

STRAHOVI RAČUNARA - deo prvi

Srđan Katić

Zašto ljudi prave viruse?

Elektronski virusi predstavljaju jednu od najvećih sigurnosnih pretnji za računarsko okruženje.

Elektronski virusi predstavljaju jednu od najvećih sigurnosnih pretnji za računarsko okruženje. Da li ste znali da kada bi ste ceo dan proveli spaljujući novčanice od po 1000 dolara ne bi ste uspeali da napravite ni 10% štete od one koju u svetu napravi jedan virus za isti taj dan? Možda zvuči suludo ali jedan tako mali softverski proizvod koji je jednostavniji od 99.9% aplikacija koje koristimo pri radu na računaru može da nam zada glavobolju o kakvoj nismo ni sanjali. Svako ko je bio pogođen virusom i doživeo gubitak svojih podataka zasigurno je osetio koliko su računari ranjivi i svakako koliko je bitno imati rezervnu kopiju podataka.

Bez imalo čuđenja možemo zaključiti da nije trebalo da prođe mnogo vremena od popularizacije prvog personalnog računara do trenutka kada je nekom palo na pamet da bi mogao da pomoću malo softvera pomrsi sve konce u operativnom sistemu. Sigurno se već pitate zašto je uopšte neko došao na ideju da kreira softver čija je namena destruktivna ali kratkim osvrtom na ljudsku prirodu jako brzo dolazimo do odgovora koji verovatni ni ne želimo da saslušamo do kraja. Zašto vam sin vašeg komšije redovno baca petarde ispod prozora? Zašto je na zidu vaše zgrade sprejom ispisano " VII-2 "? Razlog koji nam daje odgovor na predhodna pitanja je verovatno prvi od više razloga zbog kojih je došlo do pojave virusa. Jednostavno, Perici nije bilo zanimljivo da ispisuje sprejom grafitu pa je odlučio da bude savremeni *cyber* vandal i upotrebi svoje znanje na računaru kako bi pokazao da ni njega nisu zaobišle draži adolescencije iako po ceo dan kao i njegov tata gleda u monitor. Ovakvo polumetaforično objašnjenje može da se potkrepi i činjenicom da su se računarski virusi raširili sa prvim danima popularizacije računara i među računarskih komunikacija, to jest sa prvim danima Interneta i *bulletin board*-ova (*BBS*-ova). Do tada računare su koristili isključivo programeri i naučnici a svrha računara u kućnom okruženju je bila gotovo neopravdana, što zbog ogromne cene što zbog nedostatka softvera koji bi mogao da bude zanimljiv krajnjem korisniku. Jedina svrha računara u kućnom okruženju mogla se svesti na igranje igrice i korišćenje malog broja aplikacija namenjenih krajnjem korisniku. Tačnije, krajnji korisnici računarskih tehnologija nisu ni postojali osim onih koji su se bavili programiranjem kod kuće pa su u tu svrhu koristili razne aplikacije koje bi mogle da im budu od koristi.

Perica je odlučio da bude savremeni *cyber* vandal...

Možete li da shvatite kolika je bila sreća malog Perice kada se smrknuti tata ulogovao na svoj računar i shvatio da su mu podaci ispremeštani po celom hard disku? Ja mislim da je bila ogromna. Ovaj put je Perica uspeo da uradi nešto što mu nikad nije pošlo za rukom, uspeo je da promeni nešto što verovatno ni njegov veliki tata ne može a ni ne ume. U tom trenutku dolazimo do drugog razloga koji je motivisao Perice širom sveta da prave još ovakvih softverskih naprava. Moć. Gledajući Internet strane sa upozorenjem o novom virusu Perica se sigurno osećao kao da je na vrhu sveta. Eto, toliko vesti na Internetu o njegovom virusu, niko ne zna odakle stiže osim samo jednog, najmoćnijeg, Perice. Predpostavljam da je mali Perica po ceo dan u pretraživaču iščitavao broj strana koje govore o novom virusu a sa svakim porastom ovog broja rasla je i njegova sreća.

