Sigurnost u računarskim mrežama

Zlonamerni softver

Nemanja Maček

Agent Smith

- The best thing about being me... There are so many "me"s.

Sadržaj

- Pojam zlonamernog softvera
- Klasifikacija zlonamernih programa
- Trojanski konji, logičke bombe, crvi, virusi i špijunski softver
- Rootkit alati
- Ransomware
- Cyberweapon (na primeru Stuxnet-a)
- Zaštita od zlonamernog softvera

Pojam zlonamernog softvera

- Stroga i precizna definicija zlonamernog programa ne postoji!
- **Zlonameran softver** (engl. *malware*, *malicious software*) je program napravljen sa namerom da na bilo koji način ošteti umrežen ili neumrežen računar (uključujući i mrežne uređaje, kontrolere i bilo koji drugi hardver) i/ili oteža ili onemogući njegovo korišćenje.
- Programi koji inače služe u korisne (dobronamerne) svrhe mogu upotrebiti u zlonamerne svrhe što otežava raspoznavanje i zaštitu!
- Postavljaju se neka pravna pitanja.
- Primer: program koji sakuplja Vaš istorijat pregledanja Web stranica prosleđuje to reklamnoj agenciji koja Vam na osnovu toga generiše reklame.
  - Ovakav softver ima običaj da značajno **troši resurse** (reklame moraju izgledati lepo).
  - Ako ste **prihvatili EULA**, da li se softver karakteriše kao zlonameran?

Tipične aktivnosti koje obavlja zlonamerni softver

- Narušavanje performansi sistema
- Dovođenje sistema u nestabilno stanje
- Generisanje neobičnog ponašanja sistema
- Preusmeravanje zahteva za otvaranjem Web stranica
- Opsluživanje iskačućih (engl. *pop-up*) prozora ili banera reklamnim sadržajem
- Praćenje aktivnosti i uznemiravanje korisnika
- Krađa ili uništavanje poverljivih informacija, industrijska špijunaža
- Šifrovanje datoteka i ucena
- Izvršavanje DDoS napada na određeni server
- Preuzimanje dodatnog izvršnog koda sa Interneta i instalacija drugog malwarea
- Smanjivanje sigurnosti sistema, isključivanje sigurnosnih aplikacija
- Modifikacija lozinki na sistemu i dodela prava daljinskog pristupa računaru
- Menjanje podataka i sistemskih struktura (na primer, Registry baze)
- Uništenje hardvera (na primer, proizvodnih sistema)

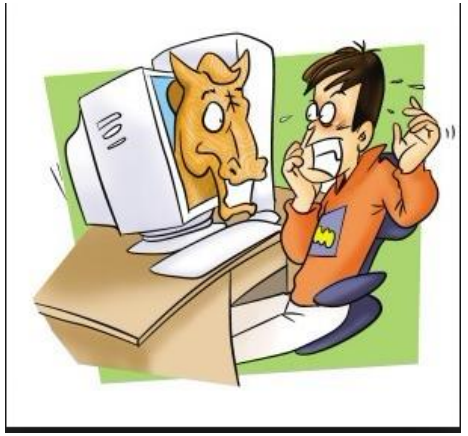
Kako se zlonamerni softver širi?

- Postoji nekoliko načina širenja zlonamernog softvera:
  - **društveni inženjering** (deljeni direktorijumi na mreži, prilozi elektronske pošte, Web stranice, itd.),
  - pomoću **otvorenih portova** koji omogućavaju izvršenje udaljenog koda na žrtvi.
  - **korišćenje drugih zlonamernih programa** koji će preuzeti maliciozni kod sa neke lokacije na Internetu i instalirati ga na žrtvi.
- Mogućnosti distribuiranja ovih programa neiscrpne i stalno se pronalaze nove!
- Najčešće žrtve:
  - komercijalne – Windows, Linux, Mac,
  - vrlo česte žrtve (u domenu tzv. *cyber warfare*) su kontroleri kontretnih proizvođača (pri čemu geolokacija igra značajnu ulogu, tj rasprostranjenost proizvoda konkretnih proizvođača po državama!

Pet kriterijuma klasifikacije

1. **Samostalnost**: zahteva nosioca (trojanski konj, virus), ne zahteva nosioca (crv).
2. **Replikacija**: replicira se (virus), ne replicira se (trojanski konj, logička bomba).
3. **Akcija** koju izvršava payload:
   - ometanje korisnika u radu (*adware*),
   - krađa podataka (*spyware*, *cyberweapon*),
   - izmena ili (potencijalno) uništenje podataka (*ransomware*),
   - uništenje hardvera (*cyberweapon*).
4. **Uslovi** izvšavanja *payload*-a:
   - ne postoje,
   - delimično kontrolisani (logičke bombe),
   - potpuno kontrolisani (*cyberweapon*).
5. **Ciljna grupa**: prosečni korisnici, serveri, industrija, vladine organizacije

Trojanski konji



- Zlonamerni programi koji se maskiraju i reklamiraju kao korisni programi kako bi se korisnici prevarili, tj. naterali da te programe pokrenu (društveni inženjering).
  - Primer: trojanac upakovan u formu programa za instalaciju neke manje aplikacije (setup.exe)
  - Datoteka se postavi na neku Web stranicu, a na nju upućuje hiperveza poput “besplatan program za ...”
- Alternativna metoda širenja trojanaca: upotreba crva kao nosioca.
- Najčešće vrste: trojanci koji otvaraju zadnja vrata, kradljivci informacija, nosioci zlonamernog softvera, i proksi serveri.

Trojanski konji

- **Backdoor trojanac**.
  - Omogućava korisniku da pristupi inficiranom računaru preko mreže.
  - Vlasnik računara najčeće nije svestan posetioca.
  - Napadač može da koristi resurse inficiranog računara (shodno privilegijama).
- **Kradljivac informacija**.
  - **Tip 1**: po inficiranom računaru traže poverljive informacije (privatni i javni ključevi, sertifikati, detalji vezani za kreditne kartice).
  - **Tip 2**: beleži pritisnute tastere (*keylogging*), snima ekrane, ili na neki drugi način omogućava napadaču da prati rad korisnika.
  - Nakon sakupljanja, trojanac šalje korisne informacije (prikupljene podatke):
    - e-poštom poruku na određenu adresu,
    - na neku Web lokaciju sa koje napadač može da ih pročita.

