Zlonameran softver

Sigurnost i bezbednost

Fakultet tehničkih Nauka, Univerzitet u Novom Sadu

Imre Lendak, 2024

Sadržaj današnjeg predavanja

- Osnovne definicije
- Osnovni tipovi
- Složen malver
- Malver u primeni
- Anti-malver rešenja

Malware

- Zlonameran softver (ili malver) → Sam softver nema zlu nameru, već njegovi autori
  - Engleski: malware = malicious software
  - Programski kod ciljano pisan za neki vid napada na računarske sisteme i mreže
- Razni sajber kriminalci koriste malver za krađu sledećih tipova informacija
  - Lični podaci
  - Finansijski podaci
  - Intelektualno vlasništvo
- Posledice uspešnih napada malverom
  - Složeniji napadi na osnovu ukradenih informacija
  - Generisanje ilegalnih prihoda
  - Sajber-špijunaža (*cyber espionage*)

slozeniji napad kasnije

Najčešći mehanizmi zaraze

- Direktno sa Interneta
  1. Zlonameran Web sadržaj (npr. stranica) iskoristi slabost nekog instaliranog programa, npr. Acrobat Reader, Internet Explorer
  2. Stekne pravo izvršavanja i/ili instalacije
  3. Skine i instalira primerak *malware*-a
- Email prilog i URL
  1. *Malware* u prilogu poruke ili URL – pa koraci 2 i 3
- Preko lanca snabdevanja

Napad preko lanaca snabdevanja je kada napadac ne napdada direktno nas, vec napadne neku komponentu ili partnera na koju se oslanjamo i preko toga dolazi do nas, na primer, imamo neki softwer recimo steam, napadac kompromituje njihov server za update, mi preuzimamo update misleci da je legitiman i onda zajedno sa update-om dolazi i zlonameran kod

Pretnje i slabosti

OSNOVNI TIPOVI ZLONAMERNOG SOFTVERA

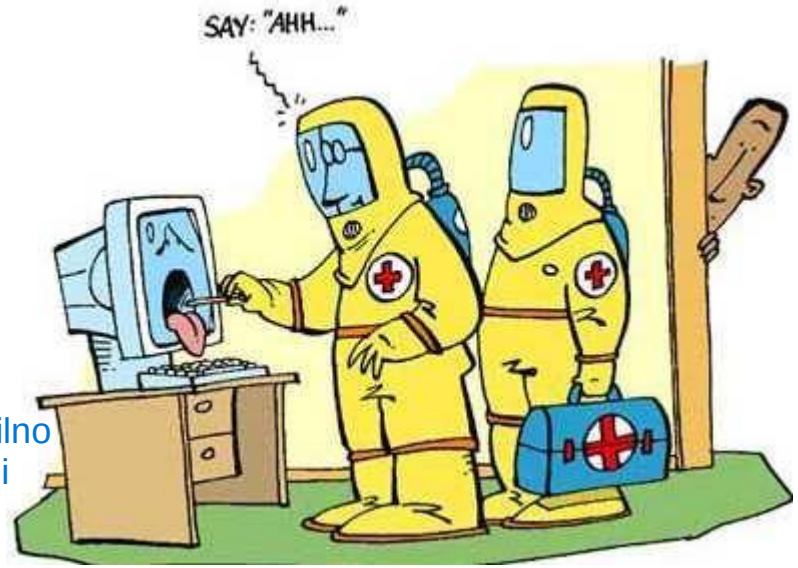
program ili fajl koji radi kako treba mi inficiramo sa virusom tj tim dodatnim kodom i onda on ne radi vise kako treba.
Virus da bi radio mora da zarazi legitimne fajlove, a danas antivirus softveri mnogo bolje brane te fajlove nego pre, takodje vecina modernih operacija je u memoriji a ne na fajl sistemu. Klasicne viruse je lako detetkovati sa modernim malwareom

Virus

Polimorfni virus stalno menja svoj kod da bi se izbegla signature detekcija, kodirani virus je sifrovan, on ne menja svoj kod, njegov cilj je sakrivanje tog malicioznog koda

- Virus modifikuje legitimne datoteke (npr. programe, BIOS, dokumenta) dodavanjem malicioznog izvršnog koda
  - Ime na osnovu bioloških virusa koji inficiraju zdrave subjekte
  - Napomena: virusi se smatraju zastarelim tipom malvera → Zašto?
- Medijum propagacije: (uglavnom) fajlovi
- Rezultat infekcije: uništenje ili koegzistencija
- Tipovi #1: rezidentni i tranzijentni
- Otežana detekcija:
  - Polimorfni modifikuje svoj kod
  - Kodirani virus kodira svoj kod
- Motivacija: narušavanje dostupnosti

rezidentni se stalno zadrzava u RAM-u cak i ako je originalni zarazeni fajl zatvoren, tranzijentni ostaje u memoriji samo dok traje rad zarazenog fajla



Cilj virusa je cesto brisanje fajlova, kvar, smetnja, to nije profitabiilno danasnji malware je fokusiran na novac, napadaci traze kontrolu i dugotrajni pristup, a ne da odmah budu otkriveni

Crv je samostalni malware koji se siri sam od sebe, preko mreze, bez potrebe da se zakaci za fajl ili korisnicku akciju

Crv deluje automatski, ne treba mu pomoc korisnika da se aktivira, on sam nalazi bezbedonosne rupe u OS ili programu.

Crv (worm)

Crv zarazi jedan racunar, onda skenira mrezu u potrazi za drugim racunarima, kada nadje ranjiv sistem onda ga iskoristi i kopira sebe i taj ciklus se ponavlja

- **DEF:** Crv je samostalan (stand-alone) izvršni program koji se autonomno se širi sa jednog računara na drugi
- **Medijum širenja:** računarska mreža
- **Metod propagacije:** ranjivost mrežnog servisa (OS ili aplikativni softver)
- **Motivacija:** narušen integritet → inicijalan pristup → CIA

Crv je samostalan fajl, dok virus mora da bude u nekom drugom fajlu, crv se mnogo brze siri od virusa

Narusavanje integriteta znaci menjanje ili ostecivanje podataka, inicijalan pristup je prvi ulazak u sistem kao otvorena vrata za dalji napad, CIA Confidentiality Integrity Availability, crv moze ciljati bilo koji deo CIA u zavisnosti od namere napdaca

Trojanac se pravi da je bezopasan ili koristan dok u pozadini radi nesto maliciozno kao sto je: kradja lozinki, spijuniranje korisnika, instalacija drugog malvera, kreiranje backroora...

