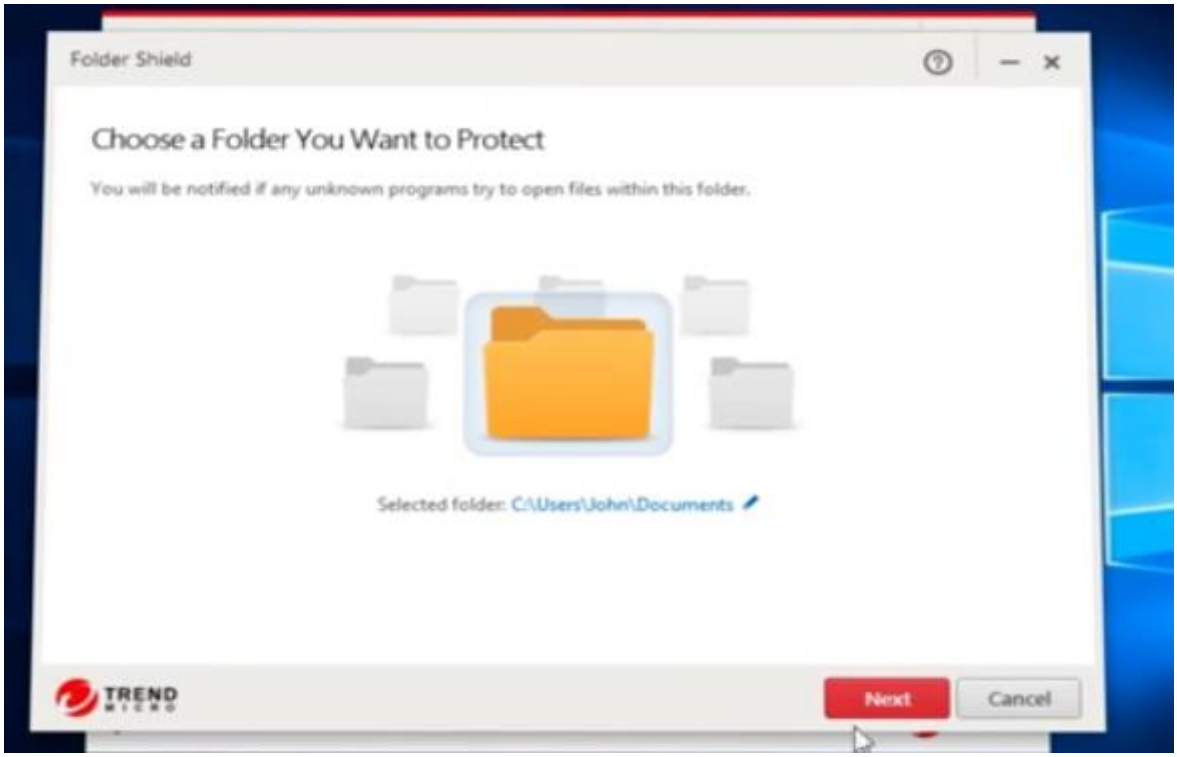
Slika 4.14 prikazuje kako izgledaju dokumenti nakon intervencije Kaspersky AV.




Slika 4.14 Kaspersky intervencija

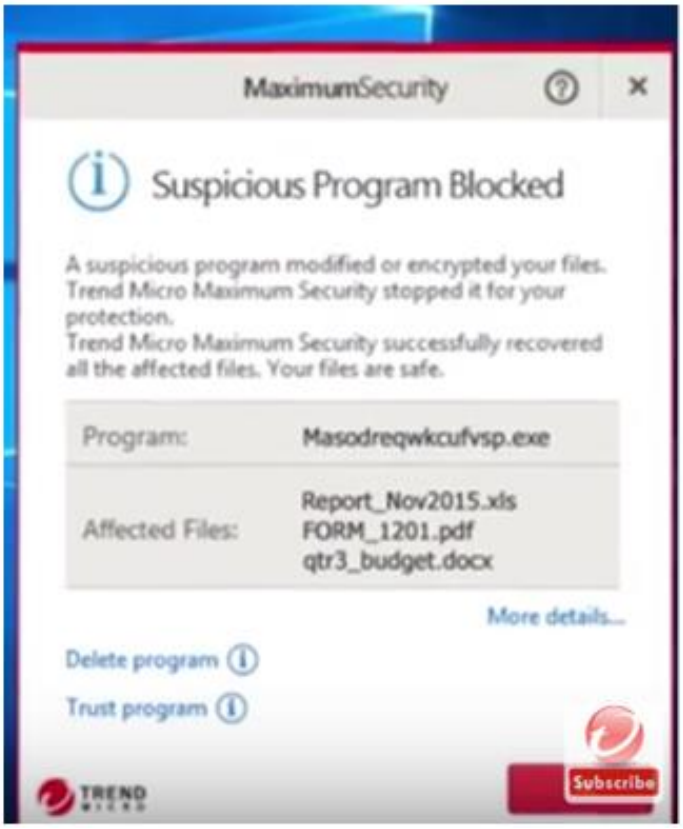
### 4.12.1.3 Trend Micro Office Scan 12.0