Trojanski konji

- **Nosioci softvera**.
  - Nakon instalacije ponašaju kao **magnet za drugi zlonameran softver**.
  - **Tip 1** (*downloader*).
    - U izvršnoj datoteci ne sadrži kod drugih zlonamernih programa.
    - Pokušava sa Interneta da preuzme i instalira drugi zlonameran softver.
  - **Tip 2** (*dropper*)
    - U izvršnoj datoteci sadrži kod drugih zlonamernih programa.
    - Prilikom pokretanja, dropper će iz svoje izvršne datoteke izdvojiti drugi zlonamerni program i smestiti ga na računar.
- **Trojanski proksi server**.
  - Pretvara inficirani računar u proksi server.
  - Udaljenim korisnicima se dozvoljava da preko inficiranog računara anonimno pristupe Internetu.

Logičke bombe

- Jedna od najstarijih vrsta zlonamernih programa.
- Zlonameran kod ugrađen u neki koristan program koji će se aktivirati kada se **ispune odgovarajući uslovi**:
  - u određeno vreme ili određenog datuma,
  - ukoliko na disku postoji određena datoteka,
  - ako se na sistem prijavi određeni korisnik.
- Kada se aktivira, logička bomba se **najčešće ponaša destruktivno**.
- Primer:
  - Programer može sakriti deo koda koji će brisati projektne datoteke u slučaju da on napusti kompaniju u kojoj radi.
  - Kasnije se taj isti programer može ponovo priključiti kompaniji kao visokoplaćeni konsultant koji će otkloniti “grešku u kodu”.
  - Do sada je zabeleženo nekoliko ovakvih slučajeva.

Logičke bombe

- Da bi se kod uopšte mogao klasifikovati kao logička bomba, akcija koju izvršava mora biti **nepoželjna i nepoznata korisniku** (do momenta izvršenja).
  - Trial program koji nakon 15 dana isključuju određenu funkcionalnost i počinje da radi kao freeware varijanta **nije** ne-destruktivna logička bomba.
  - Ovo ponašanje je očekivano!
- Virusi i crvi često sadrže logičke bombe!
  - Masovno širenje na druge sisteme u datom trenutku.
  - Destruktivne akcije virusa i crva ponekad se takođe izvove pomoću logičkih bombi.
  - Primer:
    - Virus koji briše određene datoteke ukoliko je tekući datum 1. april.
    - Izvršavanje DDoS napada na žrtvu pomoću logičke bombe (sinhronizacija velikog broja računara koji kao zombiji učestvuju u napadu)

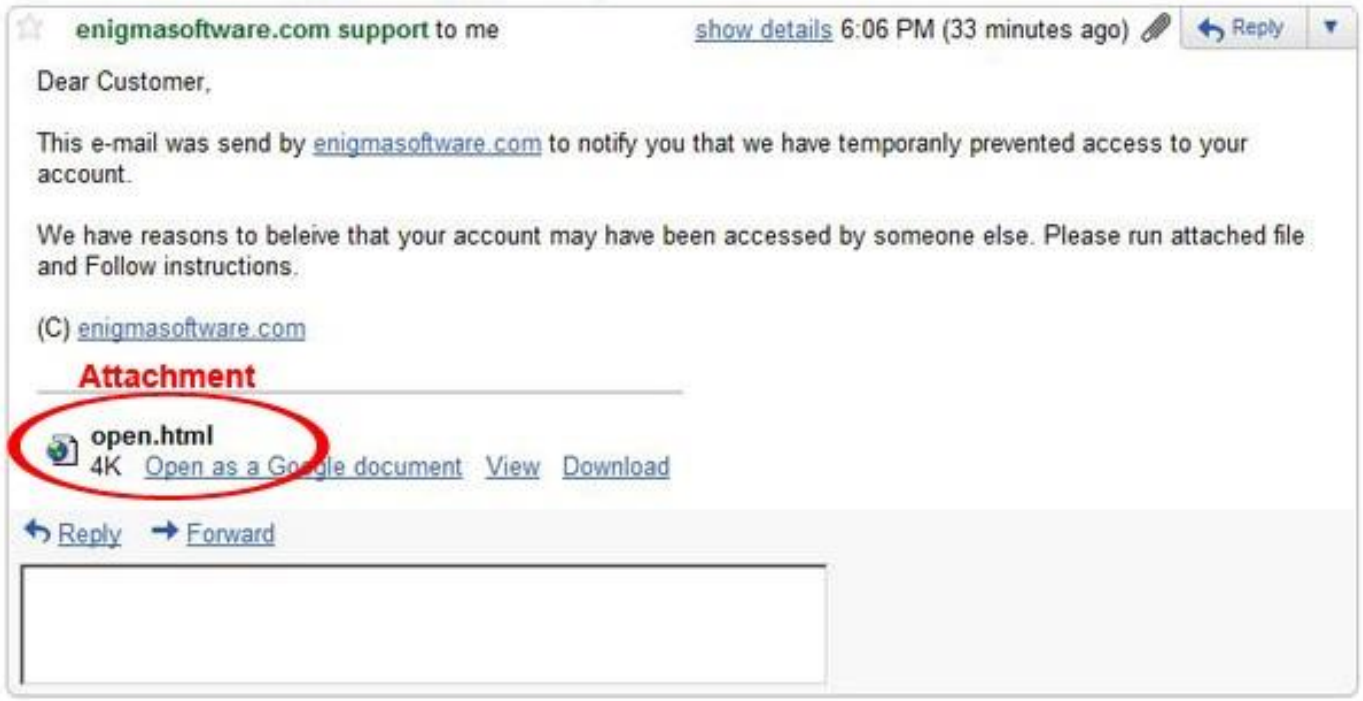
Crvi

- Samostalni (*stand-alone*) programi koji se šire s jednog računara na drugi.
- Crv eksploatiše **ranjivost žrtve** ili koristi **društveni inženjering**.
- Uobičajene metode prenošenja na žrtvu: **e-pošte** i **Internet servisi** (HTTP)
- Crvi koji su uspeli da naprave veću štetu koristili su više različitih metoda širenja!