Trojanac

Primarni cilj trojanca je najcesce kradja podataka, on ugrozava poverljivost tj Confidentiality, ali sekundarno moze narusiti i integritet i dostupnost ako instalira druge malware-e

- Pretvara se da je legitiman program
- Umesto korisnih aktivnosti izvršava sledeće akcije:
  - Krađa osetljivih informacija (npr. podaci kreditne kartice)
  - Instalacija dodatnog malware-a (npr. backdoor)
- Medijum propagacije: Internet
  - Aktivno: email prilog, klik na naizgled validan URL
  - Pasivno: slabo zaštićen web sadržaj sa linkom na drive-by-download server koji eksploatiše Internet browser slabosti
- Motivacije (CIA ciljevi): (?)

za razliku od crva i virusa trojanac se obicno ne siri sam, korisnik ga sam pokrece misleci da je to neki obican program, crack, igrica, pdf... Zato je socijalan inzenjering kljucan za njegov uspeh

Backdoor je skriveni kanal pristupa racunaru ili sistemu koji omogucava zaobilazenje uobicajenih sigurnosnih mehanizama npr autentifikacije i firewalla.

Backdoor/trapdoor

Backdoor moze biti: namerno ostavljen (od proizvodjaca softwera), ili naknadno ubacen od strane napadaca (cesto pomocu trojanca)

- Omogućava (udaljeni) pristup zaraženom računaru
  - Podatke šalje na udaljeni Command & Control (C&C) server
  - Legitiman korisnik računara nije svestan pristupa
- **Primer:** Back Orifice 2K (BO2K)
  - Praćenje rada na tastaturi
  - Prenos datoteka
  - Modifikacije Registry baze
- **Motiv (CIA ciljevi):** CIA*

Confidentiality, napadac ima tajni pristup sistemu moze da cita fajlove i da prisluskuje.
Integritet, moze da menja konfiguraciju sistema, fajlove, registre, bez znanja korisnika.
Availability, moze da iskljuci servise, uspori sistem, koristi resurse (npr ddos napad)

Logicka bomba je skriveni zlonamerni kod koji je ugradjen u legitiman program ili biblioteku, aktivira se kada se ispune neki logicki uslovi definisani od strane napadaca.

Narusava dostupnost tako sto moze da brise podatke i onesposobljuje servere

Logička bomba

Narusava integritet tako sto menja ili ostecuje fajlove sistema.

Ne ugrozava poverljivost direktno, ona ne pokusava da ukrade podatke, ne salje podatke napolje, ne spijunira korisnika, ali ona moze stvoriti uslove u kojima je kradja podataka laksa ili manje primetna

- **DEF:** Logička bomba je izvršna datoteka ili biblioteka koja sadrži neželjen i za korisnika nepoznat (izvršni) kod ugrađen u inače legitimne aplikacije
  - Aktivira se kada se stvore uslovi predviđeni od strane napadača
  - Rezultat: brisanje podataka → narušena dostupnost
- **Motivacija (CIA ciljevi):** dostupnost, integritet
- Primer: Fannie Mae – osveta otpuštenog saradnika – neuspelo brisanje 4000 servera (TODO: proveriti izvor)

bivsi administrator je hteo da obrise fajlove i onesposobi 4000 servera ali ga IT tim pronasao logicku bombu i to sprecio

Tempirana bomba

- **DEF:** Tempirana bomba je podtip logičke bombe
- Aktivira sa u predefinisanim vremenskim trenucima
  - 1. april
  - Petak 13.
- Michelangelo (1991) se aktivirao na rođendan velikog majstora (6. mart)

prosto preopteretimo stitem, on postaje spor, neupotrebljiv, ili se srusi

Zec moze biti virus ili crv, on nije zaseban softver vec je on samo nacin ponasanja

Zec / Rabbit

on ne pokusava da pristupi podaci pa ne krsi Confidentiality, on ne pokusava da menja podatke pa ne krsi Integrity, ali zato usere sistem pa krsi Availability

- DEF: Zec (eng. Rabbit) je zlonameran softver koji se replicira bez prestanka sa ciljem narušavanja dostupnosti sistema
  - Može biti tipa virus ili crv
- Jedan tip napada tipa odbijanje usluge (Denial of Service – DoS)
- Motivacija (CIA ciljevi): dostupnost (!)

Softver koji prikuplja podatke i salje ih napadacu najcesce preko interneta.

Špijunski softver (spyware)

- **DEF:** Špijunski softver prikuplja informacije, npr. slike ekrana, unos preko tastature, sadržaj formi koje korisnik popunjava, podatke o kreditnim karticama
  - Šalje prikupljene informacije na komandni server
  - Često dospeva na sistem uz pomoć trojanca
  - Rezidentan na računaru korisnika rezidentan - ostaje aktivan u pozadini, cesto prikriven
- **Metod širenja:** akcija korisnika ili slabost sistema
- Najčešći primer:
  - Tracking cookie koji prati korisnikove aktivnosti na Internetu
- **Motivacija (CIA ciljevi):** tajnost (!)

C - prikuplja privatne podatke bez znanja korisnika, ne rusi Integrity jer ne menja podatke vec ih samo posmatra, ne rusi dostupnost jer ne onseposobljava sistem, mozda samo malcice

Keylogger

- Keylogger je tip špijunskog softvera
- Pamti sve što se unosi preko tastature ili drugog ulaznog uređaja
- Prikupljene sekvence unetih podataka
  - Skladišti lokalno
  - Šalje na udaljeni server
- Keylogger se često instalira namerno da bi se pratile aktivnosti zaposlenih

Rootkit je skup alata koji napadacu omogucava administratorski (root) pristup i skrivanje svog prisustva na kompromitovanom racunaru

Rootkit

Confidentiality - nadgleda korisnika, krade fajlove i lozinke,
Integritet - admin moze da menja sve zivo,
Availability - moze da onesposobi servise, brise fajlove ili koristi sistem za ddos

- **DEF:** Rootkit je maliciozan softvera za dobijanje admin prava na sistemu
  - root = administrator na Unix sistemima
  - kit = alat
- **Metod:** korišćenje slabosti, password cracking
  - Stiče se potpuna kontrola nad sistemom
  - Omogućava prikrivanje prisustva
- **Primer:** trivijalan rootkit je zasnovan na poznavanje „zakodiranih“ lozinki administratorskih korisnika, npr. u Stuxnet-u
- Motivacija: (?)

