Inspiratron.org - Natural language processing, machine learning and cybersecurity

Malware - klasifikacija i istorija

by Nikola Miloševi? - Monday, November 12, 2012

https://inspiratron.org/blog/2012/11/12/malware-klasifikacija-i-istorija/

S obzirom da mnogo ljudi ima razli?ite probleme sa virusima i malware-om, jako je važno upoznati se sa osnovnim konceprima na kojima virusi i malware rade. Istorijski gledano virusi su sa nama ve? oko 30 godina. Za to vreme došlo je do izuzetno velike evolucije. Tako?e došlo je i do izvesnih promena u strukturi ljudi koji se bave razvojem virusa. Kada je sve po?elo ljudi su razvijali viruse iz egzibicijonizma. Jedan od prvih virusa, koji nosi ime Brain je razvijen recimo kao proof of concept da su PC ra?unari loši i razvili su ga dvojca iskrenih poklonika main frame ra?unara. Malware je imao razli?ite oblike od igara na sre?u do malicioznih programa koji su ometali korisnika u radu. Me?utim vremenom se otvorio prostor za zaradu putem špijunskog malware-a, gde su autori mogli da pamte korisni?ke šifre i lozinke ljudi zaraženih mašina. Ovo je potpuno izmenilo strukturu razvija?a, od egzibicionista i hackera koji su želeli da pokaži šta umeju do kreiranje podzemlja. Ljudi iz ovog podzemlja su finansijski jako dobro obezbe?eni, pa i sposbni da zaposle grupe programera koji ?e raditi na razvoju novog malware-a. Na ovaj na?in se ceo proces iskomplikovao, me?utim i antivirusne kompanije prate ove trendove i imaju svoje odgovore. Poslednjih nekoliko godina su krenuli da se pojavljuju malwari ?iji autori su vojske i obaveštajne agencije pojedinih mo?nih država sveta. Tako su se pojavili virusi poput Flame, Doqu (USA, Izrael), Quellen TKU (Nema?ka policija)...

Na po?etku bi bilo dobro definisati i klasifikovati malware. Malware je program ili deo programskog koda koji izvršava odre?enu neodobrenu i nepoželjnu akciju na ra?unaru žrtve.

Malware možemo klasifikovati na slede?i na?in:

Virus - Potrebna mu je datoteka koja ?e biti host. Ovaj malware ima sli?nosti sa medicinskim virusom i zato se i tako zove. Zarazi host datoteku, sam se replicira i ume?e se u druge datoteke odre?enih dipova. Obi?no su na meti .exe, .com i . dll datoteke. Ubacuje se uglavnom na po?etak izvršnog koda ili se dodaje kod na kraju, ali se u zaglavlju datoteke referencira kod. Obi?no mi je potrebna interakcija

sa ?ovekom kako bi se razširio poput otvaranja datoteke ili izvršenja neke komande u programu.

Worm - na srpskom crv. Širi se kroz mrežu. Obi?no koristi neku ranjivost sistema kako bi uspeo da do?e do odre?ene mašine i zarazi je. Tako?e, u sebi mora imati algoritam za nalaženje novih potencijalnih žrtvi ra?unara, pa tako je obi?no u mogu?nosti da skenira mrežu i proverava da li sistem na mreži poseduje odre?eni ranjiv software za koji crv ima eksploit. Kada u?e u sistem pomo?u sigurnostnog propusta ostavlja payload ili programski kod koji ?e se izvršavati na zaraženoj mašini, što može biti odre?eni špijunski software ili bilo šta drugo i nastavlja sa te mašine da skenira mrežu, kako bi se dalje replicirao. Ovaj tip malware-a se jako brzo širi, osobito ako poseduje neki 0-day exploit ili ranjivost koja još nije otkrivena i ispravljena od strane programera i bezbednostnih eksperata. Tako?e ovaj malware ne zahteva interakciju sa ?ovekom.

