

STRAHOVI RAČUNARA (deo drugi) - WORMS

Srđan Katić

Dok sam krstario Internetom i prelistavao kućnu literaturu da bih sastavio istorijat crva i virusa nailazio sam na mnoge oprečne informacije koje se nikako nisu poklapale. Uglavnom se radilo o tome koje je godine ko šta uradio, koliko je šta trajalo, na koliko računara i da li je crv mogao da uradi ovo ili samo ono. Iz tog razloga sam se trudio da se oslanjam samo na izvore onih autora koji su ili eminentni ili se iz njihovih radova vidi da su se ozbiljno pozabavili tematikom.

UVOD

Vrsta elektronske infekcije koju ćemo u ovom broju Omega magazina bolje upoznati naziva se crv odnosno *Worm*.

U trećem broju Omega magazina govorili smo o klasičnom i e-mail virusu, kako funkcionise, kako se širi i na koji način nanosi štetu zaraženim računarima a bilo je reči i o motivima koji teraju pojedince da stvaraju elektronske infekcije. Videli smo da je virus pre svega pojava koja je nastala iz želje čoveka da drugima nanese štetu ili pak pridobije finansijsku pa i "moralnu" satisfakciju a postao nam je mnogo jasniji i način na koji elektronski virus zapravo imitira pravi to jest biološki virus. Međutim klasičan i e-mail virus nisu jedine infekcije koje pogađaju računare kao što ni bilološki virus određene vrste nije jedina bolest koja može da pogodi ljude ili životinje. U kolokvijalnom govoru svaka elektronska infekcija se naziva virusom ali uz bolje razumevanje ove pojave sve više dolazimo do zaključka da je neophodno izvršiti podele ovih infekcija kako bi ih grupisali radi lakšeg prepoznavanja i bolje prevencije odnosno zaštite. Vrsta elektronske infekcije koju ćemo u ovom broju Omega magazina bolje upoznati naziva se *crv* odnosno *Worm* i svima nam je manje više poznata kao jedan od najpopularnijih načina da vam neko zagorča dan. Međutim šta je to što crva razlikuje od klasičnog ili e-mail virusa? Hajde da upoznamo istoriju ove infekcije i odgovori će sami doći...

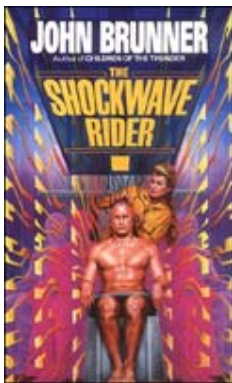
POČECI...



Prvi put kada se pomenuo termin *Worm* niko nije ni pomišljao da će ovakva pojava jednog dana steći ogromni publicitet. Zapravo, radilo se o naučnofantastičnom romanu iz 1972. godine (copyright 1975), autora John Brunner-a a pod nazivom "Shockwave Rider". U ovom cyberpunk remek-delu koje predstavlja priču o borbi protiv totalitarnog režima glavni junak Nickie Haflinger sve vreme beži od FBI-a tako što koristi softver pod imenom tapeworm kako bi menjao identitet. Zapravo, ceo svet kontroliše jedan superkompjuter kome svi pristupaju preko videotelefona (veephone-a) preko koga ih centralni računar identifikuje. Takozvani "tapeworm" pomaže Nickie-u da konstantno menja identitet i postane "cyber duh". Međutim, ovaj roman se ne smatra jednom od preteča današnjih elektronskih crva samo zbog naziva "tapeworm" koji se koristi u romanu već zbog načina na koji taj crv deluje, načina koji će uskoro inspirisati mnoge progamere da se pozabave istom tematikom. Takođe, ovaj roman je idejna preteča mnogih aktuelnih tema na današnjem Internetu i može se manje više smatrati proročkim delom. Jedna od ideja koja je predvidela današnji internet je takozvani *Hearing Aid*

service o kome Brunner piše u svom romanu a pomoću koga pojedinac može preko svog veephone-a da se ispovedi kompjuteru. Verovali ili ne ovakav servis i danas postoji na Internetu i neki od Amerikanaca se zaista odlučuju na ispovedanje softveru na nekom od Internet servera.

Do samog kraja osamdesetih (hronolozi bi rekli devedesetih) worm se nije smatrao infekcijom a njegova namena je u potpunosti bila da poboljša produkciju i rad mreže. U romanu Shockwave Rider prvi put se program tipa worm pominje kao program čija je namena da "nešto uništi ili prevari" i ovaj izuzetak u shvatanju primene crva ostaće usamljen sve do pojave prvog zlonamernog crva, tačnije do 1987. godine.