E-mail crvi

- E-mail crvi (MyDoom, Sasser) šire se pomoću:
  - priloga e-pošte (izvršne datoteke),
  - linka ka inficiranim Web stranicama (takozvana udica – engl. *hook*).
- E-mail crvi koriste metode društvenog inženjeringa.
- Korisnik dobija poruku sa naslovom tipa "*critical windows update*" ili slično.
  - Ukoliko korisnik pokrene program u prilogu crv će se aktivirati i inficirati računar
  - Ukoliko korisnik pritisne link (udicu) otvara se Web lokacija koja će instalirati crva na žrtvu.
- Nakon inficiranja crv se širi tako što:
  - pribavlja adrese iz resursa inficiranog računara (Address Book, stringovi oblika ime@lokacija.com u datotekama sa odgovarajućim tipom),
  - šalje kopije na te adrese (formira se slična poruka),
  - odgovara na svu poštu u poštanskom sandučetu.

E-mail crvi


enigmasoftware.com support to me
show details 6:06 PM (33 minutes ago)
Reply
Dear Customer,
This e-mail was send by enigmasoftware.com to notify you that we have temporanly prevented access to your account.
We have reasons to beleive that your account may have been accessed by someone else. Please run attached file and Follow instructions.
(C) enigmasoftware.com
Attachment
open.html
4K Open as a Google document View Download
Reply
Forward

Internet crvi

- Intenet crvi koriste dve traže **ranjive računare**, pokušavaju da iskoriste propust i da se instaliraju na žrtvi.
  - Računare na kojima **nisu instalirane sigurnosne zakrpe**.
  - Računare sa **otvorenim portovima** koje crv može da iskoristi.
- Tehnike za propagaciju internet crva:
  - **Eksploatacija slabosti** OS-a ili sigurnosnih propusta.
    - Crv šalje pakete koji će instalirati ili celog crva ili samo udicu koja preuzima i instalira celog crva.
  - ***Piggy-backing*** (korišćenje drugog zlonamernog softvera kao nosioca).
    - Crv identifikuje trojanca ili drugog crva koji je instalirao backdoor na žrtvi.
    - Ova funkcionalnost u većini slučajeva dozvoljava crvu da šalje komande žrtvi (na primer, da preuzme i izvrši neku datoteku, najčešće novog crva).

Virusi

- Jedna od najpodmuklijih vrsta zlonamernog softvera.
- Česti efekti infekcije virusima su brisanje važnih datoteka i/ili dovođenje sistema u stanje u kome ne može normalno da se koristi.
- Virusi se šire oslanjajući se na činjenicu da **korisnik ne zna da je poslao inficiranu datoteku** kao prilog e-poruke ili da je prijatelju poklonio DVD sa zaraženom datotekom.
- Klasifikuju se:
  - Prema okruženju u kome virus može da inficira druge objekte.
  - Prema metodama infekcije, tj. tehnikama za umetanje virusa u neki objeka.
- Virusi koji napadaju sisteme datoteka tipa **najčešće inficiraju izvršne datoteke**.
- Prema metodama inficiranja dele se na **prepisujuće** (engl. *overwriting*) i **parazitske** (engl. *parasitic*).

Prepisujući virusi

- **Prepisujući virusi** koriste najjednostavniji metod inficiranja.
- Virus zamenjuje deo koda inficirane datoteke svojim kodom, a datoteka nakon toga postaje neupotrebljiva.
- **Lako se detektuju** (korisnik primećuje da datoteka ne radi)
- **Teško se čiste** jer antivirusni softver ne zna kako da rekonstruiše originalni kod datoteke
- Metoda zaštite koja donekle može obezbediti rekonstrukciju uništenih datoteka jeste povremeno kopiranje svih izvršnih datoteka u neki zaštićeni direktorijum.
  - Čuvanje kopija zdravih izvršnih datoteka u **karantinu**.

Parazitski virusi

- Dodaju svoj kod u datoteku tako da datoteka ostane **delimično ili potpuno funkcionalna**.
- Virus može upisati svoj kod:
  - na početak datoteke (engl. *prepending*),
  - na kraj datoteke (engl. *appending*),
  - unutar postojećeg koda (engl. *inserting*).
- **Virus koji upisuje kod na početak datoteke**.
  - Pomera zdrav kod sa početka na kraj izvršne datoteke i upisuje zlonamerni na početak ili dodaje kod zdrave datoteke na svoj kod.
  - Nakon pokretanja inficirane datoteke, najpre se izvršava kod virusa.
  - Kako bi održao integritet aplikacije, virus može privremeno očistiti inficiranu datoteku, dozvoliti joj da se normalno izvrši, a zatim je ponovo inficirati:
    - Virus koristi privremene datoteke za čuvanje čistih verzija inficirane datoteke.
    - Virus čisti aplikaciju u memoriji i sređuje potrebne memorijske adrese (teško).

Parazitski virusi

- **Virus koji upisuje kod na kraj datoteke**.
  - Većina virusa pripada ovoj kategoriji.
  - Virus najpre dopisuje svoj kod na kraj inficirane datoteke, a zatim modifikuje ulaznu tačku u zaglavlju datoteke.
  - Pre izvršenja samog programa izvršava se zlonamerni kod.
  - Ovi virusi se lako otkrivaju i čiste na osnovu antivirusnih definicija.
- **Virus koji upisuje kod unutar postojećeg koda**.
  - Koristi dve tehnike za upis zlonamernog koda u zdrav kod:
    - Pomera originalni, zdrav kod na kraj datoteke.
    - Upisuje svoj kod u šupljine zdravog koda (engl. *cavity virus*), na primer, u šupljine između sekcija .exe datoteka.
  - Ukoliko je virus ovog tipa loše napisan aplikacija neće funkcionisati i virus će najverovatnije biti brzo otkriven!

