Sigurnosne prijetnje na Internetu

Povijest zlođudnog koda

Lea Faber, 13.11.2024.

Pregled predavanja

- Pitanja za ispite
- Motivacija
- Zlođudni kod
- Primjeri zlođudnog koda kroz povijest
- Zaključak

Pitanja za ispite

- Navedi i opiši jedan virus iz rane faze zlućudnog koda
- Navedi i opiši jedan virus iz rane Windows faze zlućudnog koda
- Navedi i opiši jednog mrežnog crva
- Navedi i opiši jedan rootkit ili ucjenjivačkog zlućudnog koda
- Navedi i opiši jedan primjer virtualne špijunaže i sabotaže

Motivacija

- Razvoj i napredak bilo kojeg tehnološkog područja za sobom nosi rizik iskorištavanja istog u maliciozne svrhe
- Jesu li svi zlćudni kodovi originalno imali zlćudnu namjeru?

Zlođudni kod

- Ciljevi:
  - Ometanje rada računala
  - Prikupljanje osjetljivih informacija
  - Dobivanje pristupa računalnom sustavu

- Virusi, crvi, trojanski konji, rootkitovi, keyloggeri, spyware…
  - Većinu aktivnih prijetnji čine crvi i trojanci

Povijesne kategorije zlođudnog koda

- Rana faza zlođudnog koda
- Rana Windows faza
- Evolucija mrežnih crva
- RootKit-evi i ucjenjivački zlođudni kod
- Virtualna špijunaža i sabotaža

Rana faza zloćudnog koda - Brain.A

- Zloćudni kod za PC koji se pojavio 1986.
- Virus “Brain.A” - razvijen u Pakistanu, dva brata
- Željeli dokazati da PC nije sigurna platforma
- Virus se replicirao koristeći diskete
- Zarazio bi boot sektor upravljačkog programa disketa na PC-u i sam booting sektor svake umetnute diskete

Rana faza zločudnog koda - Brain.A

- Umetnuta zaražena disketa bi zarazila upravljački program, koji potom zarazio bi sve nove umetnute diskete
- Virus nije nanosio štetu, cilj je bio samo ukazati na problem

Rana faza zloćudnog koda

- Omega virus
  - Benigan ako nije petak 13. - tada ne dozvoljava boot PC-a
- Michelangelo virus
  - 1992. na Michelangelov rođendan, onemogućio bootanje PC-a
- V-sign virus
  - Zarazio bi boot sektor, svaki mjesec na ekran napisao znak “V”
- Walker virus
  - 1992., svakih 30 sekundi prikazala bi se animacija hodača s jedne na drugu stranu ekrana. Tijekom “hoda” nije se moglo upisivati ništa.

Rana faza zloćudnog koda

- Ambulance virus
  - Slično walkeru, samo što je prelaženje s jedne na drugu stranu popraćeno i zvukovima kola hitne pomoći
- Casino virus
  - Kopira tablicu alokacije datoteka u memoriju te briše originalnu
  - Prikazuje se igra u kojoj korisnik ima 5 pokušaja dobiti 3 £ znaka
    - Ne uspije li ili restarta li PC, tablica se gubi i PC se više ne može bootati
    - Uspije li, tablica se kopira na svoje staro mjesto i PC se može normalno koristiti

Rana faza zločudnog koda

- Mutation engine (MtE)
  - Alat za dodavanje mutacijskih funkcionalnosti virusima
  - Za težu detekciju anti-virus sustava

- Virus creation laboratory
  - Prvi UI alat za stvaranje virusa

Rana Windows faza

- WinVir
  - Prvi Microsoft Windows virus
  - Zarazio bi izvršne datoteke - radio male promjene
  - Replicirao se i nije stvarao veliku štetu
  - Kada bi se zarazila druga datoteka, virus bi se izbrisao iz originalne koja ga je aktivirala

Rana Windows faza

- One-half (Slovak bomber)
  - Napada glavni zapis za podizanje sustava
  - Kriptira datotečni sustav XOR funkcijom i ključem poznatim virusu
  - Ne napada datoteke koje u nazivu sadrže određene riječi jer moguće pripadaju nekom antivirusu koji će to “uhvatiti” auto-checking algoritmom
  - Na korisnikov pristup datoteci datoteka se dešifrira i ne primjećuje razliku
  - Problem nastaje neprikladnim brisanjem virusa gdje kriptirane datoteke ostaju kriptirane

Rana Windows faza

- Concept
  - Prvi makro virus - MS Word makro
  - Širio se dijeljenjem dokumenta kompjuterima s instaliranim Wordom
  - Kada je dokument bio otvoren, maliciozna šablona bi postala glavnom šablonom svakog novog Word dokumenta nastalog na tom PC-u
- Laroux
  - Prvi MS Excel makro virus - napisan u Visual Basic-u
  - Nije stvarao štetu, samo se replicirao