Ipak, autorsko delo John Brunner-a, iako zaslužno za stvaranje termina worm i davanje inspiracije mnogima, zapravo nije jedina preteča ove pojave. U vreme pisanja romana Shockwave Rider, jedan od programera koji se bavio pisanjem softvera za aviokompanije, napisao je program koji bi se svakako mogao shvatiti kao crv iako nije posedovao sve osobine koje današnji crv ima. Ime tvorca ovog crva je Bob Thomas i već pogađate da je ovo ime dospelo na Internet stranice tek pošto je crv postao redovna pojava u mrežnom saobraćaju i kada su počele da se pišu prve studije o ovoj potencijalno najopasnijoj pretnji za računarski svet. Program koji je Bob napisao zapravo je trebalo da informiše kontrolora leta kada se radarski prikaz određenog aviona premesti sa jednog monitora na susedni. Ovaj program iako ne baš pisan iz razloga iz kojih se danas pišu crvi ipak je donekle koristio operativni sistem na način na koji to rade današnji, zlonamerni crvi. Uskoro, posle nekoliko manjih pokušaja da se ovakva vrsta programa eksploatiše i na drugim segmentima mreže, upotreba "crvljivog" softvera zamire i pada u zaborav.

VAMPIRSKA POSLA

Ime ovog moćnog crva je bilo Vampir.

Godine 1982. ideja o crvu se vraća na velika vrata a za to su zaslužna dvojica programera koja su u to vreme bili zaposleni u istraživačkom centru kompanije Xerox. John Shock i Jon Hepps su kreirali pet vrsta crva od kojih je svaki bio zadužen da radi određenu radnju koja je imala za cilj bolje iskorišćenje mrežnih resursa. Može se reći da je u ovom slučaju primena crva bila menadžmentske prirode. Najjednostavniji crv je napisan kao neka vrsta glasnika i njegova uloga je bila da šalje obaveštenja korisnicima na mreži, malo komplikovaniji crv je merio performanse mreže dok je najkompleksniji crv bio toliko moćan da se uz zlonamernu upotrebu istog mogla zagušiti cela mreža ili jednostavno u potpunosti oboriti. Ime ovog moćnog crva je bilo Vampir. Zapravo on je preko dana postojao u mreži ali nije ništa radio dok je noću kada nema nikog u kancelarijama preuzimao kontrolu nad terminalima i računarima i upošljavao njihove procesore da rade operacije koje su bile previše zahtevne čak i za velike mainframe računare. Neposredno pre početka radnog vremena Vampir bi sačuvao sve podatke, oslobodio procesore i vratio se u svoju "tamu"... Međutim, jednu noć je Vampir očigledno dobio napad obesti pa je odlučio da demonstrira svoju moć kako bi ljudi konačno shvatili njegove potencijale. Zapravo, kada su zaposleni stigli ujutro na posao shvatili su da njihovi računari i dalje u "ropstvu" i pod totalnom kontrolom Vampira. Ko god bi pokušao da fizički resetuje računar nije dobro prolazio jer bi se operativni softver opet "srušio" i računar odnosno terminal bi i dalje bio neupotrebljiv. Da li je crv pod imenom Vampir pronašao način da izađe na svetlost dana ili se samo preterano "napio krvi" tokom noći u tom trenutku nikom nije bilo poznato ali ono što je bilo sigurno je da je tog dana bio predsedavajući istraživačkog centra Xerox-a. Postalo je očigledno da jedino Blade može da reši situaciju tako da su se Jon i John latili

svojih "sečiva" i brzinom svetlosti napisali vakcinu. Ovakva "crveća" katastrofa nanela je Xerox-u veliku štetu tako da su se ubuduće svi trudili da što pre zaborave da je nekada postojao vampir kome je bilo previše dozvoljeno. Nakon ove katastrofe ideja o eksploataciji crva je zamrla i ovakav softver se nije pravio, bar ne u većim kompanijama u narednih 5-6 godina.

Međutim, crv crvu ne da mira tako da je sledeći slučaj worm napada pogodio IBM mrežnu infrastrukturu tačno na Božić 1987. U pitanju je bila kombinacija trojanskog konja i crva koja je paralizovala celu IBM mrežu. Ovaj trojanski crv može da se shvati i kao neslana šala koja i nije mnogo zlonamerna. Naime, božićni crv bi tražio od korisnika da otkuca reč Christmas kako bi ga ostavio "na miru". Pošto korisnik otkuca šta je traženo od njega crv bi isctrao božićno drvo na ekranu i poslao sebe svim korisnicima čija bi imena pronašao u datotekama "Names" i "Netlog".