Trend Micro nudi rješenja slična kao Bitdefender i Kaspersky. Rješenje slično kao kod Bitdefendera zove se Folder Shield koje štiti dokumente od neautoriziranih pristupa i mijenjanja od strane Ransomware-a i ostalih malicioznih kodova ovu opciju korisnik sam treba uključiti i onda može birati koje sve podatke želi da mu Trend Micro štiti. Slika 4.15 prikazuje kako izgleda Folder Shield zaštita dokumenata koju nudi Trend Micro



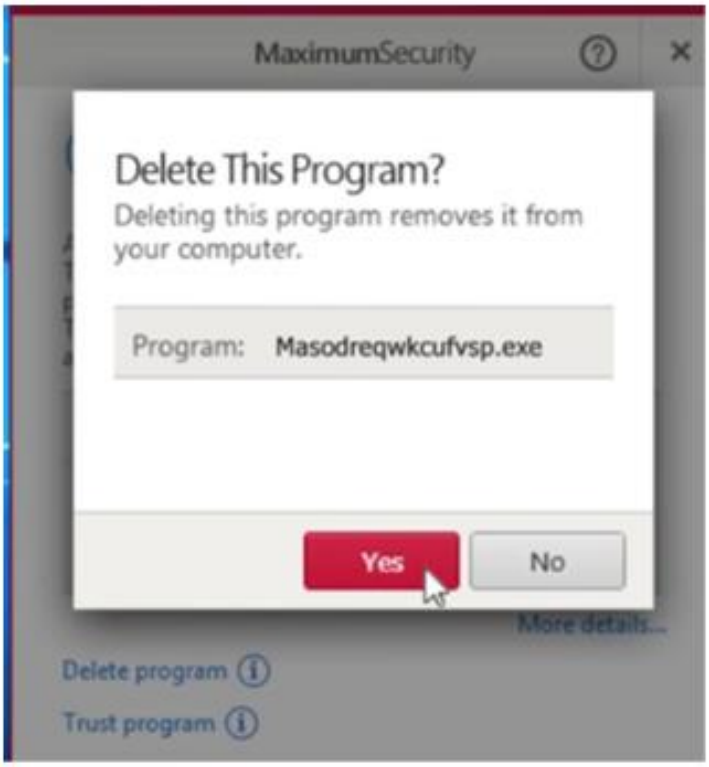

Slika 4.15 Trend Micro Folder Shield

Drugo rješenje koje je slično Kaspersky-om je kada Trend Micro otkrije neuobičajenu aktivnost nad dokumentima poput kriptiranja započinje pričuvna pohrana istih dokumenata. Nakon toga zaustavlja program koji obavlja enkripciju, podatci se vračaju na stanje i mjesto prije nego što je Ransomware utjecao na njega. Kada je procedura gotova korisnik može obrisati maliciozni program kroz Trend Micro prozor koji iskoči kada se pojavi maliciozna radnja. Nakon brisanja programa Trend Micro preporučuje ponovno pokretanje računala. Slika 4.16 prikazuje izvješće o blokiranju koje se pojavi u desnom kutu računala kada primijeti sumnjivu radnju nekog programa




Slika 4.16 Trend Micro intervencija

Slika 4.17 prikazuje što korisnik može učiniti s određenim programom. Ova opcija brisanja ili ne brisanja postoji zato što ponekad korisnik treba nekakvu aplikaciju koja radi na sličan način, ali zbog loše napisanog programa AV takav program smatra prijetnjom.




Slika 4.17 Trend Micro intervencija

# Zaključak

Danas je napadaču potrebno jako malo znanja kako bi se infiltrirao u informacijski sustav i zarazio ga svojim kodom. Dovoljno je primjerice slijediti instrukcije s Youtube-a te na taj način počiniti veliku štetu na informacijskom sustavu. S druge strane da bi administrator zaštitio svoj sustav mora znati kakve prijetnje sve postoje, koje sigurnosne propuste njegov sustav ima. Navedeno zahtijeva veću razinu znanja i resursa.