Špijunski programi

- ***Spyware*** je neželjeni program instaliran bez znanja (ili odobrenja) korisnika koji prikuplja informacije o aktivnosti korisnika, lozinke i finansijske informacije.
- ***Adware*** ove informacije prikuplja i šalje *behavioural marketing* kompanijama.
  - Oglašavaju se preko pop-up prozora i banera ugrađenih u aplikativni softver.
- Simptomi infekcije:
  - neželjeni pop-up prozori s reklamama koji se pojavljuju dok pretražujete Internet,
  - otvaranje nove instance čitača Weba sa neželjenim reklamama,
  - novi toolbar i/ili promenjen home page u Web čitaču,
  - Web zahtevi su preusmereni.
- Adware se često ugrađuje u *freeware* / *shareware* programe (ponekad kao zasebna aplikacija, ponekad *hard-coded*)
- Ovakav softver je obično praćen veoma dugim EULA.

Rootkit

- **Rootkit** se definiše kao skup alata koji napadačima omogućavaju **najviši nivo pristupa i potpune kontrole kompromitovanog sistema**.
- Da bi napadač mogao uspešno da završi napad, rootkit mora ostati **skriven u sistemu**, tj. ne sme biti vidljiv za administratore i programe za zaštitu od zlonamernog softvera.
- Primeri incidenta nastalih upotrebom rootkita:
  - nelegalno nametanje DRM-a – *Sony BMG copy protection rootkit scandal* (2005),
  - nelegalno prisluškivanje oko 100 mobulnih telefona na Vodafone Greece mreži koji su pripadali članovima Grčke vlade – *Greek Watergate* (2004-2005).
- U nekim slučajevima Rootkit pruža željenu funkcionalnost a korisnik ga sam instalira:
  - zaobilaženje *Microsoft Product Activation* rutina,
  - *anti-theft* zaštita laptop računara BIOS rootkitom.

Rootkit tipovi

- ***User mode*** (najmanje privilegije, prsten > 0).
  - Veliki broj instalacionih vektora koji presreću i modifikuju ponašanje API-ja.
- ***Kernel mode*** (najviše privilegije na nivou OS-a, prsten 0).
  - Dodaje se kod ili se menjaju delovi jezgra.
  - Implementacija: LKM (Linux), drajveri (Windows).
- ***Bootkits*** (kernel mode rootkit koji inficira MBR)
  - Služi za napad na tzv. *full disk encryption* sisteme.
  - Postojan do tranzicije u zaštićeni mod, subverzija kernela.
  - *Stoned Bootkit*: kompromitovani boot loader koji presreće kriptografske ključeve i lozinke.
- ***Hypervisor level rootkit*** (prsten -1).
  - Presreće komunikaciju OS – hardver
- ***Firmware level rootkit*** (najviše privilegije).

Linux rootkit

- Napad na sistem zasnovan na rootkit alatima izvodi se u četiri faze:
  1. **Sakupljanje informacija** o ciljnom sistemu.
     - Koji je OS u pitanju, koja verzija jezgra, koji korisnički nalozi postoje itd.
  2. **Sticanje administratorskih prava**, tj, prava koja ima korisnik root.
     - Napadač mora da na sistemu pronađe i iskoristi neku ranjivost ili da se posluži metodama društvenog inženjeringa.
     - Ostvarivanje root pristupa nasilnom promenom lozinke NIJE dobro rešenje.
       - Napadač će biti vrlo verovatno neprimećen ako se root lozinka promeni.
  3. **Instaliranje rootkit alata**.
     - Na primer: dodaje se kao kernel modul komandom `insmod rootkit_modul`.
     - Prikrivanje tragova napadača i obezbeđivanje zadnjih vrata.
  4. **Uspostavljanje kontrole** nad ciljnim sistemom.

Aplikacioni Linux rootkit

- Rad aplikacionih rootkit alata zasniva se na **zameni legitimnih aplikacija**.
- Ubačene datoteke omogućavaju napadaču da **prikrije svoje prisustvo** i da **obavi željene aktivnosti na sistemu** (na primer, alat može da obezbedi zadnja vrata).
- Programi koje napadač menja kako bi sakrio svoje prisustvo na sistemu:
  - skrivaju datoteke i direktorijume koje je napadač podmetnuo (ls, find, du),
  - skrivaju procese koje je napadač pokrenuo (ps),
  - sprečavaju ubijanje procesa koje je pokrenuo napadač (kill, killall),
  - prikrivaju aktivnosti napadača na mreži poput veza ka otvorenim portovima (netstat, ifconfig),
  - skrivaju zapise u dnevničkoj datoteci o vezama koje napadač ostvaruje sa udaljenim sistemom (syslogd).

Aplikacioni Linux rootkit

- Programi koje napadač menja kako bi **sebi ostavio backdoor**: chfn, chsh i passwd.
  - Primer: chfn zmenjen tako da omogući pristup shell-u sa root privilegijama ako se umesto novog punog imena korisnika unese odgovarajući niz karaktera (tzv. ***backdoor* lozinka**).
- Napomena: razmatramo situaciju u kojoj je na sistem prijavljen neprivilegovan korisnik koji želi da otvori komandni interpreter sa privilegijema korisnika root!
- U najefikasnijem slučaju, napadač menja program login:
  - Ako korisnik navede korisničko ime jsmith i odgovarajuću *backdoor* lozinku, izmenjeni login program pokrenuće shell instancu sa akreditivima korisnika jsmith.
- Napadač može da izmeni i izvršne datoteke nekih mrežnih servisa i sebi otvori *backdoor*.
  - Za postavljanje *backdoor*-a može se iskoristiti i sshd slično programu login.

Linux kernel rootkit

- **Rootkit alati na nivou jezgra** otkrivaju se teže od aplikacionih!
- Integrišu u samo jezgro OS što znači da ih može zaobići provera integriteta sistema obavljena u neprivilegovanom režimu rada!
- Rootkit alati jezgra zasnovani su na činjenici da je **jezgro Linux sistema modularno**.
  - Korisnik sa root privilegijama može u jezgro učitati neki modul (*Loadable Kernel Module*, *LKM*) i na taj način proširiti funkcionalnost operativnog sistema.
  - U normalnim okolnostima LKM je veoma koristan jer omogučuje proširenja.
- Napadači mogu da iskoriste ovu prednost tako da presreću sistemske pozive, sakrivaju datoteke, zaobilaze prava pristupa, promenu chroot okruženja, itd.
- Kako?