Motivacije su: trajni i dugorocni pristup sistemu, kradja poverljivih podataka, omogucavanje trajnog backdoora, komprovitovanje sistema za dalji napad

Stuxnet (iran) je koristio rootkit da ostane neotkriven duzi vremenski period i prikaze normalan rad dok unistava stvari

Pretnje i slabosti

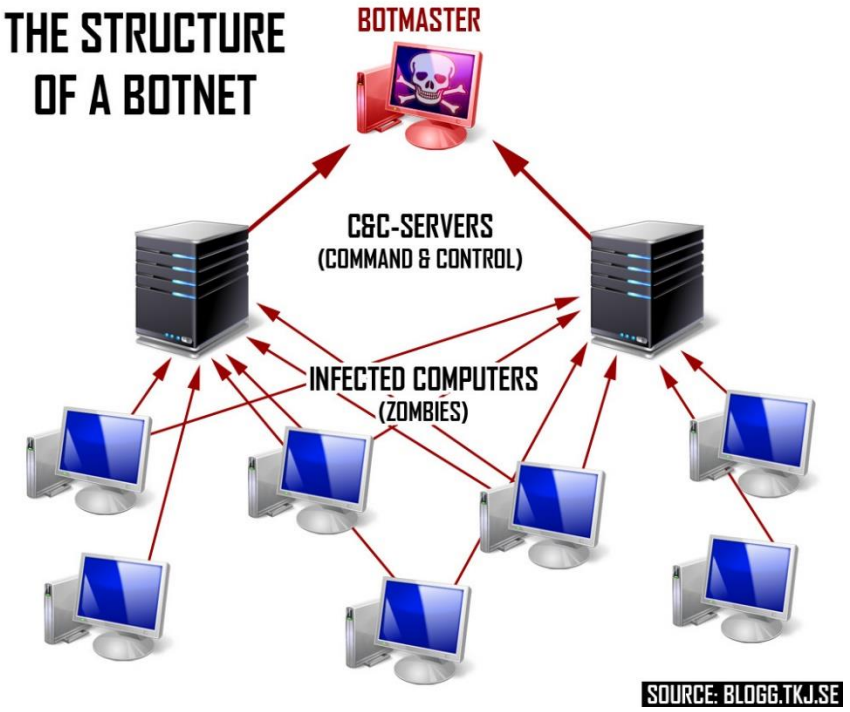
PRIMENA ZLONARMERNOG SOFTVERA

Botnet je mreza zombija kojima napadac upravlja daljinski, obicno putem Command & Control (C&C) servera. Racunari mogu da se zaraze uz pomoc trojanca, phishinga tj socijalnog inzenjeringa, slabe lozinke, neki ranjiv mrezni servis itd.

Botnet

botnet moze da salje spam poruke, krade poverljive informacije, i time nargusava integritet. takodje moze da narusi dostupnost tako sto pravi ddos napade. Sto se tice tajnosti, botnet moze a ne mora da remeti tajnost, cesto on ne pristupa podacima i ne krade ih vec sluzi da uspori mrezu i spamuje

- **DEF:** Botnet je mreža “uhakovanih” računara
  - Članovi mreže se često zovu zombiji
- **Metod:** trojanac + backdoor, socijalni inženjering, ranjivost mrežnih servisa, slabe lozinke
- **Motiv:** moze i tajnost, ali najcesce ova dva
  - Integritet → Neželjene elektronske poruke (tj. Spam)
  - Dostupnost → Distributed Denial of Service (DDoS)
- **Primeri (2020ih):** (?)



Zero day

- **DEF:** (Prvi) napad (tj. korišćenje do tada nepoznate ili nezakrpljene slabosti sistema) pre pojave bilo kakve zaštitne mere je *zero day exploit (zero-day, 0day)*
- Životni vek slabosti nekog softverskog sistema
  1. Pronalaženje dotad nepoznate slabosti u softveru
  2. White/black hat prikaže napad na slabost
  3. Proizvođač saznaje za slabost (*vulnerability*)
  4. Proizvođač napravi i distribuira kontrolu (zakrpu) patch
  5. Korisnici implementiraju kontrolu
  6. Neko iskoristi slabost za napad

XSS je ranjivost koja omogucava ubacivanje i izvrsavanje zlonamernog JavaScript koda na veb stranici - obicno u pregledacu drugog korisnika

Cross-site scripting

Presistent je kada se sacuva na serveru npr u vidu nekog komentara na koga sad mogu da kliknu drugi korisnici
Reflektovani je kada se skripta ubaci u URL na primer, i sad kad korisnik klikne taj link onda se kod njega izvrsava skripta, ovaj napad je brz i lak za izvodjenje ali ne ostaje trajno na sajtu za razliku od perzistentnog XSS-a

- **DEF:** Cross-site scripting (XSS) je **ranjivost veb sadržaja** koja (uglavnom) nastaje usled nenamerne greške tokom razvoja
  - XSS omogućava hakerima da ubace skripte koje se izvršavaju u Internet pretraživačima ili na veb serverima
  - XSS je identifikovan od strane Microsoft-ovih inženjera 2000. godine
  - Jedno vreme je (tokom 2000ih) XSS bio najčešći vid napada na veb sadržaje
- Najčešći i najpoznatiji tipovi XSS: reflektovani moze biti vrlo efikasan ako se dobro sakrije u nekom linku, ili reklami
  - **Perzistentni** – ubacivanje klijentskih skripti u sadržaje koji se čuvaju na serveru i prikazuju drugim korisnicima, sa ciljem krađe osetljivih informacija od drugih korisnika, npr. <script> tag na kraju poruke na forumu
  - **Reflektovani (ne-perzistentni)** – ubacivanje skripti u polja za unos podataka u HTML formama i izvršavanje skripti na serverskoj strani
- Zaštitne mere: validacija ulaza, tj. provera ubačenog koda, isključivanje skripti na klijentskoj strani