Najveći razlog postojanja Ransomware-a je taj što uvijek postoji neka žrtva koja će platiti određenu količinu novaca samo da vrati svoje slabo štićene podatke. Kao što je već spomenuto u radu oko 70% poslovnih korisnika bi platilo Ransomware otkupninu samo kako bi došli do svojih kritičnih podataka. Ti rezultati jasno ukazuju da se napadi neće smanjiti.

U ovom radu su prikazane jasne sigurnosne kontrole koje mogu biti primijenjene u svakoj organizaciji. Pojasniti ćemo navedeno na primjeru jedne organizacije sa oko tristo klijentskih računala i dvadesetak servera. Početkom 2016. godine većina navedenih sigurnosnih pravila i politika spomenutih u ovom radu je uvedena u produkcijsku okolinu. Do implementacije sigurnosnih politika i pravila organizacija je imala u prosjeku jednom mjesečno kriptiran sustav. Od implementacije do pisanja ovoga rada rezultat kriptiranih podataka od strane Ransomware-a iznosio je nula. Da bi se takav rezultat postigao bilo je potrebno uložiti jako puno vremena u otkrivanju sigurnosnih propusta, implementaciji sigurnosnih rješenja i edukaciji  korisnika računala.

Ažuriranje sustava i aplikacija je informatička higijena koju bi svaki administrator sustava morao koristiti.

Svaki IT sustav mora imati pričuvnu pohranu podataka. Dovoljno je samo napomenuti kako postoje dvije vrste administratora, oni koji rade pričuvnu pohranu podataka i oni koji će tek raditi pričuvnu pohranu podataka.

Anti virusna zaštita detektira u prosjeku oko 99,5 – 99,9 % malicioznih kodova. Na uzorku od 250,000 malicioznih kodova koliko se naprave svaki dan, neće biti detektirano oko 250 – 1250 malicioznih kodova. Anti virusna rješenja pomažu u zaštiti protiv Ransomware-a, ali to ne smije biti jedina zaštita. Odabirom bilo kojeg top proizvoda kojeg je navela organizacija AV-TEST korisnik ne može pogriješiti, jer su razlike između njih minorne.

Najučinkovitija kontrola koja se može primijeniti je popis dopuštenih aplikacija. Sa ovom kontrolom administrator ima potpuni nadzor nad aplikacijama koja se nalaze na krajnjim računalima. Nedostatak ove kontrole što ona tijekom implementacije zahtjeva jako puno vremena. Da bi se takva kontrola ispravno implementirala administrator mora provjeriti svaku dopuštenu ekstenziju, dali je sigurna i što ju pokreće. Kada se implementira ova kontrola njeno održavanje je jednostavno, brzo i učinkovito.

Sustav je moguće zaštiti od napada Ransomware-a, ali za to je potreban stalan angažman administratora kako u kontinuiranom educiranju o novim sigurnosnim propustima i novim sigurnosnim zaštitama, tako i u administriranju sustava.

# Popis kratica

ABE Access-Based Enumeration

ABL Access Black List

AD Active Directory

AV Anti Virus

AWL Access White List

CHKDSK Check Disk

DHCP Dynamic Host Configuration Protocol

GP Group Policy

HTTP HyperText Transfer Protocol

ICT Information and Communication Technology

IOS Iphone Operatins System

IOT Internet Of Things

IT Information Technology

MFA Multi Factor Authentication

OS Operatins System

RDP Remote Desktop Protocol

SMB Server Message Block

TOR The Onion Router

WMI Windows Management Instrumentation

WMIC Windows Management Instrumentation Command-line

# Popis slika

# Literatura


[1] Allan Liska and Timothy Gallo Ransomware. Defending Against Digital Extortion, studeni 2016.

[2] https://support.microsoft.com/hr-hr/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and, veljača 2018

[3] https://blog.barkly.com/largest-Ransomware-demand-paid-1-million, siječanj 2018

[4] http://www.cert.hr/Ransomware, siječanj 2018

[5] https://www.veeam.com/blog/tips-to-prevent-Ransomware-protect-backup-storage.html, veljača 2018

[6] https://www.av-test.org/en/antivirus/business-windows-client/windows-10/, siječanj 2018

[7] https://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-Ransomware-including-cryptolocker/, siječanj 2018

[8] https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm, siječanj 2018

[9] https://www.av-test.org/en/news/news-single-view/adobe-java-make-windows-insecure/, siječanj 2018

# Prilog

Algebra
visoka škola za
primijenjeno računarstvo

# ZAŠTITA INFORMACIJSKOG SUSTAVA OD RANSOMWARE NAPADA

Pristupnik: Žarko Vujanić, 0321004730

Mentor: Mr.Sc. Dražen Pranić