Linux kernel rootkit

- Prilikom izvršavanja **sistemskih poziva** prelazi se **iz korisničkog režima u zaštićeni režim**.
- Napadač dodavanjem LKM rootkita **menja funkcionalnost određenih sistemskih poziva**.
  - Na taj način vara sve programe u korisničkom režimu i koriste te sistemske pozive.
- Nakon instaliranja LKM rootkit alata:
  - Korisnik se normalno obraća jezgru preko sistemskih poziva.
  - Prosleđivanje određenih parametara imaće za posledicu to da **trojanski sistemski poziv** obavlja neke akcije u korist napadača.
- Primer:
  - Napadač ubacuje LKM koji menja funkcionalnost sistemskih poziva za rad sa datotekama kako bi sakrio datoteke.
    - Posledica: sve komande koje koriste ove sistemske pozive neće videti te datoteke.
- Modifikacijom sistemskih poziva mogu se sakriti i aktivni procesi!

Ransomware

- Ransomware predstavlja **digitalni mehanizam iznude**.
- Formalno se može definisati kao vrsta zlonamernog softvera koja:
  - šifruje datoteke računara žrtve.
  - korisniku zaraženog računara prikazuje uputstvo o načinu plaćanja otkupnine odgovarajućim elektronskim metodama plaćanja kako bi dobio ključ za dešifrovanje datoteka.
- Ransomware koristi algoritme otporne na kriptoanalitičke napade, tako da je nemoguće doći do ključa za dešifrovanje u razumnom vremenu primenom alternativnih metoda.
  - Isključujući direktan napad na server ključeva, ukoliko isti uopšte postoji.
- Korisniku inficiranog računara preostaje da bira između plaćanja iznude ili trajnog gubitka podataka (u slučaju da nema rezervnu kopiju).

Ransomware

- Vremensko ograničenje nakon koga se brišu ključevi sa servera u većini slučajeva postoji, što psihološki dodatno stimuliše korisnike da izvrše uplatu.

Ransomware

- Mnoge žrtve odlučuju da plate otkupninu.
- Razlog plaćanja je velika vrednost podataka za koje **ne postoji aktuelna rezervna kopija**.
  - Bolnica u Holivudu isplatila $17.000 kako bi povratila važne podatke pacijenata.
  - Uplata je izvršena 10 dana nakon napada a ključevi su nakon uplate predati bolnici.
- **Garancija da će žrtva nakon isplate dobiti ključeve ne postoji**!
  - Korisnik može platiti otkupninu i na kraju ostati praznih ruku.
  - Još gore, otmičar može tražiti još veći otkup ukoliko su podaci žrtvi značajni, što se može zaključiti na osnovu pasivnog izviđanja ili brzine uplate.
- Metode distribucije:
  - iskorišćavanje ranjivosti mrežnih servisa,
  - distribucija putem USB fleš memorija i zaraženih memorijskih kartica,
  - društveni inženjering.

