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

Kratka istorija malware-a | Tre?i deo: crvi (worms)

by Nikola Miloševi? - Sunday, December 09, 2012

https://inspiratron.org/blog/2012/12/09/kratka-istorija-malware-a-crvi-worms/

Nastavljam sa malware serijom. U ovom delu ?emo se pozabaviti crvima, kao i nekim malware-om koji je imao ozbiljne posledice po infrastrukturu.

Prvi crv nije novijeg datuma, ve? je nastao 1988. godine. Napisao ga je Robert Tappan Moris, koji je bio u to vreme student na MIT-u. Njegova namera je bila da prebroji broj ra?unara na internetu. Me?utim napravio je grešku u programu, pa se crv replicirao ponovo i na one ra?unare na kojima je ve? bio. Na taj na?in je generisao veliki saobra?aj i gotovo onesposobio internet. Morris je bio prva osoba koja je osu?ena na osnovu ameri?kog zakona iz 1986. godine o ra?unarskom uznemiravanju (Computer Fraud and Abuse Act). Bitno je napomenuti da u to vreme nije bilo potrebno koristiti exploite da bi se ušlo na neki ra?unar, ve? se moglo jednostavno preko otvorenog porta pristupiti. Odnosno u ovo vreme još nije bio razvijen koncept sigurnosti na mreži.

CodeRed (2000) - CodeRed je prvi crv koji se širio, a da pri tome nije zahtevao nikakvu interakciju korisnika. Na taj na?in on se proširio svetom za nekoliko minuta. Skrivao se vešto od zaštita i imao je nekoliko funkcionalnosti koje su se odvijali u ciklusima. Napadao je IIS (Internet Information service). Prvih 19 dana u mesecu se širio mrežom. Od 20 do 27 dana lansirao je Denail of Service napade na nekoliko sajtova me?u kojima je bio i sajt Bele ku?e. Poslednjih dana meseca je odmarao.

[youtube=http://www.youtube.com/watch?v=v6GnX3ZhuAg]

Nimda - Prva varijanta Nimde se pojavila 18. septembra 2001. godine i brzo se proširila svetom. Nimda kad se ?ita naopako poše admiN. Bila je relativno sli?na što se skeniranja mreže i širenja ti?e kao i CodeRed, ali imala je nekoliko dodatnih funkcionalnosti. Da objasnimo najpre osnovnu funkciju širenja ova dva virusa. Oba su skenirala ra?unare u potraži za ra?unarom sa IIS servisom. Algoritam je skenirao sve IP adrese (CodeRed samo javno, dok je Nimda mogla da skenira i privatne IP adrese). Prilikom skeniranja algoritam bi naišao na ra?unare koji nemaju odgovaraju?i operativni sistem ili nemaju instaliran IIS ili je njihov IIS patchovan. Ovakve mašine bi ignorisao, ali bi tako?e naišao na mašine koje imaju sve odgovaraju?e i njih bi zarazio.

Nimda je imala osobinu da je mogla da menja hostovane web sajtove tako da pružaju download inficiranih fajlova. Na ovaj na?in je mogla da izbegne firewall i da se dalje širi u privatnim mrežama. Mogla je da inficira Windows 95,98, Me, NT 4 i Windows 2000. Nimda je imala i jednu grešku zbog koje u odre?enim situacijama je crashovala i nije mogla dalje da se širi.

Fizzer (2003) - Fizzer je bio prvi virus ?ija jedina svrha je bila da kreira profit. Dolazio je sa inficiranim attachmentno. Kada je attachment bio otvoren, inficirao je ra?unar i slao sa njega spam poruke. U ovom trenutku se i menja struktura kreatora virusa. Do 2003. uglavnom se malware pisao entuzijasti?no, da se dokaže nešto, pokaže, eventualno osveti nekom zbog ne?ega. Od 2003. profit igra veliku ulogu. Tako i zemlje porekla se menjaju sa razvijenijih država, na države tre?eg sveta. Dok sami kreatori se menjaju sa tinejdžera geekova, na poslovne ljude, ?iji interes je kreiranje profita.