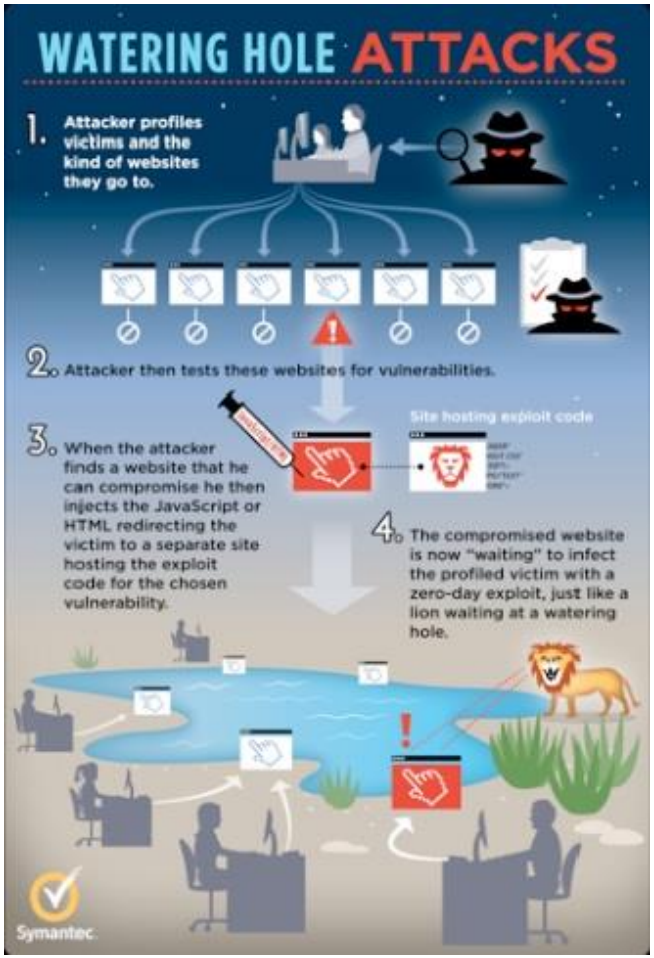
kod perzistentnog se kod cuva na serveru, kod reflektovanog use ubacuje privremeno kroz URL formu, meta napada kod perzistentnog je svi koji vide link, dok je kod reflektovanog samo onaj korisnik koji klikne na link, perzistentni je trajan sve dok se ne obrise sa sajta, dok je reflektovani privremen, zavisi od klika, perzisentni je opasinij jer se lako siri

watering hole je kada napadac kompromituje legitimne i popularne sajtove koje ciljane zrtve redovno posecuju, kako bi zarazeni sadrzaj automatski inficirao njihove sisteme, zivotinje dolaze da piju vodu i predator ih tamo ceka

Watering hole

Gledamo koje sajtove nasa ciljna grupa posecuje, zatim inficiramo te sajtove tako sto iskoristimo neke njihove slabosti i onda on zarazi korisnika

- Termin iz životinjskog sveta
  - Neki tip malware-a se instalira na popularan veb sadržaj korišćenjem neke slabosti
  - Ciljani korisnici posete zaražen veb sadržaj
  - Iskoristi se slabost na njihovim sistemima i zaraze se
- Moguća ciljana primena nakon izviđanja i upoznavanja sa navikama žrtve
- Napomena: napade na softverske lance snabdevanja možemo smatrati specijalizacijom ovog vektora



Pojilo je sajt za azuriranje softvera ili repozitorijum a zrtve su svi korisnici tog softvera, primer je Solar Winds 2020, azuriranja su dolazila sa legitimnog izvora, ali su bila kompromitovana

Napadac ubaci lazne informacije u kes DNS servera, kako bi korisnici bili preusmereni na pogresnu IP adresu, tj maliciozni sajt, taj sajt obicno izgleda identicno kao original, ali je pod kontrolom napadaca

DNS spoofing/poisoning (nije malver!)

- **DEF:** DNS spoofing je (uglavnom) zasnovan na ubacivanju nelegitimnih mapiranja u keš DNS servera
- **Metod:** korišćenje slabosti u DNS serveru
- **Rezultat:** preusmeravanje saobraćaja na maliciozni server (umesto legitimnog)
  - Napomena: traženi veb sadržaj može izgledati potpuno isto i tako prevariti i edukovane korisnike
- **Diskusije:** Gde prebaciti ovo narušavanje integriteta DNS podataka?

moze se povezati sa socijalnim inzenjeringom jer sajt izgleda kao pravi takodje sa watering hole ili phishing napadima jer navodimo korisnika da sam dodje

ovo nije malware, ovo je napad na infrastrukturu interneta

Ransomware

- DEF: Softver za iznudu (eng. *ransomware*) kodira fajlove na disku žrtve i napadač traži uplatu za dobijanje ključa za otključavanje kodiranih fajlova
- Koraci napada na sistem se koristi
  - Ubacivanje trojanca kroz phishing (ili spear phishing) → Moguće je i korišćenje poznate slabosti (Windows, Flash, Acrobate Reader)
  - Generisanje ključa
  - Kodiranaje fajlova na napadunom računaru/mreži, npr. sva Word dokumenta
  - Slanje ključa na (udaljeni) C&C server
  - Prikazivanje poruke na zaraženom računaru i instrukcija za plaćanje
- Otkupnina se često traži u bitcoin-ima da bi bilo otežano praćenje „novca“
- Pošto se koriste jaki algoritmi za kodiranje, jedina prava protivmera je adekvatna zaštita računara i redovno kreiranje bekapova
- Jedan vidi protivmere je dovoljno brz kontra-udar na sisteme hakera i zaplena (master) ključeva za dekodiranje sadržaja

ovde menjamo nacin kojim pristupamo zastiti sistema, efemeralan znaci kratkotrajan, privremen. Ovo je malver koji ne ostaje trajno na disku, nema .exe, .dll itd. On postoji samo u RAM-u dok je aktivan, ne ostavlja tragove za tradicionalne anti viruse koji pretrazuju fajlove. Znaci tesko ga je detektovati, moze da napada u realnom vremenu, koristi ram da manipulise data in use, npr podatke u obradi na serveru.

