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

Kratka istorija malware-a | Drugi deo: Windows era

by Nikola Miloševi? - Saturday, December 01, 2012

https://inspiratron.org/blog/2012/12/01/kratka-istorija-malware-a-drugi-deo-windows-era/

Kako sam u predhodnom postu na?eo temu istorije razvoja malware-a, sada ?u da nastavim. U ovom delu ?u se pozabaviti delom razvoja od nastanka windows operativnog sistema, do dana kada su se crvi krenuli da se koriste i kada je malware krenuo da se upotrebljava za materijalnu dobit, kao i za napade na infrastrukturu. Odnosno sabotažu.

Pre nego što pre?emo na windows malware, bitno je pomenuti Morrisovog crva. Ovaj crv se pojavio u vreme kada je internet bio na po?etku i kada nisu postojale gotovo nikakve zaštite prilasku ra?unaru. Napravljen je kao studentski projekat studenta MIT, koji je želeo da izra?una broj ra?unara na internetu. Crv se širio preko mreže tako što je slao svoju kopiju svim povezanim ra?unarima, tamo se replicirao i ponovo prosle?ivao na ostale povezane ra?unare. Crv je imao bug, da nije obra?ao pažnju na to da li je ve? posetio neki ra?unar. To je u to vreme dovelo gotovo do potpunog zagušenja i pada mreža. Robert Morris je bio prvi ?ovek osu?en po ameri?kom zakonu iz 1986. godine o ra?unarskoj šteti i zloupotrebi.

WinVir je prvi Windows virus. Kreirao ga je ?ovek sa pseudonimom Masud Khafir, koji je tako?e kreirao i Plague virus. WinVir nije ?inio neku naro?itu štetu, ali je bio prvi virus koji je mogao da inficira novu PE strukturu izvršnih fajlova. Pokrenuti zaraženi fajl je tražio druge .exe fajlove i radio na njima odre?ene izmene, dok je pokrenuti fajl vra?ao u originalno stanje. Odnosno WinVir je brisao sebe iz fajla koji je pokrenut.

Monkey je virus koji je inficirao Master Boot Record hard diskova i floppija. Premeštao je prvi sektor MBR u tre?i i prvi sektor zamenjivao svojim kodom. Kada se korisnik bootovao normalno, ništa se ne bi prime?ivalo, me?utim kada bi se bootovao sa floppija, ispisivala bi mu se poruka Invalit drive specification.

One_Half ili Slova?ki bombarder. Inficirao je master boot record hard diska, COM fajlove i EXE fajlove. Nije inficirao fajlove koje sadrže SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE, MSAV ili CHKDSK u imenu, kako bi izbegao algoritme autoprovere fajlova koji pripadaju antivirusima. Poznat je po svojoj ?udnoj osobini da je enkriptovao delove korisni?kog hard diska, ali onda ih je dekriptovao prilikom pristupa, tako da korisnik ne bi primetio ništa. Enkripcija se radila uz pomo? XOR funksije sa nasumi?no generisanim klju?em, dok je dekripcija mogla da se uradi tako?e uz pomo? XOR-a istim tim nizom bajtova ponovo. Me?utim, nepažljiva dezinfekcija je mogla da dovede do gubitka podataka, ukoliko korisnik ne dekriptuje podatke, a uništi virus koji dekriptuje i pristupa podacima.Virus je prikazivao slede?u poruku 4.,8.,10.,14.,18.,20.,24.,28 i 30. svakog meseca pod odre?enim okolnostima:

Dis is one half.

Press any key to continue ...

Concept - WM.Concept (1995) je bio velika promena u filozofiji širenja virusa i veliki game changer. Radi se o prvom macro virusu koji se širio pomo?u Microsoft Word dokumenata. Napisan je u macro jeziku za word. Funkcionisao je kako na IBM PC, tako i na Macintosh ra?unarima, sve dok je na ra?unarima bio instaliran MS Word. Inficirao je sistem kad god je bio u?itan dokument za zaraženim template-om. Makro je kopirao zaraženi template u master template, pa tako svaki dokument koji bi na tom sistemu bio otvoren i prošao kroz Word je nosio zaraženi template.

Laroux (X97M/Laroux) je bio prvi Microsoft Excel macro virus. Detektovan je u julu 1996. Napisan je u Visual Basic za applikacie (VBA), makro jeziku baziranom na Visual Basic-u. Virus je mogao da radi pod Excelom 5.x i 7.x i pod Windowsom 3.x, WIndows 95 i Windows NT. Tako?e funkcionisao je i na lokalizovanim verzijama Excela. Nije ?inio nikakvu štetu, samo se replicirao.

Boza - Radi se o prvom virusu koji se širio pod Microsoft Windows 95 operativnim sistemom. Na?en je januara 1996. Virus ima australijsko poreklo, ali je detektovan u celom svetu, ali nije bio ozbiljna pretnja po korisnike windowsa 95.

Inficirao je Windows Portabilne EXE datoteke- fajlove koji koriste Windows 95 i Windows NT. Me?utim nije napadao mašine koje su koristile NT OS. Za sad nije na?en virus koji se specifi?no bazira na Windows NT.

