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

Kratka istorija malware-a | Peti deo: Neka rat po?ne

by Nikola Miloševi? - Wednesday, January 09, 2013

https://inspiratron.org/blog/2013/01/09/kratka-istorija-malware-a-peti-deo-neka-rat-pocne/

Stigli smo i do poslednjeg posta u seriji o istoriji malware-a. Prošli smo po?etke, pozabavili se onim šta se desilo kad je izašao windows, pozabavili smo se makro virusima, mail crvima, mrežnim crvima, rootkitovima i najzad je došlo vreme da se pozabavimo najkompleksnijim malware-om do sad vi?enim. Ovih nekoliko malware-a, koje ?emo opisati su se pojavili u poslednjih nekoliko godina i gotovo u potpunosti promenili malware arenu. Naravno re? je Stuxnet-u, DoQu i Flame-u. Krenimo redom.

Stuxnet je prvi od supervirusa koji ?emo opisati. Otkriven je u junu 2010. godine, me?utim kada je otkriven došlo se do spoznaje da je malware u opticaju ve? bar godinu dana, a da nije detektovan. U trenutku kada je otkriven stuxnet je ve? obavio ono za šta je bio namenjen. Njegova namena, veruje se, je bila da uspori ili uništi Iranski nuklearni program. Stuxnet je to radio tako što je fizi?ki sabotirao uz pomo? menjanja frekvencija turbine za oboga?ivanje uranijuma. Tako?e, ovo je radio na vrlo prefinjen na?in. Kopirao se sa ra?unara na ra?unar uz pomo? USB stick-a. Nije pomagalo ukoliko je isklju?en autorun ili autoplay, ukoliko bi se zaraženi USB ubacio u ra?unar, ra?unar bi bio zaražen. Ni jedan antivirus nije bio sposoban da ga otkrije. Koristio je rootkit osobinu da se sakrije na zaraženoj mašini i ne bi radio ništa osim kopirao sebe na sve USB stickove koji se ubace u ra?unar. Za ulaz u ra?unar bi koristio 5 exploit-a, od kojih 4 u vreme otkrivanja su bili 0-day exploiti. Aktivirao bi svoje rutine samo ukoliko bi ra?unar bio priklju?en na odre?eni Siemens Step 7 kontroler i ra?unar služio za programiranje kontrolera. Tako?e ni tad ne bi radio ništa pametno, opet ukoliko taj kontroler ne bi bio priklju?en na ta?no odre?en sistem. U takvom slu?aju krenuo bi da menja frekvencije rada, a repreogramirao bi alate za automatsko reagovanje, tako da njima izgleda, kao da sistem radi savršeno dobro. Sadržao je i validan sertifikat, koji kada je black listovan u roku od dan je bio zamenjen drugim validnim sertifikatom. Imao je death date 24. jun 2012., kada bi sve instance Stuxneta sebe ubili i prestale da postoje. Veruje se da je ovaj malware, kao i ostali o kojima pišem u ovom postu kreirani od strane obaveštajnih agencija Sjedinjenih Ameri?kih Država i Izraela. Zvani?nici ovih država nikad nisu ni potvrdili ni demantovali ove tvrdnje. Za još informacija možete pogledati slede?a 2 videa:

[youtube=http://www.youtube.com/watch?v=gFzadFI7sco]

Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon

DoQu je malware, koji je imao sli?nu bazu koda kao i Stuxnet, tako da se predpostavlja da poti?u iz istog izvora, odnosno od istog kreatora. Tako?e se povezuju operacije Stuxnet sa operacijom DoQu. DoQu je koristio iste ranjivosti kao i Stuxnet, me?utim imao je druga?iju namenu. Njegova namena je bila pribavljanje informacija, odnosno špijuniranje zaraženih mašina. Napisan je u višim programskim jezicima. Naime, ve?ina malware-a je pisano u niskim jezicima poput asemblera, C, eventualno C++, ili nekog skript jezika poput Python, Lua i sl. DoQu je napisan u objektno orijentisanom C i veruje se da je koriš?en Visual Studio 2008 za njegovo kompajliranje.

Flame je najkompleksniji malware koji se do danas pojavio. Pojavio se u 2012. godini i najviše ra?unara je bilo zaraženo na bliskom istoku, pa se sa razlogom tako?e smatra da je nastao u obaveštajnim agencijama SAD i Izraela. Ovo je modularan malware, koji udaljeno može da kontroliše napada? i da dodaje nove module. Sa svim modulima mogao je da dostigne veli?inu i do 20MB. Flame je mogao da se širi preko USB-a ili preko mreže. Koristio je rootkit sposobnost da se sakrije na sistemu. Imao je mogu?nost da snima audio, video, skype pozive, mrežnu aktivnost, krade fajlove i šalje sve to napada?u. U trenutku kada su antivirusne kompanije pribavile samplove za analizu Flame malware-a poslata je komanda koja je uništila sve inkarnacije ovog malwar-a. Flame je napisan u Lua i C++, kao i Flame i DoQu i on je imao validan ukraden sertifikat. Na slici je prikazan broj detektovanih zaraženih ra?unara flame-om, detektovanim od strane Kaspersky laboratorija

Pojavom ovakvog malware-a kao što je Stuxnet, DoQu ili pak Flame, promenio se dosta na?in na koji pojimamo malware. U prvoj etapi egzibicionizam je bio pokreta? pravljenja malwara. U narednoj etapi pojavila se zarada, kao motiv koji su mnogi iskoristili za pravljenje malwara. Naravno ova zarada je dolazila na ilegalan na?in. U ovom trenutku, kao i u budu?nosti na malware možemo posmatrati kao na oružje. Ovo oružje ?e imati svakako dvostruku namenu, jedna je špijunaža, a druga je masovno uništenje i paraliza. Živimo u svetu gde sve više stvari zavisi od ra?unara i kontrolisani su razli?itim ra?unarima. Taj trend se nastavlja i u budu?nosti možemo o?ekivat još više sistema da se upravlja pomo?u ra?unara. Samim tim razorna mo? malware-a raste i potrebno je paziti na sigurnost svih tih sistema.

- Kratka istorija malware-a | ?etvrti deo: rootkit
- Kratka istorija malware-a | Tre?i deo: crvi (worms)
- Kratka istorija malware-a | Drugi deo: Windows era
- Kratka istorija malware-a | Prvi deo: Po?eci