Efemeralan zlonameran softver

Moze dospeti na racunar preko phishinga, napadac posalje word dokument koji ima skriptu koja ucita softwer u ram, moze da se iskoristi neka ranjivost softwera, ili preko power shella da se ucita malwer iz mreze direktno u ram

- Fokus u zaštiti podataka i servisa je u većini slučajeva na zaštiti snimljenih podataka (data at rest) i podataka koji se šalju (*data in transit*)
  - Snimljen podataka: podatak u bazi podataka, konfiguracioni fajl
  - Podatak na „žici“: HTTP zahtev sa lozinkom poslat serveru
- U drugoj polovini 2010ih se postepeno uvodi i zaštita podataka tokom korišćenja (*data in use*)
- Jedan faktor koji utiče na uvođenje tih mera je eferemeralni zlonameran softver (*ephemeral malware*)
  - Nema binarnih fajlova na disku → nije moguća detekcija tradicionalnim skeniranjem diska
  - Jedino mesto pojave je u radnoj memoriji (npr. servera)

detektuje se preko analzie logova, analize memorije, heuristike ponasanja

- **Diskusija:** Kako dospeva ovaj tip malvera na računar? Kako se pokreće? Da li je perzistencija moguća/potrebna/poželjna?

pokrece se kroz shellcode, powershell skripte, makroe itd. znaci pokrece se u memoriji, perzistencija je moguca, ali nije potrebna, npr ako zelimo nesto samo na kratko da zarazimo onda nam ne treba. Ako je cilj brza kradja podataka i bekstvo onda nije pozeljna jer ostavljamo manji trag, ako zelimo dugorocno prisluskivanje onda je pozeljna

Malver i lanci snabdevanja

- 2020ih godina (i delimično i ranije) je postalo popularno ubacivanje zlonamernog softvera preko lanca snabdevanja
  - Napadač N iskoristi ranjivost u IS kompanije X za proizvodnju softvera ili hardvera
  - N ubaci zlonameran kod (npr. Backdoor) u izvorni kod ili hardver koji se proizvodi u X
  - X zapakuje novu verziju softvera/hardvera zajedno sa ubačenim trojancem
  - X isporuči novu verziju klijentu (KT)
  - Klijenti (koji imaju poverenja u X) instalira softver ili hardver
  - Napadač N koristi ubačenu ranjivost za neovlašćen pristup sistemu KT
- Ovaj vid napada preko lanca snabdevanja možemo smatrati trojancem na steroidima
- **Napomena:** Povremeno se pojavi u vestima da je kompanija Y naručila hardver slanje nacrta i na kraju dobila hardver koji je modifikovan dodvanjem dodatnih čipova i/ili drugih elemenata

Klasifikacija malware-a

- Klasifikacija po **tipu nosica**
  - **Samostalni:** crv
  - **Potreban nosilac:** virus, *backdoor*, trojanac, špijunski softver(i), logička bomba, rootkit
- Klasifikacija po **načinu propagacije**
  - **Replicirajući:** virus, crv oni se koriste bas za rabbit
  - **Nereplicirajući:** *backdoor*, rootkit, špijunski softver(i), logička bomba
  - Trojanac može u obe klase, npr. jeste replicirajući ako pošalje svoj primerak svim kontaktima iz adresara
- Po **složenosti**:
  - **Osnovni tip:** crv, trojanac
  - **Složene pretnje** (bazirane na kombinaciji osnovnih pretnji, fizičkog pristupa i socijalnog inženjeringa): botnet, softvera za iznudu
- Po **vidljivosti**:
  - Prikriven: špijunski softver, crv
  - Vidljiv: softver za iznudu

Pretnje i slabosti

„USPEŠNI“ PRIMERI MALVERA

sirio se automatski bez korisnicke akcije, DCOM RPC servis se koristi za mreznu komunikaciju izmedju procesa, crv koristi b
overflow da ubaci i izvrsi svoj kod, on kreira fajl mblast.exe na sistemu i doda ga u registry kako bi se on pokrenuo pri sled
paljenju racunara, takodje skenira druge dostupne ip adrese i ako pronadje ranjiv racunar inficira ga.

“Uspešan” crv #1: Blaster (2003)

Narusava dostupnost tako sto rusi RPC servis sto dovodi do automatskog restarta sistema, takodje salje ddos napad na windows update servis da bi sprecio korisniku da nabavi zakrpu protiv njega

- Metod:
  - Napad na (buffer overflow) slabost DCOM RPC servisa u Windows-u (XP i 2000 Pro)
  - Aktivno se širio preko Interneta spamovanjem širokih opsega IP adresa
  - Ruši RPC servis što dovodi do restarta sistema
  - Pokretao je DDoS na Windows Update sajt
- Autori originala: kineska grupa Xfocus
- Autor varijante B: tinejdžer iz SAD osuđen na 18 meseci zatvora

ovo je dodatni napad, osim sto se sistem resetuje on vrsi ddos napad na microsoftov update sajt.

bio je uspesan jer je bio zero day, sirio se automatski i agresivno, korisnik nije morao nista da klikne, zarazavao je hiljade racunara dnevno

zrtva dobije email koji izgleda bezopasno, klikom taj .exe .scr .zip fajl u mailu se pokrece crv, instalira se lokalno na racunar, otvara backdoor na TCP port 3127 sto omogucava daljinski pristup napadacu, pretrazuje adresar i salje sebe svima kojima pronadje u adresaru, ima sam svoj sopstveni SMTP server (ne zavisi od outlooka).