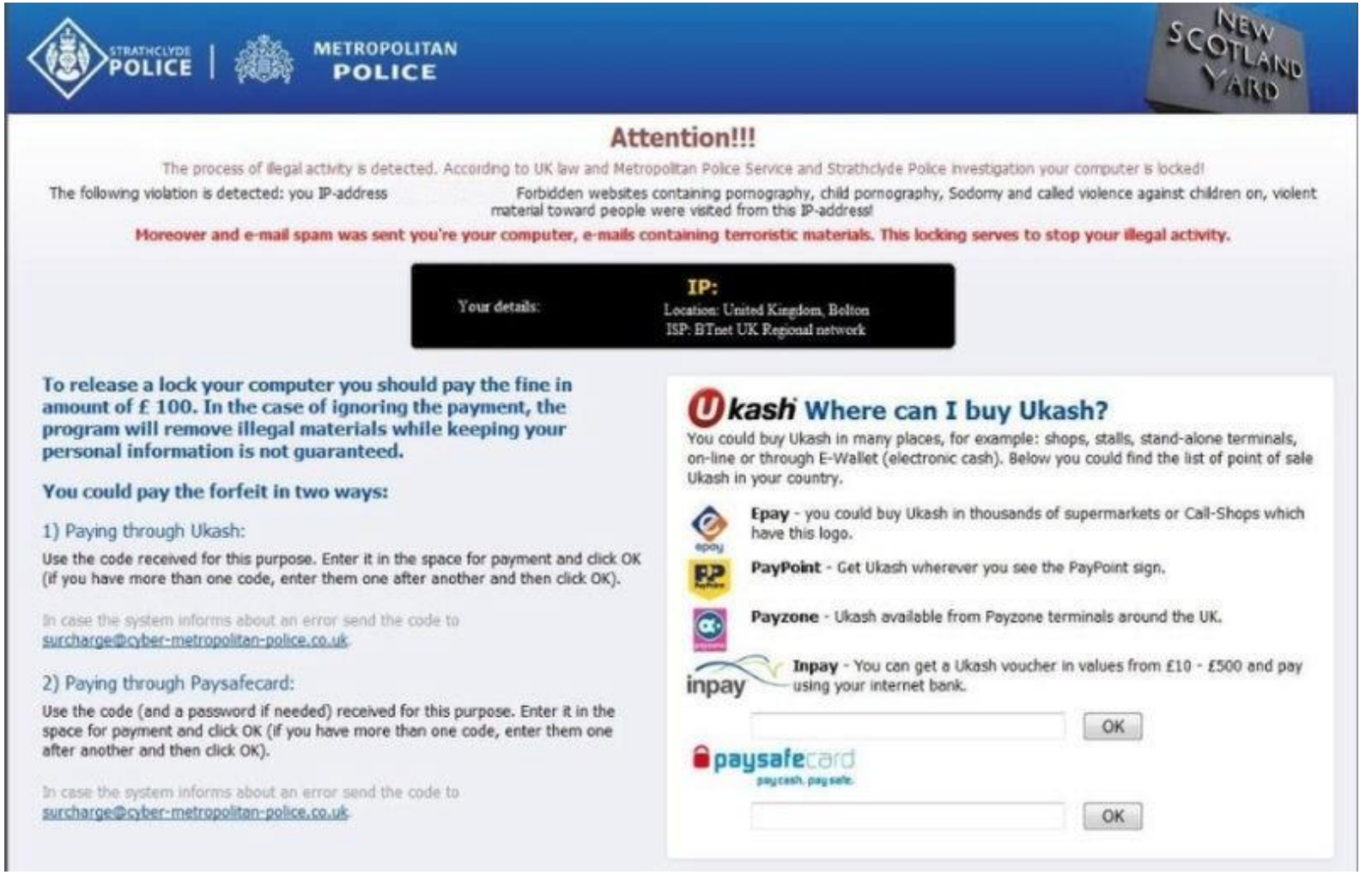
Ransomware

- Ransomware pored šifrovanja datoteka sprečava ili ograničava korisnicima pristup OS-u (šifruju se određene sistemske datoteke).
- U ovom slučaju se prilikom prvog restartovanja računara nakon infekcije pojavljuje prozor u kome navodno MUP, FBI i njima slične institucije upozoravaju korisnika da je računar zaključan jer je izvršio određene nelegalne aktivnosti sa tog računara.
- Payload u ovom slučaju ima takozvanu ***scareware* formu**.
- Tipična poruka koja se prikazuje korisniku može imati sledeći sadržaj:

„Računar je zaključan od strane FBI zbog toga što ste 11. aprila 2015. godine Vi ili neko drugi sa ovog računara posećivali sajtove sa dečjom pornografijom”

Scareware forma upozorenja

Scareware forma upozorenja



Zaštita od ransomwarea

- Zaštita od ransomwarea:
  - redovna izradu rezervnih kopija podataka,
  - edukacija korisnika,
  - upotrebu softvera za zaštitu od zlonamernih programa (antivirusni alati sa ažuriranim definicijama koje uključuju i *ransomware*).
- Jedina 100% sigurna zaštita od gubitka podataka uzrokovanog ransomwareom je **redovna izrada rezervnih kopija svih podataka**.
  - **Eksterni HDD za backup** ne sme da bude stalno povezan na računar.
    - U suprotnom, ransomware će šifrovati i datoteke na backup HDD-u.
  - Ako se **rezervna kopija smešta u Cloud**, datoteke treba uploadovati ručno.
    - Ako je sinhronizacija automatska datoteke na Cloudu mogu takođe biti šifrovane.

Da li platiti otkupninu ili ne?

- Postoje dva oprečna mišljenja.

1. Kriminalci žele da način plaćanja učine jednostavnim i da žrtvi dostave ključ.
   - Samo žele da im ljudi plate i da se pročuje za to da tim plaćanjem zaista dobijaju pristup svojim podacima.
   - Ne ide im u prilog širenje informacija da nakon plaćanja žrtve ne dobijaju pristup svojim podacima.
2. Kriminalci nemaju nameru da predaju ključ iako do uplate dođe.
   - Mala je verovatnoća da će ljudi koji plate otkup i ne dobiju ništa pričati o tome.
   - Žrtva koja dobije ključ ili određeni alat za dešifrovanje i dalje nije bezbedna.
   - Kriminalci i dalje imaju pristup računaru žrtve i ponovo mogu zahtevati otkup, najčešće mnogo veći.

Kada je nastao prvi „komercijalni“ ransomware?

- Tipična greška: većina ljudi će reći da se ransomware pojavio 2000-ih godina!
- Prvi zvanični ransomware pojavio se 1989. godine.
  - AIDS Trojan (distribucija preko floppy diskova)
  - Menja AUTOEXEC.BAT i broji koliko se puta podigao sistem
  - Ako je boot count = 90, AIDS krije direktorijume i šifruje datoteke na disku C:
  - Od korisnika se traži da „obnovi licencu“ i kontaktira PC Cyborg Corporation za detalje uplate
  - Nakon uplate $189 na PO Box u Panami korisnik dobija flopi disk za dešifrovanje.
- Drugim rečima: ništa novo, ali vremenom evolvira!

Evolucija od lažnih ka kriptografskim rešenjima

- **Napadi na antivirusna rešenja** (2008-2009).
  - Skeniranje sa gomilom namernih *false positive*-a (lažne infekcije).
  - Traži se $100 za rešavanje „problema“.
  - Deinstalacija najčešće rešava problem: napadač ne dobija novac.
- **Zaključavanje računara** (2008-2012).
  - Računar se zaključava.
  - Traži se otkup u opsegu $150 – $ 200 (digitalni vaučer).
  - Evolucija od lažnih ka pravim kripto-rešenjima i opravdanim zahtevima za otkup.
- **Kriptografska rešenja** (2013-).
  - Otkupnina je reda veličine $300 (uglavnom Bitcoin).

Neki primeri ransomwarea

- Primer *locker ransomware*-a: **Reveton**, **police trojan** (2012).
  - Payload prikazuje upozorenje koje potiče od policije u kome se navodi da je računar korišćen za nelegalne aktivnosti poput preuzimanja nelicenciranog softvera
  - Lokalizacija upozorenja: varijante koje su inficirale računare u Britaniji prikazivale su logo ustanova Metropolitan Police Service i Police National E-Crime Unit.
- Primer kriptografskog *ransomware*-a: **Cryptolocker** (2013).
  - Šifruje datoteke sa specifičnim ekstenzijama.
  - Otkupnina 400 dolara (ili protivvrednost u evrima) putem anonimnog pre-paid gotovinskog vaučera (MoneiPak ili Ukash) ili ekvivalentnog iznosa u Bitcoin valuti u roku od 72 ili 100 sata.
  - Kreirala i kontrolisala bot net grupa Gameover ZeuS (Evgenij Bogačev).
  - Širenjem CryptoLocker-a i naplatom otkupa **zaradili oko 3 miniona dolara**.