Rana Windows faza

- Boza
  - Virus namijenjen specifično za Windows 95
  - Napadao izvršne datoteke
  - Kada bi se zaražena datoteka pokrenula, zarazile bi se jedna do tri datoteke u njenom direktoriju i pokrenuo originalni program
  - Nije bio destruktivan, ali pod određenim okolnostima zaražene datoteke bi mogle narasti do nekoliko megabyte-a
  - Svakog 31. u mjesecu bi prikazao prozor s porukama:
    - “The taste of fame just got tastier!”
    - “From the old school to the new”

Rana Windows faza

- Happy99
  - Prvi e-mail virus
  - Širio se kao EXE privitak u e-mailu
  - Na pokretanje korisnik bi vidio vatromet, a virus bi se replicirao i poslao svim korisnikovim kontaktima
- Melissa
  - Zaraženi MS Word privitak u mail-u
  - Pri otvaranju bi se replicirao u nasumičnu datoteku na korisnikovom tvrdom disku i poslao ju svim kontaktima
  - Najveći problem je širenje korisnikovih informacija
  - Nekad dodavao citate iz Simpsona u zaražene datoteke

Rana Windows faza

- LoveLetter
  - Najuspješniji virus društvenog inženjeringa
  - Privitak se činio kao ljubavno pismo
  - Virus bi modificirao neke dosta bitne datoteke sustava
  - Uzrokovao štetu od 5.5 mlrd. dolara
- Anakurnikova
  - Slao EXE datoteku, a uvjeravao žrtve da su to eksplicitne slike Ane Kurnikove

Mrežni crvi

- Robert Tappan Morris
  - student na MIT-u 1988.
- Želio pobrojati računala spojena na internet
- Napravio mali program koji se replicira s jednog spojenog kompjutera na drugi i brojao
- Bug: crv posjećivao već posjećene PC-eve
  - stvorilo veliki promet koji je skoro srušio tadašnji internet
- Prva osoba uhićena zbog računalne zlouporabe

Mrežni crvi

- Svi kompjuteri su prije imali otvorene portove, spajanje i replikacija mogla je biti postignuta bez korištenja eksploata

Mrežni crvi

- Code Red
  - Prvi crv nakon Morrisa koji nije trebao interakciju s korisnikom
  - Prvi namjerno napravljen crv
  - 2000. godine se u par sati proširio cijelim svijetom
  - Uspješno zaobilazio obrambene mehanizme
  - U prvih 19 dana se samo širio mrežom koristeći ranjivost u IIS-u.
  - Od 20. do 27. dana je pokrenuo DoS napad na par web stranica
    - pr. Whitehouse

Crvi

- Fizzer
  - Mail crv iz 2003.
  - Prvi maliciozni kod kojem je jedina svrha bila zarada
  - Zaraženi privitak je računala pretvarao u pošiljatelje spama
- Blaster
  - Koristio buffer overflow ranjivost DCOM RPC-a
  - Stvoren za SYN preplavu windowsupdate.com stranice
    - Prava stranica je bila windowsupdate.microsoft.com, pa nije puno naštetilo
    - Ali zbog velikog prometa usporio je neke usluge, npr. Air Canada

Mrežni crvi

- Slammer
  - Koristio ranjivosti Microsoft SQL Severa i MS Data Enginea
    - Svaka aplikacija koja je koristila jednu od ovih usluga je bila potencijalna meta i ulaz Slammeru
  - Nije ništa pisao na tvrdi disk, širio se kao memorijski proces
    - Na restart bi se izbrisao, ali zbog umreženosti PC bi se opet zarazio
  - Stvarao veliki mrežni promet - puno izgubljenih paketa
  - Uzrokovalo rušenje mnogih usluga:
    - ATM mreža američke banke
    - 911 usluga u Seattle-u
    - Kontrola leta na aerodromima
    - Stvaralo probleme nuklearnoj elektrani u Ohio-u

RootKit-evi

- RootKit
  - Zloćudni alat koji mijenja postojeće programe operacijskog sustava tako da napadač može nastaviti pristupati računalu i skrivati se na istom
  - Prvi nastao 1999.
- User-mode RootKit
  - Djeluje na programe koje pokreću korisnici i administratori
- Kernel-mode RootKit
  - Djeluje na jezgrene funkcije i programe

RootKit-evi

- SONY BMG RootKit
  - Nastao 2005. godine, utjecalo na SONY-jev ugled
  - Ideja je bila detektirati i onesposobiti kopiranje njihovih publikacija putem drugih medija
  - Npr. ako bi se njihov CD album umetnuo u discman-a ili normalan CD player ništa se ne bi desilo. Ali u slučaju umetanja u PC RootKit bi se instalirao i sakrio u sve sys datoteke i kontrolirao kako korisnik pristupa glazbi - ako se pokuša kopirati RootKit bi to spriječio
  - Thomas Hesse, direktor globalne prodaje SONY BGM-a
    - "Most people, I think, don't even know what a rootkit is, so why should they care about it?"