“Uspešan” crv #2: MyDoom (2004)

Takodje ima funkcionalnost da pokrene ddos napad na SCO group, americku softversku firmu u sporu sa linux zajednicom u to vreme

- Napadao je starije verzije Windows OS: 95, NT 4.0, 98, ME, 2000, XP
- Do tada najbrže širenje kroz email
- Originalni autor je nepoznat – prve email poruke potiču iz Rusije
- Usporio ceo Internet za ~10%

ogroman broj SMTP poruka je izazvao opterecenje infrakstrukture

- Rezultati
  - Šalje repliku na adrese iz adresara
  - Za par dana na kraju januara 2004. zarazio milion računara
  - Backdoor na TCP portu 3127
  - DDoS napad na web prisustvo kompanije SCO Group

otvoreni backdoor se mogao koristiti za dalje napade i kontrolu

napadao je windows RPC mrezni servis, imao je dodatni brute force metod da nagadja administrativne lozinke, zarazio je milione racunara, blokira antivirus, modifikuje sistemske procese, on je hibrid crva i virusa

“Uspešan” crv #3: Conficker (2008)

taj RPC servis je omogucavao daljinsko izvrsavanje koda i to je ovaj crv iskoristio, takodje pogadja neke lozinke u ostalim umrezenim racunarima, pokusava sa "admin123", "password123" i tako to. Zatim infektuje sistemske fajlove kao sto su explorer.exe i tako postaje rezidentan i otezava se njegovo uklanjanje

- Metod:
  - Windows slabost u mrežnim servisima
  - Pogađanje administratorskih lozinki
- Rezultat: milioni zaraženih računara u:
  - Ministarstvo odbrane UK
  - Mornarica Francuske
  - Nemačke oružane snage, itd.
- Blokira anti-malware
- Hibridni crv+virus: modifikuje svchost.exe ili explorer.exe

ovaj crv se jako dobro branio, blokirao je updatove i onemogucavao je antivirus software, menjao je svoj binarni oblik da bi izbegao signature detekciju,

Složen malver #1: Stuxnet (2010)

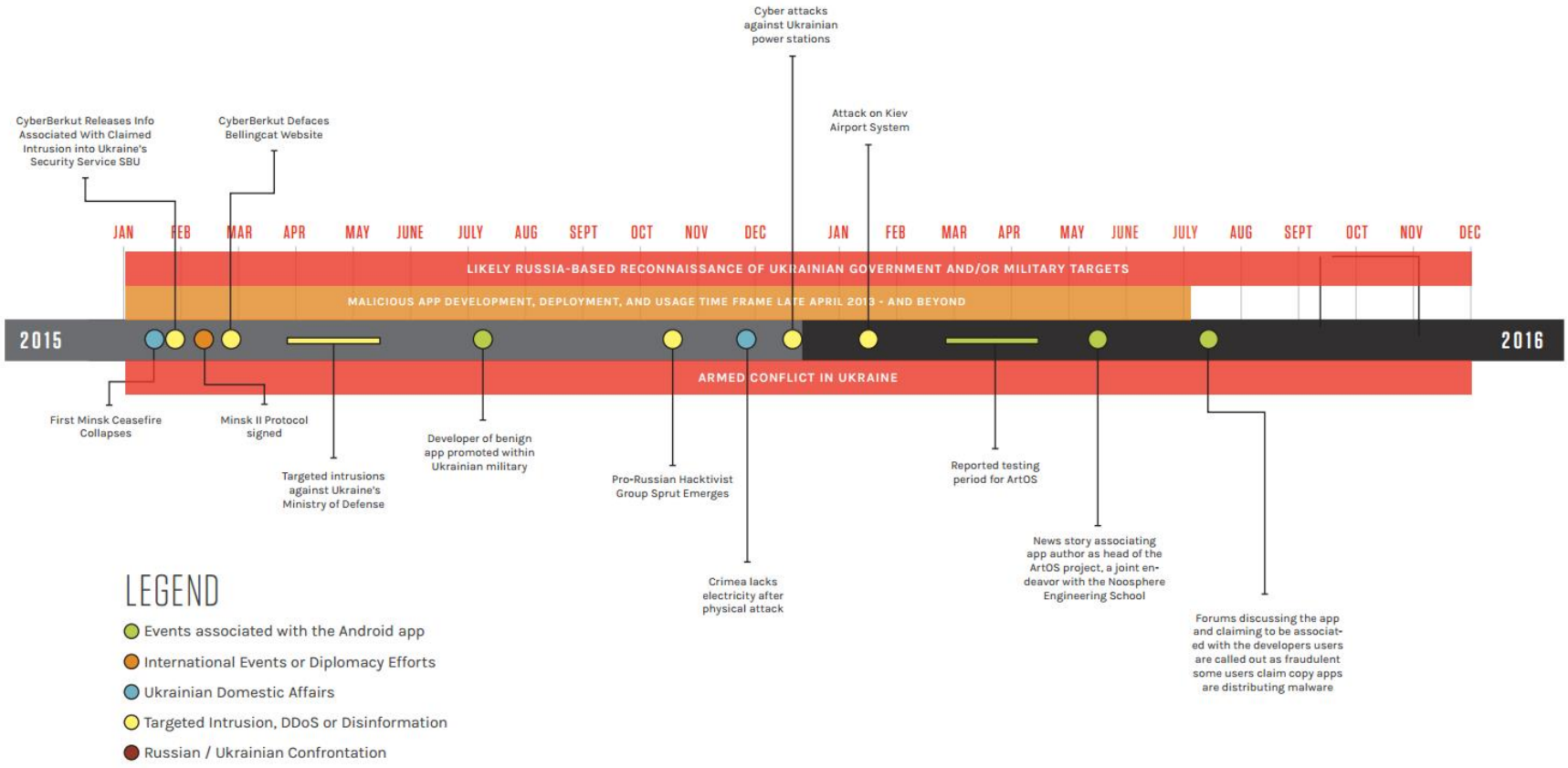
- **Datum:** jun 2010 (detekcija)
- **Motiv:** sabotiranje centrifuga za obogaćivanje uranijuma
- **Izvor:** SAD i Izrael
- **Metod (kompleksni):**
  - **Fizički pristup:** unet zaražen USB drajv
  - **Crv:** zero day exploit (x4)
  - **Nenamerna greška #4:** “zakodirane” lozinke u Siemens Step7 (kontrola PLC-ova)
  - **Rootkit:** prikrivanje izmena na Windows i PLC računaru

- Kontrolisan:
  - briše se 24.06.2012 i
  - širi se na 3 druga računara

Složen malver #2: Flame (2010)

- Slučajno nađen tokom istrage nakon Shamoon
- Koristi iste/slične slabosti kao Stuxnet i Duqu
- Ciljano napada po jednu mrežu
- Kreira slike ekrana, snima mikrofon, lozinke
- Prilično velik sa ~20 MB
- Motiv: sajber-špijunaža
- Metod:
- Meta: Iran i drugi na Bliskom Istoku
- Izvor: SAD/Izrael (?)