Teritorije porekla virusa pre 2003.

Teritorije porekla virusa nakon 2003.

Slapper je virus otkriven 13. septembra 2003. godine. Za upad na sistem koristio je ranjivost u OpenSSL-u i jedan je od prvih ra?unarskih crva koji je inficirao Linux, odnosno Apache hostove. Tako?e Slapper je imao backdoor, odnosno napada? je mogao da se prika?i na zaraženi ra?unar, izvrši komande ili instalira novi software. Backdor je osluškivao na portu UDP2002.

Slammer (2003) - Slammer je crv koji je koristio ranjivost u SQL serveru i Microsof Data Engine 2000. Svi programi koji su koristili bilo koji od ova 2 su bili potencijalna ulaznica za Slammer. Neki od programa preko kojih je ulazio su:

- Microsoft Biztalk Server
- Microsoft Office XP Developer Edition
- Microsoft Project
- Microsoft SharePoint Portal Server
- Microsoft Visio 2000
- Microsoft Visual FoxPro
- Microsoft Visual Studio.NET
- Microsoft .NET Framework SDK
- Compaq Insight Manager
- Crystal Reports Enterprise
- Dell OpenManage
- HP Openview Internet Services Monitor
- McAfee Centralized Virus Admin
- McAfee Epolicy Orchestrator
- Trend Micro Damage Cleanup Server
- Websense Reporter
- Veritas Backup Exec
- WebBoard Conferencing Server

Crv se širio samo kao memorijski proces. Nikad nije pisao ništa na hard disk. Kada bi se ra?unar restartovao infekcija bi nestala. Me?utim ukoliko je ra?unar vezan na mrežu sa zaraženim ra?unarom, verovatno bi uskoro bio ponovo inficiran. Slammer je kreirao velike koli?ine saobra?aja, a na taj na?in gušio mrežu i paketi su krenuli da se gube u mreži. Na ovaj na?in prouzrokovao je ozbiljnu štetu, kao na primer ATM mreža Bank of America je bila srušena i 911 servis u Sietlu. Ni kontrole letenja nisu bile imune na zarazu.

Blaster je detektovan u augustu 2003. godine. Koristio je buffer overflow ranjivost na DCOM RPC (Distributed Component Object Model Remote Procedure Call). Koriš?en je da napravi SYN flood na sajt windowsupdates.com. Me?utim nije napravio veliku štetu jer je pravi sajt bio na windowsupdates.microsoft.com. Microsoft je privremeno i ugasio microsoftupdates.com. Sadržao je 2 poruke:

- *I just want to say LOVE YOU SAN!!soo much*
- *billy gates why do you make this possible ? Stop making money and fix your software!!*

Sasser (2004) - Sasser je koristio buffer overflow ranjivost na Local Security Authority Subsistem Servisu. Širio se kroz mrežu i ?esto je umeo da sruši LSAS servis, ?ime bi se pojavio dijalog koji je odbrojavao minut do restartovanja ra?unara. Kada je microsoft izbacio patch koji je mogao da se skine sa sajta je kod mnogih korisnika doveo do frustracija, jer je skidanje i instaliranje patcha trajalo obi?no više nego što je bio vremenski interval za koji je Sasser rušio sistem. Srušio je mreže od Australije, preko Hong Konga do Sjedinjenog kraljestva.

Toliko za sad o crvima. U slede?em postu, koji ?e iza?i uskoro ?u se pozabaviti pojavom rootkitova poput SonyBMG, Mebroot, Conficker, kao i ransomware-om. Stay tuned.

- Kratka istorija malware-a | Peti deo: Neka rat po?ne
- Kratka istorija malware-a | ?etvrti deo: rootkit
- Kratka istorija malware-a | Drugi deo: Windows era
- Kratka istorija malware-a | Prvi deo: Po?eci