RootKit-evi

- StormWorm
  - Crv koji se širio putem maila s pomoću društvenog inženjeringa
  - Neki od naslova:
    - "230 dead as storm batters Europe"
    - “British Muslims Genocide”
    - “Naked teens attack home director.”
    - “Radical Muslim drinking enemies's blood.”
  - Zaražena računala su činila botnet mrežu
  - Kontrolni čvor se mogao mijenjati
  - Instalirao se i RootKit na zaraženo računalo

RootKit-evi

- Mebroot (2008.)
  - Žrtva se mogla zaraziti samo surfajući internetom preko ranjivosti u pregledniku
  - Službena stranica Monice Belluci je bila jedna od prvih stranica koja je širila ovaj virus
  - Kada je dobio pristup PC-u instalirao bi RootKit koji se mogao skrivati od RootKit detektora
  - Pratio je što žrtva tipka i slao te podatke napadaču
  - Dobro debugiran - nikad nije uzrokovao pad sustava
    - I da je pao sustav, poslao bi podatke o tome napadaču koji je mogao ispraviti taj problem što je činilo taj zloćudni kod znatno naprednijim

RootKit-evi

- Conficer
  - Koristio ranjivost u Windowsima i otkrivene slabe lozinke za širenje
  - Instalirao backdoor, rootkit i napravio računalo botnet čvorom
  - Oko 10 milijuna zaraženih računala stvaralo jako kompleksnu botnet mrežu
  - Nikad nije bilo korišteno za ikakav napad - namjera nije nađena

Ucjenjivački zlćudni kod (ransomware)

- Maliciozni kod koji je kriptirao žrtvine podatke, i prikazivao joj poruku na radnoj površini u kojoj zahtjeva novčanu svotu za povrat podataka
- Širili su se putem ranjivosti preglednika i PDF datoteka sa skriptama za preuzimanje i instalaciju zlćudnog koda
  - Na radnu površinu bi bila postavljena how-to-decrypt.txt datoteka

Virtualna špijunaža i sabotaža

- Od 2010. zlćudni kod smatra se oružjem
- SAD smatra da je uzvraćanje bombardiranjem za cyber napad ravnopravna mjera
  - Zlćudni kod može napraviti štetu iste razine kao i bomba, ali bez direktnog riskiranja ljudskog života

Virtualna špijunaža i sabotaža

- Stuxnet
  - Otkriven u lipnju 2010., već se širio oko godinu dana neotkriven
  - Kad je otkriven već je izvršio namjeru za koju je napravljen
  - Cilj mu je bio uništiti ili barem usporiti iranski nuklearni program
  - Fizički je sabotirao turbine za obogaćivanje urana promjenom frekvencije njihove rotacije.
  - Širio se preko USB-a, a novi USB-ovi bi postali zaraženi kada bi se umetnuli u zaraženi PC
  - Koristio RootKit da bi se sakrio na zaraženom računalu

Virtualna špijunaža i sabotaža

- DoQu
  - Baza koda slična Stuxnet-u, vjeruje se da imaju istog autora
  - Koristio iste eksploate kao i Stuxnet, ali za drugu svrhu
  - Služio je za prikupljanje podataka o žrtvama
  - Špijunirao je zaražena računala

Virtualna špijunaža i sabotaža

- Flame
  - Najkompleksniji zloćudni kod ikad viđen, otkriven 2012.
    - Vjeruje se da su ga napravili Izrael i SAD
  - Većina zaraženih računala na bliskom i srednjem istoku
  - Modularan, napadač može njime upravljati na daljinu i dodavati nove module
  - Širio se preko USB-a ili internetskom mrežom te se skrivao
  - Mogao snimati zvuk, video, Skype pozive, aktivnost mreže, krasti i slati datoteke napadaču
  - Kada su antivirus firme dobile primjerak na analizu, sve instance Flame-a bile su uništene remote kill komandom

Zaključak

- Razvoj zlućudnog koda eksponencijalno napreduje
- Treba se educirati o obrani i načinima zaraze te posljedicama potencijalnog napada

Literatura

- Milošević, Nikola. "History of malware." arXiv preprint arXiv:1302.5392 (2013).
- https://www.fortinet.com/blog/threat-research/evolution-of-malware
- https://www.youtube.com/@danooct1 - prikaz rada zlođudnog koda

Hvala!