Međutim, Perica se jedno jutro probudio, nakačio na Internet i pročitao vest o tome kako je nađen lek za njegov virus i kako uz dva klika možete da spasite svoj računar od virusa pod imenom "Pera.car.exe.js". Smrknutom i osujećenom Perici nije preostalo ništa drugo nego da sedne ispred svog računara i pokuša da napravi nešto novo ne bi li njegov osmeh opet dobio na širini. Kocka je bačena i to se mora uraditi. Dakle, treći razlog je svakako potreba da se ovako pridobijena "slava" zadrži po svaku cenu, uostalom Perica je godinama sedeo ispred svog "kućnog ljubimca" tako da teško da bi ovakav podvig mogao da napravi ako bi otišao do školskog dvorišta da odigra fudbal ili basket sa prijateljima. Jednostavno, ljudi koji prave viruse to znaju najbolje da rade i teško da ćete ih odgovoriti od bavljenja poslom koji im daje toliku moć, moć da nanese veliku štetu nekom ko im se ne sviđa ili bar bilo kome.

Možda zvuči apsurdno ali ovakve primere kao sa Pericom možemo slobodno nazvati "kompleksom Isusa". Pokušavajući da menjaju svet na globalnom nivou Perice širom sveta zapravo pokušavaju da skrenu pažnju na svoje delo i samim tim na sebe kako bi verovatno umanjili odbačenost koju osećaju ili dali sebi svojih "5 minuta". Kompleks Isusa je već i zvanično poznat kao psihološki fenomen.

Međutim, sve bi bilo mnogo lepše kad bi samo ova tri razloga bila motivi za programere koji prave računarske viruse. Ovakvu vrstu znanja i poznavanja sigurnosnih rupa u informatičkim sistemima često koriste i oni koji žele da nešto preokrenu u svoju korist. Probajte samo da pomislite na moguću finansijsku dobit koja bi za nekog proizišla iz širenja virusa i biće vam jasno koliko je to unosan posao. Međutim, konkretne primere za ovako nešto ne možete očekivati od autora ovog članka ali je sasvim izvesno da je virus oružje koje može da naškodi vašem konkurentu na tržištu ili da doprinese prodaji vašeg antivirusnog programa.

Kao sledeći ali ne i bezazleni razlog naveo bi ideološke motive.

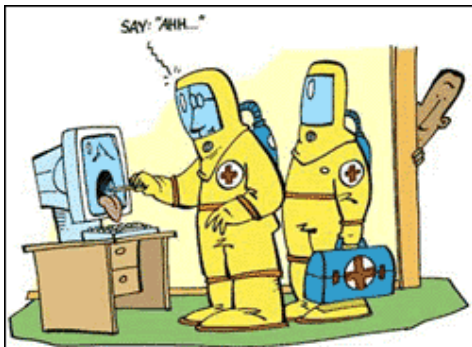
Kao sledeći ali ne i bezazleni razlog naveo bi ideološke motive. Siguran sam da veliki broj ljudi pomoću virusa pokušava da iskaže svoj gnev prema određenim kompanijama, organizacijama ili društvenim grupacijama. Praveći i šireći viruse koji pogađaju njegovog neprijatelja programer virusa svakako doprinosi borbi protiv neistomišljenika, bilo da je rezultat delovanja virusa koji je napravio oboren server, ugrožena bezbednost na određenim delovima javne elektronske mreže ili direktno uništavanje podataka. Ne zaboravite da virus može da deluje tako što menja sadržaj podataka što predstavlja ozbiljno kompromitovanje bezbednosti i moćno oružje ukoliko ste sposobni da ovaku ilegalno stečenu prednost iskoristite.

Poslednji bitniji razlog iz koga ljudi prave viruse zapravo se može shvatiti kao kombinacija nesposobnosti da se usmeri negativna energija i neodgovornosti. Neretko se dešava da se ljudi po raznoraznim *chat* kanalima posvađaju ili lepše rečeno grubo suprotstave. U takvim situacijama uvek se nađe neko kome reči nisu dovoljne pa se odluči da upotrebi neke od zaraženih disketa koje čuva u svom arsenalu za elektronske obračune. U ovakvim afektnim stanjima retko se vodi računa o tome da virus koji se šalje nekom bude rizik samo za tu osobu već neretko izvršenjem osвете nad nekim, "pobesneli" *chat* kauboji postaju deo lanca zaraze a da toga nisu ni svesni.