Kad god bi EXE datoteka inficirana Boza virusom bila pokrenuta, on bi inficirao programe u teku?em direktorijumu. Jedan do tri EXE fajla su bila inficirana prilikom svakog pokretanja. Nakon ovoga Boza bi izvršio kod originalnog inficiranog fajla. Boza nije ostajao aktivan u memoriji nakon izvršavanja. Širio se relativno sporo. Me?utim proces infekcije je bio dovoljno brz da ne bi mogao da bude prime?en na ve?ini mašina.

Boza nije imao nikakve destruktivne rutine, ali imao je grešku pri kojoj bi inficiran fajl mogao da poraste do nekoliko megabajta. Ovo bi moglo da redukuje brzo prostor na hard disku (s obzirom da u to vreme hard diskovi su iznosili nekoliko stotina megabajta). Virus je imao aktivacionu rutinu koja je prikazivala prozor sa tekstom 'The taste of fame just got tastier!' i 'From the old school to the new', koji se pojavljivao 31. bilo kog meseca.

Marburg - Win95/Marburg je virus koji je po?eo da cirkuliše u augustu 1998. godine, kada je zarazio master CD popularne MGM/EA PC igre Wargames.

MGM - izdava? igre je izdao saopštenje 12. augusta 1998:
From: "K.Egan (MGM)" <kegan@mgm.com> Subject: MGM WarGames Statement Date: Wed, 12 Aug 1998 18:03:39 -0700
MGM Interactive recently learned that its WarGames PC game shipped with the Win32/Marburg.a virus contained in the electronic registration program. The company is working as fast as it can to resolve the problem ... MGM Interactive is committed to delivering top quality products to consumers. This is an unfortunate circumstance and we sincerely apologize for any convenience this has caused you. ... If you have any questions or if you would like to receive a replacement disc, please contact MGM Interactive.

Isti virus se proširio i autustu 1998., kada je bio sadržan na prate?em CD austrijskog PC Power Play ?asopisa.

Maburg je polimorfni Windows 95/98 virus. Inficirao je Win32 i SCR (screen saver) fajlove, enkriptovao svoj kod sa variabilnim polimorfnim slojem enkripcije. Polimorfni motor virusa je bio poprili?no napredan, jer je enkriptovao virus sa 8, 16 i 32 bitnim klju?en i nekoliko metoda. Virus je koristio spori polimorfisan, što zna?i da je menjao svoj dekriptor jako sporo.
Maburg je brisao integriti bazu nekoliko antivirusnih produkta. Tako?e je izbegavao inficiranje izvršnih fajlova poznatih antivirusnih programa, uklju?uju?i sve izvršne fajlove koji sadže slovo V u svom imenu. Ovo je ura?eno kako bi se izbeglo okidanje samo proveranja ovih programa.

Maburg se aktivirao 3 meseca nakon inicijalne infekcije. Ukoliko je inficirana aplikacija pokrenuta u isti sat kao i inicijalna infekcija, virus bi prikazivao standarnu Windows error ikonicu (crveni krst u belom krugu) na nasumi?nim pozicijama po ekranu.
Happy99 - Prvi mail virus. Prilikom otvaranja file-a iz attachmenta prikazivao je animaciju u kojoj je želeo sre?nu novu 1999. godinu, ali je uz to sebe mailovao svim kontaktima. Otkriven 1998. Važno je napomenuti da u to vreme nisu postojale zaštite na mail serverima

Melissa -Imenovan po ženskoj egzoti?noj plesa?ici, poznatoj pisa?u virusa, Melissa je kombinovala tehnike virusa i mail virusa. Inficirala je Word fajl, koji je posle slala emailom svim kontaktima u korisnikovom imeniku. Na ovaj na?in je Melissa postala prvi virus koji se proširio svetom za samo nekoliko ?asova. Virus je tako?e ubacivao komentare iz serije The Simpsons u zaraženi dokument. Tako?e slala je nasumi?ni dokument koji je našla na hard disku korisnika, što je moglo da na?ini prili?nu štetu, s obzirom da su tu mogli biti odre?eni planovi, ljubavna pisma...

LoveLetter (2001) - Mail virus koji je slomio milijone srca, LoveLetter je do danas jedan od najve?ih širenja virusa u istoriji. Širio se preko email attachmenta i prepisivao je mnoge krucijalne fajlove na inficiranom ra?unaru. Ovo širenje je bio zapravo jedan jako uspešan pokušaj socijanog inženjerstva. Koriste?i premisu ljubavi, virus je ubedio milijone da otvore attachment, što je prouzrokovalo štetu od 5,5 milijardi dolara širom sveta.

Anakournikova - Još jedan popularan virus koji se širio putem email-a. Navodno je slao slike Ane Kurnjikove, lepe i sexi teniserke. Me?utim attachemnt je bio izvršni fajl, koji je opet slao zaraženi fajl svim kontaktima. Ljudi iz antivirusnih kompanija su imali problem da ubede ljude koji su dobili mail, da ne mogu da vide sliku Ane Kurnjikove i da ne mogu da otvore attachment, pa ?ak i ako ga otvore, sliku Kurnjikove ne?e videti. ?ak i molbe da potraže sexy slike Ane Kurnjikove na internetu nisu mnogo urodile plodom...

Nastavak o crvima i malware-u koji se koristio za finansijsku dobit i sabotažu, idu?e nedelje.

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 | Prvi deo: Po?eci