INTERNET WORM

Dana 2. Novembra 1988 opet se desila katastrofa iz koje je odmah proizišao termin "Internet worm". Robert Tappan Morris, 23-godišnji vunderkind koji je već uveliko spremao doktorat na univerzitetu Cornell, vršio je eksperimente sa programskim kodom crva i greškom pustio crva u mrežu pod nazivom Arpanet, javnu mrežu koju mi danas znamo pod imenom Internet. Za manje od osam sati ovaj internet crv je zarazio 3000 računara koje je zagušio do neupotrebljivosti.



Koristeći kontrolu nad zaraženima računarima i rupe u operativnom sistemu internet crv se replicirao na druge mašine na Arpanetu a izgledalo je kao da ovoj agoniji nema kraja. Kao posledica ove katastrofe bilo je uklanjanje većine računara i servera sa Arpanet-a i mukotrpan danonoćni rad grupe naučnika koji je trajao tri dana kako bi se kreirala vakcina. Neopisiva je sreća za korisnike Arpanet-a što je eksperimentalni crv bio nesposoban da uništava podatke već je jedino umeo da preuzme kontrolu na računaru i da se dalje proširi. Ipak, internetu je naneta ogromna šteta zbog *downtime* perioda od nekoliko dana a da ne pominjemo kroz kakva "sita i rešeta" je jadni Robert Morris prošao zbog toga što je uradio.



Ono što je zanimljivo pomenuti u vezi ovog incidenta je zapravo enorman publicitet koji je Morris-ov crv stekao. Više od nedelju dana vest o oborenem Internetu je bila na naslovnim stranama mnogih časopisa iako su se iste nedelje održavale predizborne kampanje i bili u toku predsednički izbori u Sjedinjenim Državama (!). Međutim, nakon prve nedelje novinari su shvatili da ne znaju kako da prate ovakav događaj i na koji način da pišu članke o nečemu što ni sami ne razumeju, ama ni malo. Delovalo je kao da su sami novinari kukali za časopisom koji bi im objasnio o čemu se zapravo radi. Kada bi pročitao u novinama da "Internet crv kontroliše rupe u dizajnu aplikativnih i mrežnih slojeva operativnog sistema" prosečnom podgojenom amerikancu bi se desilo nešto što bi mogli

metaforično da shvatimo kao "spontano sagorevanje" s' obzirom na to da ni sam autor članka nije razumeo šta reč "rupa" zapravo znači. U tom slučaju je sasvim razumljivo zašto su vesti o ovom nemilom događaju utihnule nakon desetak dana od pojave crva u javnosti, mada su mnogi mislili da su vesti utihnule jer je problem bio rešen.

Zvanična procena štete nasene internet crvom bila je i do deset miliona dolara po USGAO-vim (United States General Accounting Office) statistikama.

WANK

WANK je napadao VAX i VMS računare i bio je poprilično neprijatan za korisnike i administratore.

Ubrzo, tačnije nakon manje od godinu dana, kada su već svi mislili da je crv samo prošlost pojavio se jedan pod nazivom WANK. WANK je napadao VAX i VMS računare i bio je poprilično neprijatan za korisnike i administratore. Šta je on zapravo radio? Pre svega WANK bi napadao korisničke naloge, isključivao bi sistemski mail za korisnika, promenio bi login komandu tako da bi korisnik pomislio da su mu fajlovi obrisani i takođe bi ispisivao sistemsku poruku na ekranu po svojoj želji. Poruka koju je ispisivao je bila "Worms Against Nuclear Killers" od koje je i sam WANK dobio ime. Nakon ispisane poruke grafički bi se prikazala reč sastavljena od prvog slova svake reči poruke i zadnja tri slova poslednje reči killers. Time bi dobili reč WANKERS što bi u slobodnom prevodu značilo "vankeri" ili "oni koji vas upravo vankuju".

Ukoliko WANK ne bi uspeo da uzurpira korisnički nalog na VAX i VMS računarima onda bi počeo da se ponaša kao kakav mali zloća koji pokušava da uradi bilo šta što bi moglo da iznervira pogođenog korisnika. To je išlo dotle da je preko PHONE funkcije pozivao kućne brojeve korisnika iz firme kako bi ih budio cele noći i kako bi im koliko toliko napakostio. Dok bi pola grada gađalo papučom telefon WANK bi u međuvremenu krao korisničke lozinke sa mreže i pokušavao da se probije na neke druge sisteme. Dokaz da je u pitanju mali pakosnik je i to što je WANK mogao da telefonsku liniju koristi isključivo da bi se dalje širio preko RAS servera ali umesto toga draže mu je bilo da cela firma sutradan dođe na posao sa podočnjacima do kolena.