Elektronske infekcije

Nažalost, virus nije jedina napast koja može da zadesi vaš računar mada sa sigurnošću možemo reći da je cilj svih oblika elektronskih infekcija isti a to je nanošenje štete, probijanje sigurnosti, finansijska dobit, samozadovoljenje i sticanje ugleda u krugovima programera "iz podzemlja". U ovom članku pokušaćemo da definišemo dve osnovne vrste virusa a u narednim brojevima omegamagazina biće vam predstavljeni i drugi popularni oblici elektronskih infekcija kao i standardne odnosno napredne metode pomoću kojih možete da se borite protiv istih.

Klasičan virus



Klasičan virus je prvi oblik elektronske infekcije. Virus je napisan tako da ga možemo definisati kao "slepeg putnika". On nikad nije samostalan i uvek se "nakači" na neki program i pokreće zajedno sa njim. Zato je i dobio ime po biološkom virusu. Slično pravom virusu on se uglavi u izvršni kod nekog programa i čeka da se taj program pokrene. Pravi, to jest biološki virus, zapravo nije u stanju da se sam reprodukuje, on se nastani u ćeliju i čeka njenu reprodukciju kako bi se klonirao. To je takozvani period inkubacije tokom koga virus ne deluje ali se širi koristeći mehanizam domaćina

pomoću koga se replicira zajedno sa ćelijom. U određenom trenutku kada se dovoljno proširio biološki virus počne da napada ćelije organizma, drugim rečima da deluje. Računarski virus radi skoro istu stvar mada se ne ponaša baš identično biološkom virusu. Kada se zaraženi program pokrene virus je spreman da se proširi i u stanju je da zarazi druge podatke i aplikacije, uglavnom one koje prvobitno zaraženi program poziva pri radu. Na ovaj način računarski virus efikasno koristi period inkubacije tokom koga niste ni svesni da vam je računar zaražen. Naravno ovo nije uvek inkubacija kao kod biološkog virusa jer do delovanja može da dođe pri prvom izvršenju zaraženog programa ali čak i u tom slučaju dok vi shvatite da vam sa sistemom nešto nije u redu i dok se nakanite da istestirate vaš računar na virus on se već poprilično proširio i verovatno već zarazio veliki broj datoteka. Zbog toga je bitno da vršimo redovno skeniranje našeg računara jer je postojanje virusa u retkim slučajevima baš očigledno.

Kako se interno širenje virusa zapravo odigrava?

Kako se interno širenje virusa zapravo odigrava? Najbitnija sposobnost virusa koja mu omogućava širenje unutar softverskog okruženja je mogućnost da se "dočepa" operativne memorije računara koje svako parče softvera koje držimo na računaru mora kad-tad da poseti. Naime, zaraženi program se startuje i učita u memoriju a sam virus se "šlepuje" uz izvršni kod zaraženog programa. Dalje, skoro svaki program koji se učita u memoriju biva zaražen. Međutim šta se dešava kada ugasimo računar i kada se operativna memorija isprazni? Da bi prevazišao ovaj problem virus ima sposobnost da se učita u *boot* sektor hard diska ili *floppy* diskete. Da podsetimo, *boot* sektor je softver male veličine koji sadrži informacije neophodne za inicijalno dizanje operativnog sistema. Samim tim jasno je da je neophodno da se prvo učita sadržaj *boot* sektora u memoriju kako bi bilo omogućeno dalje dizanje sistema. Na taj način virus je zagarantovao svoju omiljenu poziciju, RAM.