Slučaj maja meseca 2016. godine

- Maj mesec 2016. godine može se neformalno obeležiti kao mesec ransomware-a.
  - 16 novih ransomware trojanaca se pojavilo na Internetu (Shujin, Cryptohitman, Crypren, 8Lock8, Zyklon, ...)
  - Postojeći su unapređeni.
  - Kao novitet pojavljuje se i ransomware kao usluga (**Ransomware-as-a-Service**, **RaaS**).
- Dobra vest koja donekle parira ovoj najezdi trojanaca je da se pojavilo barem šest novih alata za dešifrovanje koji ne zahtevaju plaćanje otkupa (npr, za CryptXXX v2).

Cyberweapon

- **Cyberweapon** je zlonamerni softverski agent koji se upotrebavlja u vojne, paravojne ili obaveštajne svrhe.
- Kriterijumi koje agent mora da ispuni kako bi bio klasifikovan kao cyberweapon su:
  - **Formalno sponzorstvo** (sponzor je vladin ili ne-vladin entitet).
  - **Namenjen je specifičnim metama** (visoka selektivnost).
    - Precizno definisana ciljna grupa i metode identifikacije potencijalnih meta
  - Izvršava zadatak koji bi inače zahtevao **špijunažu** ili **upotrebu sile**:
    - Nadgledanje proizvodnih sistema, državnih ili vojnih institucija i slično.
    - Krađa intelektualne svojine, poverljivih državnih ili vojnih podataka.
    - Uništenje koda ili podataka na računaru ili povezanom sistemu.
    - Nanošenje štete ili uništenje računarskog hardvera.
    - Nanošenje štete upravljačkim sistemima: rezultujuća industrijska nesreća za posledicu ima gubitak imovine, ljudskih života i/ili značajnu ekonomsku štetu.

Stuxnet

- Prvi put identifikovan sredinom juna 2010. godine (kompanija VirusBlockAda).
- Kaspersky Lab navodi da je Stuxnet počeo da se širi marta 2010. godine, a prva verzija ovog crva pojavila se juna 2009. godine.
- Symantec navodi da su najugroženije zemlje u ranim danima infekcije:
  - **Iran (58,85%)**
  - Indonezija (18,22%)
  - Indija (8,31%)
  - Azerbejdžan (2,57%)
  - SAD (1,56%)
  - Pakistan (1,28%)

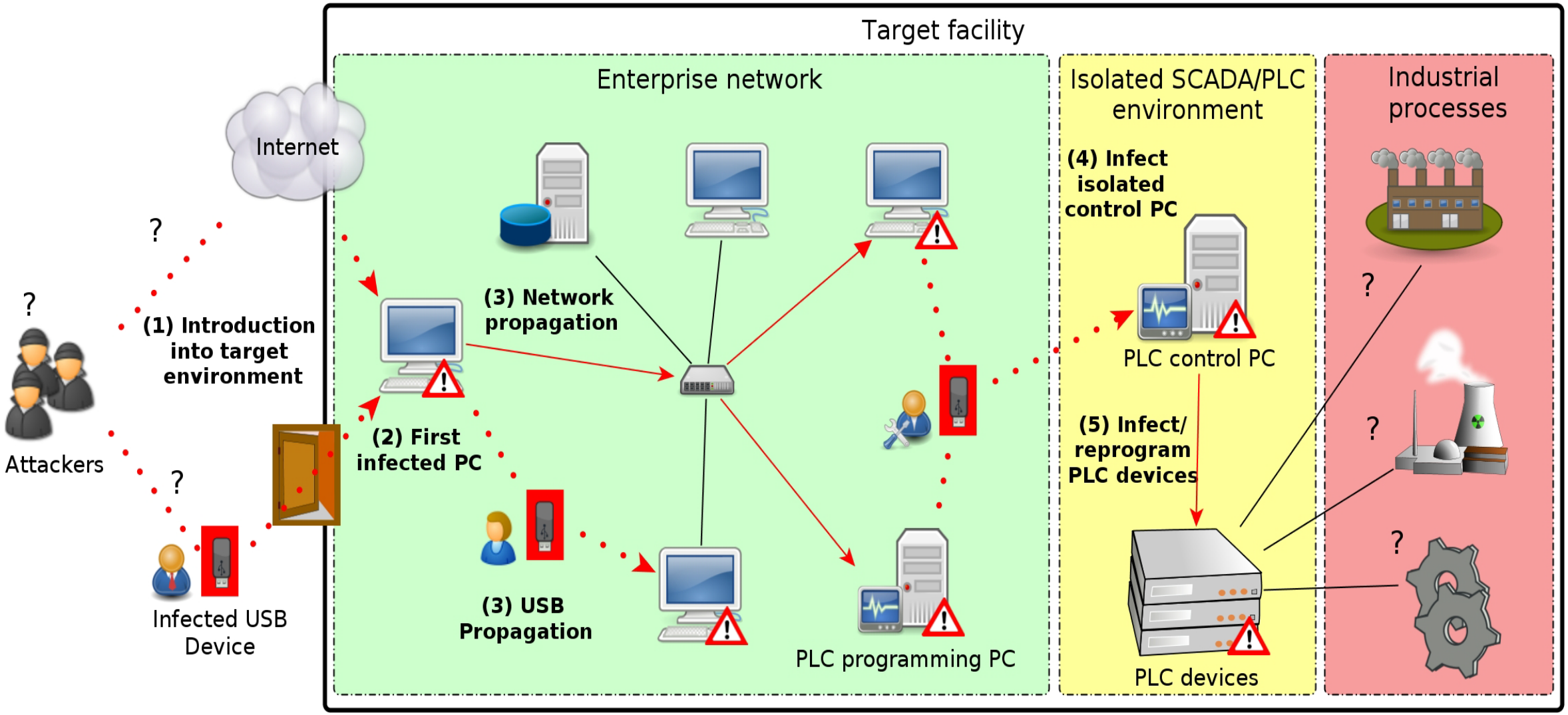
Anatomija Stuxnet napada

- Stuxnet koristi **višestepeni vektor napada** za dostizanje krajnjeg cilja.
- **Cilj**: upravljanje programabilnim logičkim kontrolerima koji se koriste za kontorlu industrijskih procesa u okviru računarski kontrolisanih industrijskih sistema.
- Sutxnet je **VEOMA precizan**!
  - Rootkit ovog crva, dizajniran je originalno da napada isključivo sistem SCADA (*Supervisory Control and Data Acquisition*) koji proizvodi kompanija Siemens.
  - Napada se deo koda ovog sistema koji se naziva Operacioni blok 35.
  - Ova komponenta zadužena je za kontrolu procesa i očekuje brzinu odgovora za 100 milisekundi.
- Bilo koja (čak i najmanja izmena) može da dovede do katastrofalne eksplozije kontrolisanog sistema!