Složen malver #3: BlackEnergy (2015)

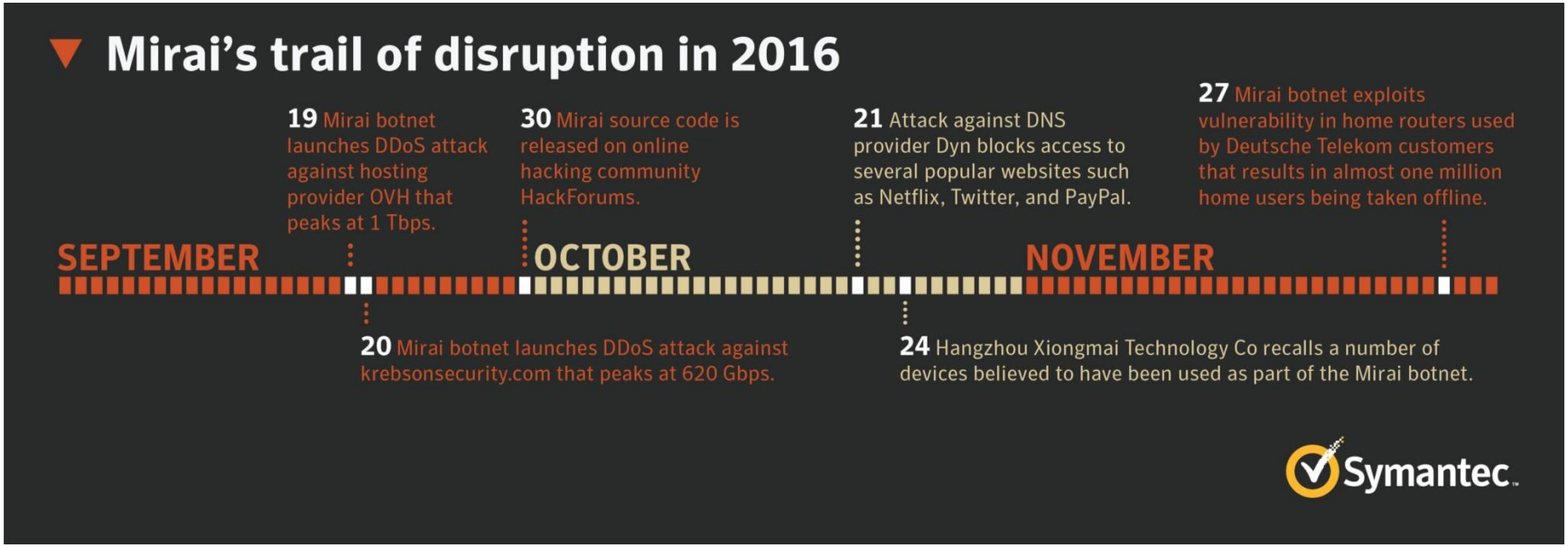


mirai bot skenira javne IP adrese da pronadje IoT uredjaje sa otvorenim telnet ili ssh portovima, proverava hardkodovane i defualt lozinke, admin admin, root 123, onda ako se uredjaj zarazi postaje zombi u bot mrezi, zarazeni uredjaji se povezuju sa centralnim serverom i cekaju instrukcije Command & Control.

Složen malver #4: Mirai botnet (2016)

Zatim ide izvrsavanje ddos napada, kada se aktivira svi zarazeni uredjaji istovremeno salju zahteve ka odabranoj meti, cime paraliziuju ciljane server ili mrezu. Ovo je bilo jako uspesno jer mnogi IoT uredjaji nemaju azuriranja, firewall i jake lozinke, telnet port je cesto ukljucen isto da radi bez nadzora pa je lako napasti preko njega.

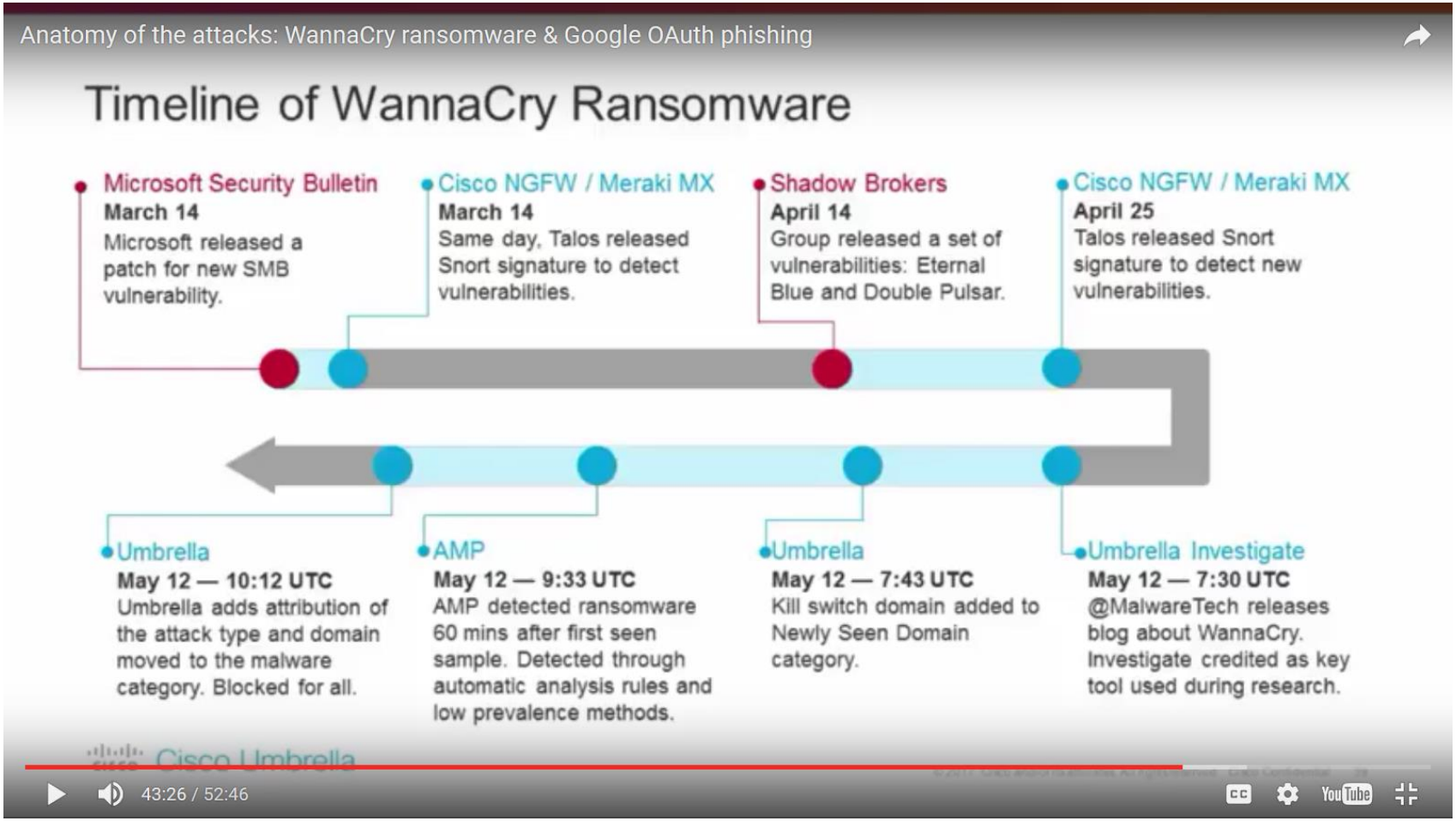
IoT uredjaji: kamere, ruteri, pametni kucni sistemi itd...