Primeri poznatih crva su:
Morris Worm, Code Red, SQL Slammer

Malicious mobile code - Maliciozni mobilni kod. Sastoje se od laganih programa koji se downloadoju kako bi se izvršili na udaljenom sistemu, odnosno sistemu žrtve sa minimalnom interakcijom korisnika.Obi?no su napisani u JavaScript-u, VBScript-u, Javi ili ActiveX. Da bi se žrtva zarazila dovoljno je da otvori odre?enu web stranicu ili da otvori zaraženi Office dokument. Krajem '90 su naro?ito bili popularni malware-i pisani u VBScriptu koji su se širili putem zaraženih office dokumenata. Danas tako?e vi?amo dosta na internetu Cross Site Scripting ranjivosti na web stranama koje mogu biti iskoriš?eni za ovaj napad.

Backdoor - Zadnja vrata. Ovaj malware daje napada?u pristup udaljenom ra?unaru žrtve, bez teškog prolaza korz bezbednosne kontrole. ?esto napada?i ukoliko pro?u sigurnosne kontrole uz pomo? nekog ekspolit-a prvo što urade je instalacija odre?enog backdoor alata, kako bi kasnije nesmetano mogli da se vrate i koriste taj sistem. Poznati alati su Netcat i Virtual Network Computing (VNC), koji oba mogu legitimno da budu koriš?eni i kao alati za udaljenu administraciju, kao i nelegitimni napada?ki alati za backdoor.

Trojan horse - Trojanski konji. Predstavljaju se kao korisni programi ili odre?ene igre, ali u sebi sadrže maliciozan sakriven kod. Obi?no se pokretanjem applikacije korisniku otvori zaista odre?ena igra ili koristan program, ali paralelno se i zarazi ra?unar i instaliraju odre?eni napada?ki alati poput zadnjih vrata ili špijunskog software-a, keylogger-a i sli?no.
Poznati trojanski konji su:
Setiri, Hydan

User-level RootKit - RootKit korisni?kog nivoa. Menja ili modifikuje programe koje se koriste za sistem administraciju ili za upravljanjem sistema od strane korisnika. Izvršenjem zaražene komande se obavljaju još odre?ene malicijozne radnje na sistemu. ?esto zaražena komanda je ls komanda na linux sistemima, jer se ona gotovo naj?eš?e koristi. Poznati RootKit korisni?kog nivoa su:
Linux RootKit (LRK) family, Universal RootKit, FakeGINA

Kernel-level RootKit - RootKit nivoa jezgra sistema. Ovo je jedan od najopasnijih vrsta malware-a, jer ga je nemogu?e obrisati i detektovati. Jedini na?in kako da se odstani iz sistema je ?esto formatiranje i reinstalacija operativnog sistema. Manipuliše srcem operativnog sistema, kernelom, i instalira se obi?no kao odre?eni driver ili modul. Sakriva druge alate poput zadnjih vrata ili špijunskog software-a. S obzirom da se nalazi u jezgru operativnog sistema manipuliše izlazom koje operativni sistem daje. Pa tako ni na kakav na?in nije mo?i prona?i servise, procese ili datoteke koje krije. Na ovaj na?in ni anti virusi ne?e mo?i da detektuju malware jer ih operativni sistem laže. ?esti su za Linux operativne sisteme, dok zbog zatvorenosti Windows sistema su re?i.
Poznati:

Adore, Kernel Intrusion System

Combination malware - Malware kombinacije kombinuli osobine opisanih malware, kako bi popoljšali efektivnost. Neki od poznatih su: Lion, Bugbear.B

Interesantno za prou?avanje malware-a je i istorija razvoja razli?itih klasa malicijoznog koda. Sve je po?elo po?etkom 80tih godina 20. veka, a danas je aktivan ovaj razvoj više nego ikad i verovatno se ne?e zaustaviti sa napredkom tehnologije. Osobito zbog toga što danas sve više postrojenja, infrastrukture zavise od ra?unara, pa tako malware predstavlja jako oružje za diverziju, bez rizikovanjua života ljudi ili tehnike. Evo kratkog pregleda:

- 1981–1982—Prvi ra?unarski virusi. Najmanje tri razli?ita virusa uklju?uju?i Elk Cloner su bili na?eni u igrama za Apple II ra?unarske sisteme, iako re? virus nije u to vreme bila iskoriš?ena za imenovanje ovih pojava.
- 1983—Formalno se definiše ra?unarski virus: Fred Cohen definiše ra?unarski virus kao program koji može da inficira druge programe modifikuju?i ih da uklju?e, mogu?e i evoluiraju?u, verziju sebe.
- 1986—Prvi PC virus: Takozvani Brain virus inficirao je Microsoft DOS sisteme. Ovo je važan korak za viruse, kako ?e kasnije Microsoft DOS i kasnije Windows platforme postati primarna meta virusa i crva zbog svoje popularnosti i velike zastupljenosti.
- 1988—Morrisov internet crv. Napisan od strane Roberta Tappan Morisa Mla?eg, kao student MIT, novembra 1988. Crv je trebalo da prebroji ra?unare povezane na internet u to vreme. Me?utim crv je imao grešku da se replicirao i na ra?unare na kojima je ve? bio. Na taj na?in je uspeo da zaguši ve?inu interneta tog vremena, što mu je donelo naslovne strane u novinama širom sveta.
- 1990—Prvi polimorfni virusi: Kako bi izbegli detekciju od strane antivirusnih sistema, koji su uglavnom radili na principu baze potpisa poznatih virusa, koji su se dobijali hashiranjem koda virusa, ovi virusi su menjali svoj oblik prilikom svake replikacije. U po?etku su menjali odre?ene stringove ili imena promenljivih. Ovakvi virusi su i danas tema mnogih istraživanja.
- 1991—Virus Construction Set (VCS) Objavljen: U martu, ovaj alat je dao novim razvija?ima virusa jednostavan alat za kreiranje custom malware koda. Pojavio se na bulletin board sistemima i forumima u to vreme
- 1994—Good Times Virus Hoax: Ovaj virus nije napadao ra?unare. Bio je kompletno fikcioni. Me?utim, uplašeni ljudi su prenosili usmeno od ?oveka do ?oveka. Govorilo se o jakim strašnim posledicama zaraze ovog izmišljenog virusa.
- 1995—Prvi Macro Virusi: Ova izuzetno gadna vrsta virusa se pojavila u po?etku implementirana u Microsoft Word makro jezicima, koji su zaraživali dokument datoteke. Kasnije ovi virusi su se proširili i na makro jezike drugih programa. Virus se naj?eš?e startova prilikom otvaranja Office dokumenata.
- 1996—Netcat objavljen za UNIX: Ovaj alat je napisan od strane Hobbit-a i postao je najpopularniji backdoor alat za UNIX sisteme do danas. Iako ima mnogo legitimih upotreba, Netcat se ?esto zloupotrebljava kao backdoor alat.
- 1998—Prvi Java Virus: StrangeBrew virus je inficirao druge Java programe, donose?i brigu o virusima u svet applikacija baziranih na Webu.
- 1998—Netcat objavljen za Windows: Napisan od strane Weld Pond, koristi se kao ekstremno popularan backdoor za Windows sisteme tako?e.
- 1998—Back Orifice: Ovaj alat je objavljen u Julu od strane hackerske grupe Cult of the Dead Cow (cDc). Omogu?avao je udaljenu kontrolu Windows sistema preko mreže.
- 1999—Melissa Virus/Worm: Objavljen u martu, ovaj makro za Microsoft Word zarazio je hiljade ra?unara širom sveta šire?i se pomo?u e-maila. Bio je zapravo i virus i crv, pošto je napadao dokument datoteke i širio se kroz mrežu.
- 1999—Back Orifice 2000 (BO2K): U Julu, cDc je objavila ovu komepletno prepisanu verziju Back Orifice za udaljenu kontrolu Windows sistema. Nova verzija eje posedovala primamljiv interface (point-and-click) i programerski interfejs (API) za proširivanje funkcijonalnosti, kao i kontrolu miša, tastature i ekrana.
- 1999—Distribuirani Denial of Service Agenti: U kasno leto, Tribe Flood Network (TFN) i Trin00 denial of service agenti su objavljeni. Ovi alati su pružaliu napada?ima kontrolu nad stotinama ili hiljadam ra?unara sa instaliranim zombi procesima preko jedinstvene klijenske aplikacije. Sa centralizovanom ta?kom koordinacije, ovi distribuirani agenti su mogli da pokrenu izuzetno jake napade poplavom.
- 1999—Knark Kernel-Level RootKit: U Novembru, osoba sa pseudonimom Creed je objavio alat kreiran na nazi predhodnih ideja za kernel manipulaciju Linux sistema. Knark je obuhvatio set alata za prilago?ivanje Linux kernela, pa je napada? mogao biti jako efikasan u sakrivanju datoteka, procesa i mrežne aktivnosti.
- 2000—Love Bug: U maju, ovaj VBScript crv je ugasio desetine hiljada sistema širom sveta, kako se širio uz pomo? nekoliko slabosta u Microsoft Outlook-u.
- 2001—Code Red Crv: U julu se ovaj crv širio uz pomo? buffer overflow ranjivosti u Microsoft IIS Web serveru. Preko 250 000 mašina je bilo žrtva ovog crva za manje od 8 ?asova.
- 2001—Kernel Intrusion System: Tako?e u julu, ovaj alat od Optyx je revolucionizirao manipulaciju Linux kernela uklju?uju?i lak za koriš?enje grafi?ki interfejs i izuzetno efikasne mehanizme za sakrivanje.
- 2001—Nimda Crv: Nedelju dana pre teroristi?kog napada 11. septembra, pojavio se ovaj jako razširen virus koji je inficirao Windows mašine brojnim metodama poput buffer overflow web servera, exploita za web browsere, Outlook email napadima i uz pomo? file