Anatomija Stuxnet napada

- Proces širenja Stuxnet-a može se, grubo, podeliti u dve faze, od kojih je svaka realizovana na osnovu različite funkcionalnosti crva.
  - Prva faza predstavlja širenje crva u okviru jedne ili više različitih mreža.
  - Druga faza predstavlja sam proces infekcije izolovanog industrijskog sistema.
- U drugoj fazi se pravi razlika između infekcije Windows računara korišćenih za programiranje i samih PLC uređaja.
- Na taj način se dobija interfejs između računarskih sistema i kontrolisanih industrijskih procesa, što i jeste krajnji cilj Stuxnet-a.

Anatomija Stuxnet napada



Anatomija Stuxnet napada

- Pretpostavlja se da proces širenja i infekcije sadrži pet faza

1. Crv je na izvestan način implementiran u ciljno okruženje (najverovatnije preko USB memorije, što još uvek nije zvanično potvrđeno).
2. Nakon toga inficira se prvi računar.
3. Crv se dalje širi preko određenog tipa mreže, USB memorije i zaraženih fajlova iz projekta PLC programiranja.
4. Crv se širi sve dok se ne inficira računar koji upravlja PLC sistemom.
5. Otkrivanjem specifične kombinacije procesa operativnog sistema, kontrolnog softvera i PLC sistema, Stuxnet modifikuje softver za PLC programiranje i napokon inificira sam PLC sistem, čije se funkcionalnosi sada mogu lako modifikovati.
   - Ovo se može iskoristiti za manipulisanje fizičkim industrijskim procesima koje PLC uređaji kontrolišu!

Faze napada

- Infekcija Windows sistema.
  - Trojanski deo Stuxnet-a (dva drajvera) + Rootkit komponenta.
  - Zero-day-attack.
- Infekcija Step 7 softvera.
  - Jednom instaliran na bilo koju Windows platformu, inficira fajlove koji su deo Siemens-ovog WinCC/PCS 7 SCADA kontrolnog softvera.
  - Podriva ključnu komunikacionu biblioteku WinCC-a.
  - To omogućava da se presretne komunikacija između WinCC softvera, koji radi pod Windows-om i ciljnog Siemens PLC uređaja.
  - Na taj način, crv može sam da se instalira na PLC uređaj potpuno neprimećen, a zatim maskira svoje prisustvo.

Faze napada

- Infekcija PLC sistema uređaja.
  - Napad se vrši na PLC sisteme sa uređajima promenljive frekvencije koji su prizvedeni od strane dva specifična proizvođača: Vacon, Finska i Fararo Paya, Iran.
  - Nakon toga prati se frekvencija povezanih motora i vrši napad isključivo na sisteme koji rade između 807Hz i 1210Hz.
  - Industrijske primene motora sa ovim parametrima: raznovrsne pumpe, centrifuge gasa .
  - Stuxnet se instalira u memorijski blok PLC sistema koji se naziva DB890, a koji posmatra Profibus messaging bus sistema.
  - Kada su ispunjeni određeni kriterijumi, dolazi do periodične modifikacije frekvencije na 1410 Hz, pa na 2Hz, pa na 1064 Hz i na taj način se utiče na rad motora povezanih na PLC sistem odnosno, menja se njihova rotaciona brzina.
  - Takođe, automatski se instalira Rootkit, koji maskira i sakriva Stuxnet i ujedno modifikuje rotacionu brzinu sitema za nadgledanje.

Par napomena o Stuxnet-u

- Po mnogo čemu razlikuje od ostalih malwarea: glavni cilj je potpuno drugačiji.
- Pisan je u nekoliko programskih jezika, pa stručnjaci smatraju da je na njemu radila čitava grupa ljudi, iza koje stoji veoma jaka organizacija.
- Gotovo 60% računara zaraženih Stuxnet-om nalazi u Iranu (nešto više od 30.000)
- Crv je imao svoju specifičnu metu: centrifuge koje rotiraju nuklearne materijale u iranskim postrojenjima za obogaćivanje uranijuma
- *Institute for Science and International Security* pretpostavlja da bi Stuxnet mogao biti zaslužan za isključivanje 1.000 centrifuga u iranskom glavnom nuklearnom postrojenju, Natanzu, 2010.
- Mnogi ugledni stručnjaci smatraju da je suština generisanja Stuxnet-a upravo za veoma inteligentnu i moćnu operaciju protiv Irana.
- Ko stoji iza Stuxnet-a? Dve zemlje na koje se najviše sumnja su Izrael i SAD.

Zaštita od zlonamernih programa

- **Bolje sprečiti nego lečiti**!
- Obavezno napravite **plan akcije** za slučaj da dođe do „zaraze“.
- Redovno pravite **rezervne kopije** važnih podataka ili arhivirajte ceo sistem.
- Instalirajte i redovno ažurirajte odgovarajući **zaštitni softver**.
- Pažljivo proverite **programe koje instalirate**.
- Budite oprezni od koga uzimate fleševe i USB HDD.
- Vodite računa o tome koje **Web lokacije** posećujete i šta sa njih **preuzimate**.
- Ne dozvolite pokretanje **sumnjivih programa** (ili ih pokrenite u karantinu).

Literatura

1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić (2007): Sigurnost računarskih sistema i mreža. Mikro knjiga, Beograd.

Hvala na pažnji

Pitanja su dobrodošla.