Ransomware crv kombinuje sifrovanje i automatsko sirenje, wannacry se ponasa kao crv - kada zarazi jedan racunar automatski skrenira mrezu i siri se na druge ranjive uredjaje bez ljudske interakcije. Nakon sto zarazi racunar korsti RSA + AESenkripciju za zakljuavanje fajlova, dodaje extenziju .wncry i prikazuje poruku da korisnik mora da plati otkup

Složen malver #5: WannaCry (2017)

300 - 600 dolara u bitcoinima po racunaru



Diskusija: Šta se dešava od 2017. godine?

Softverske mere bezbednosti

ANTI-MALVER

Uvod u anti-malver

- **DEF:** Anti-malver je softver za detekciju softverskih pretnji i slabosti
- Najčešće funkcije anti-malver proizvoda:
  - Ugradnja u **operativni sistem (OS)**, npr. povezivanje na kernel
  - **Detekcija** crva, trojanaca i ostalih vidova zlonamernog softvera pre „zaraze“ – na osnovu potpisa ili na osnovu heuristike
  - **Čišćenje** zaraženog računara nakon „zaraze“ – posebni boot-up alati
  - **Skeniranje e-mail priloga** i uklanjanje zlonamernih priloga
  - On-the-fly **analiza sadržaja na Internetu**, npr. kao zaštita od *watering hole* tipa napada
  - **Detekcija zastarelog softvera** koji može sadržati slabosti, itd.
- Primeri: Avast, ESET, Kaspersky, Symantec, itd.

heuristika je prethodno zabelezeno normalno ponasanje

Fuzzy hashing: Upoređuje sličnosti između fajlova, čak i ako nisu 100% identični.

Heuristička analiza: Detekcija bazirana na ponašanju, a ne na tačnom sadržaju.

Princip rada

ova dva pomazu kod :

Tradicionalni AV alati

- Radili su na bazi potpisa

1. Analitičar detektuje i analizira novi malver
2. Analitičar napravi heš malver fajla
3. Heš se ubaci u repozitorijum malver fajlova
4. AV alati imaju učitane heš vrednosti iz repozitorijuma sa kojima porede sumnji fajlove

Izazovi

- Milioni i milioni sličnih, neznatno različitih uzoraka malvera → Kako detektovati sitne razlike i grupisati malver?
- Brz razvoj malvera, kako novih, tako varijanti postojećih → „Najjači“ napadači imaju posebne alate za 0-day ranjivosti
- Kodiran kod malvera → Gde sakriti ključ za dekodiranje?

problem ako neko doda samo nesto malo u fajl neku malu izmenicu onda se hash skroz promeni i ne mozemo ga detektovati

Kaspersky

- Kaspersky Lab je međunarodna grupa za računarsku bezbednost
  - Centrala: Moskva (Rusija)
  - Osnovan: Kaspersky Anti-Virus je objavljen 1997. godine
  - Broj zaposlenih: ~2800
  - Broj korisnika: 300 miliona
  - Portfolio: anti-malware za pojedince i kompanije, istraživanje (eksperti za lov na malware), SecureList.com stranica za edukaciju
- Detekcije: BlackEnergy (2010), Flame (2012), Equation Group (2015)
- Trivia #1: 2015. su optuženi za saradnju sa Ruskom vojskom i tajnim službama
- Trivia #2: 2017. je predsednik SAD izdao ukaz da se Kaspersky proizvodi obrišu sa sistema državnih institucija SAD

Symantec

- Symantec Corporation je tehnološka kompanija:
  - Centrala: Mountain View, California, USA
  - Osnovan: 1982, sa National Science Foundation (NSF) podrškom
  - Broj zaposlenih: 11,000
  - Portfolio: softver za sigurnost, skladištenje, bekap, istraživanje
- Detekcije: DDoS napadi preko IoT uređaja
- Trivia #1: 2012. godine su hakeri ukrali izvorni kod starijih Symantec proizvoda nakon upada na server državne uprave u Indiji
- Trivia #2: Vlasnik Norton brenda

ESET

- ESET je kompanija čija je primarna delatnost IT sigurnost
  - Centrala: Bratislava, Slovačka
  - Osnovan: 1992 – najuspešnija slovačka kompanija 2008, 2009 i 2010
  - Portfolio: anti-malware, firewall
  - Isis (ili Eset) je egipćanska boginja zdravlja, braka i ljubavi
  - Istraživački centri u Slovačkoj, SAD, Kanadi, Poljskoj

Avast

- Avast je češka kompanija fokusirana na razvoj softvera sigurnost i bezbednost
  - Osnovan: 1988, privatna kompanija od 2010. godine
  - Centrala: Prag (Češka)
  - Korisnika: 400 miliona
  - Zaposlenih: 650 (u Češkoj)
  - Portfolio: anti-malware (nema IPS)
- Nagrade: 2016 PCMag.com Editor's Choice za besplatan anti-malware
- Trivia #1: 2016. su kupili AVG Technologies

Rezime

- Osnovne definicije
- Osnovni tipovi malvera
- Malver u primeni
- Konkretni primeri malvera
- Anti-malver

Hvala na pažnji!