shareing.
- 2002—Setiri Backdoor:Iako nikad formalno objavljen, ovaj trojanac je mogao da pro?e li?ne firewall, mrežne firewall, Network Address Translation ure?aje ponašaju?i se kao nevidljivi browser.
- 2003—SQL Slammer Crv: Januara 2003, ovaj crv se proširio jako brzo, gase?i nekoliko internet servis provajdera u Južnoj Koreji i poprili?no prave?i probleme širom sveta.
- 2003—Hydan Executable Steganography Tool: U februaru, ovaj alat je omogu?io korisnicima mogu?nost da sakriju podatke u programima koriste?i polimorfi?ke tehnike programiranja na Linuxu, BSD i Windows. Ovaj koncept je tako?e mogao da se proširi za antivirus i intrusion detection sisteme.

Bitno je pomenuti još dve tehnike za sakrivanje virusa koji su se razvili tokom vremena. Jedna tehnika, je ranije pomenut **polimorfizam**. U ovoj tehnici se menja potpis virusa, tako što se prilikom replikacije koristi inicijalni kod, menjaju imena promenljivih i onda se kompajlira i replicira. Na ovaj na?in potpis ne?e biti isti. Me?utim struktura koda se mnogo ne menja, pa su brzo razvijeni antivirusni alati koji su mogli da prepoznaju sli?ne kodove. U ovom slu?aju se inicijalni algoritam ne menja.

Druga metoda je **Metamorfizam**, koja je malo komplikovanija, u kojoj se menja struktura koda, pomeraju?i blokove i delove koda. Funkcijonalnost virusa uglavnom ostaje isti, ali se struktura koda mnogo više razlikuje nego kod polimorfizma.

Nikola Miloševi?