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

Kratka istorija malware-a | Prvi deo: Po?eci

by Nikola Miloševi? - Saturday, November 24, 2012

https://inspiratron.org/blog/2012/11/24/kratka-istorija-malware-a-prvi-deo-poceci/

Još jednom ?u se osvrnuti na istoriju malware-a, jer mislim da je tema izuzetno zanimljiva a i otkriva slika o tome gde smo nekad bili, kako je sve po?elo, kako se razvilo, gde smo danas i ka ?emu ?e se i?i u budu?nosti, kako u razvoju malware-a, tako i u borbi protiv njih. ?lanci o kratkoj istorij malware-a ?e biti podeljeni u 4 dela. Prvi ?e se odnositi na po?etke u uglavnom dos okruženju. Drugi deo ?e biti posve?en ranim Windows virusima. Dok ?e tre?i biti posve?en modernim spyware alatima, cybercrime sceni i dok ?e ?etvrti biti posve?en vojnoj upotrebi virusa.

Sve je po?elo sa **Brain.A**. Ovo je prvi PC virus iz 1986. Ovaj virus su napisali Basit i Amsat, dva tada mlada ?oveka iz Pakistana. U source kod su upisali svoje podatke,broj telefona, kao i adresu. Naravno, tada ih niko nije gonio, ali danas, 25 godina nakon toga što su napisali virus Miko Hypponen, glavni analiti?ar F-Secure-a je odlu?io da ih podtraži i pita zašto su napisali prvi virus u PC istoriji. Otišao je u Pakistan, na adresu upisanu u kodu Brain.A virusa i vrata su mu otvorili upravo Basit i Amsat. Trenutno oni vode internet provajdersku firmu koja se zove Brain telecommunications. Objasnili su Miku da je virus bio proof of concept. Naime, imali su pozadinu u svetu Unix-a i mainframe sistemima. Kada je došao PC i DOS, što se njima nije svidelo. Mislili su da nije bezbedan, kao što o?igledno nije bio. Odlu?ili su da to dokažu, tako što ?e napisati virus. Naravno nisu imali pojma da ?e virus obi?i svet i zaraziti ra?unare u preko 100 država sveta.

[youtube=http://www.youtube.com/watch?v=lnedOWfPKT0]

Virusi poput Brain.A su tipi?ni za period kasnih '80tih, kao i motiv autora. Oni nisu želeli ništa konkretno da postignu, ve? su hteli da probaju nešto i dokažu. Naprave svojevrstan proof of concept. Ve?ina njih se i širila na sli?an na?in. Zaraza je bila u boot sektoru diskete. Kada ubaci korisnik disketu njegov ra?unar se zarazi, kao i svaka slede?a disketa koju on ubaci. S obzirom da u to vreme nisu postojale mreže, ovo je bio najefikasniji na?in širenja. Neki ra?unari ?ak nisu imali ni hard disk, ve? samo 2 floppy drajava. Ve?ina ovih virusa je imalo i vizuelnu komponentu. Zaražena žrtva bi znala kad je zaražena, jer bi joj se odre?eni tekst ili animacija prikazala u konzoli.

Omega je bio virus koji je zarazio boot sektor. Me?utim, nije pravio mnogo štete do odre?enog datuma. Ukoliko bi bio petak 13. aktivirao bi na ekranu omega karakter.

Michelangelo virus 1992 prepisivao prvih 100 sektora hard diska i sistem nije mogao da se bootuje više.File allocation tabela bude uništena. Prepisivanje File allocation tabele se dešavalo ukoliko je ra?unar bootovan na godišnjicu ro?enja Michelangela. U suprotnom virus nije radio ništa

V-sign je inficirao boot sektor i jednom mese?no iscrtavao slovo V na ekranu.

Walker je slede?i virus koji se pojavio 1992. godine i koji je iscrtava hoda?a po kome je dobio ime na DOS konzoli s vremena na vreme i tako ometao korisnike.

Ambulance je virus jako sli?an Walker-u, ovaj virus je iscrtavao ambulantni auto kako prolazi ekranom. Me?utim ovaj virus je imao i zvu?ne efekte, odnosno mogla se ?uti sirena ambulantog auta.

Casino virus je igrao igru sa zaraženim korisnikom. Prilikom zaraze obrisao bi file alocation tabelu, me?utim ?uvao bi kopiju u memoriji. Pokretao bi jackpot igricu u kojoj igra? treba da dobije 3 znaka £, kako bi pobedio. Ukoliko igra? pobedi, virus je kopirao nazad iz memorije file alocation tabelu i korisnik je mogao da nastavio. Ukoliko ne, korisnik bi izgubio sve fajlove. Tako?e, prilikom restarta, pošto je file allocation tabela samo u memoriji, ona bi se potpuno izgubila i korisnik bi opet izgubio fajlove.

MtE - Mutation engine, napisan od strane bugarskog razvija?a virusa poznatog pod pseudonimom Dark Avenger. Radilo se o programu kome se mogao proslediti bilo koji virus, koji bi dodao novu funkcijonalsnot tom virusu da može da mutira, odnosno da ima funkciju polimorfizma. Do tada virusi su se pretraživali na ra?unarima isklju?ivo pomo?u potpisa. Ali ovaj nova funkcijonalnost je stvorila problem antivirusnim programima tog vremena, jer prilikom svake replikacije virus bi imao za nijansu druga?iji kod i samim tim i potpis. Tako?e mogao je kriptovati file virusa.

VCL - Virus Creation Laboratory - user interface za kreiranje virusa. U ovom trenutku je postalo poprili?no jednostavno i za script kiddies da naprave svoj virus. VCL je davao grafi?ki interfejs, gde su se mogle birati funkcionalnosti virusa i gde se sam virus mogao kreirati klikom na F9 ili Make padaju?i meni.

U ovo vreme po?inje da bude popularan i Windows. Kre?e veliki broj korisnika da ga koristi, a samim tim po?inje bezbednost windows-a i pravljenje virusa za windows da bude interesantna tema kreatorima virusa. Opširnije o ovome u drugom delu.

Nikola Miloševi?

- Kratka istorija malware-a | Peti deo: Neka rat po?ne
- Kratka istorija malware-a | ?etvrti deo: rootkit
- Kratka istorija malware-a | Tre?i deo: crvi (worms)
- Kratka istorija malware-a | Drugi deo: Windows era