Što se tiče klasičnih virusa opadanje njihove popularnosti leži u činjenici da ne mogu da se prošire brzinom kojom to rade e-mail virusi. Nekada davno kada je Internet bio nerazvijen i kada elektronska pošta nije bila standard za komunikaciju virusi su se uglavnom širili putem *floppy* disketa i *bulletin board*-ova. Pošto je većina današnjih programa prevelika za diskete ovaj način širenja je neatraktivan i spor. Međutim, klasičan virus i dalje možete pokupiti sa neke *newsgroup*-e ili sumnjive ftp lokacije, preko *floppy* disketa, putem deljenja fajlova na lokalnoj mreži pa čak i putem mejla mada takav virus nema sposobnost da se dalje širi po Internetu već je praktično namenjen samo vašoj e-mail adresi.

E-mail virus

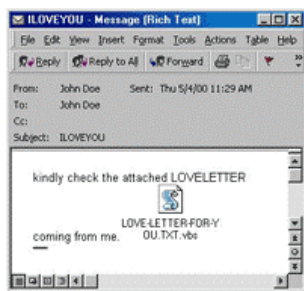
E-mail virus je najmlađi oblik elektronske infekcije. Kao što samo ime kaže širi se putem e-mail pošte a, pošto se proširi i zarazi korisnikov računar njegovo delovanje postaje slično ili identično delovanju klasičnog virusa.

Širenje e-mail virusa se odigrava u dve faze:

1. Inicijalno širenje – Za delovanje u ovoj fazi odgovoran je sam autor virusa ili pak grupacija programera koji se organizovano bave ovakvim delatnostima. Cilj ove faze je da se virus pojavi u javnosti kako bi dalje mogao da se samostalno širi. Obično kreatori virusa imaju bazu sa nekoliko stotina ili hiljada adresa na koje pošalju novi virus. Spisak ovih adresa možemo svakako smatrati crnom listom. Na ovaj način e-mail virus se inicijalno proširi i utvrdi svoje početne pozicije. Sa istim ciljem autori virusa postavljaju virus na *newsgroup*-e u formi tekstualnih datoteka tako da korisnici skidaju te datoteke misleći da se radi o informacijama koje su domenu njihovog interesovanja. Inicijalno širenje putem *newsgroup*-a se odnosi kako na e-mail viruse tako i na klasične viruse koji nisu u stanju da koriste prednosti mejling sistema.

MELISSA je e-mail virus koji se najbrže širio u istoriji ove zarazne bolesti.

2. Samostalno širenje – Šta se dalje dešava? Pošto je prvih nekoliko hiljada ljudi zaraženo e-mail virus automatski sam sebe šalje na adrese koje se nalaze u *address book*-u zaraženog sistema. Kada se povežemo na Internet zaražene poruke odu širom Interneta a da često pritom nismo stanju da ih vidimo u *outbox*-u našeg mejl klijenta. Na taj način ni ne znamo šta nas je zadesilo a isto tako ni korisnik koji primi zaraženu poštu sa naše adrese. Jedan od najpopularnijih virusa ove vrste ikada je virus MELISSA. MELISSA je e-mail virus koji se najbrže širio u istoriji ove zarazne bolesti. Njegovo postojanje je prvi put uočeno marta 1999. godine a naneo je toliko štete širom sveta da je veliki broj velikih kompanija pa i samih dobavljača e-mail usluga zatvorilo svoje e-mail sisteme na neodređeno vreme. Procena štete nanese ovim virusom širom sveta a tokom najvećeg udara govori o više milijardi dolara na svakih 12 sati. MELISSA je zapravo virus koji je iskoristio funkcije *Microsoft Visual Basic*-a na taj način da svaki put kada pokrenete zaražen dokument virus se pokrene i koristeći VBA mehanizme aplikacije izvršava radnje poput slanja pošte ili modifikovanja fajlova. Na taj način često vam uništi fajlove i pošalje sam sebe na adrese koje imate u .wab datoteci koja predstavlja vaš elektronski adresar.



Sledeći virus, hronološki gledano, koji je drastično privukao pažnju javnosti je virus ILOVEYOU za koji ste svakako čuli. Njegov struktura je bila tako jednostavna da se i dan danas smatra da nije moguće napraviti jednostavniji virus. Pojavio se 4. maja 2000 godine a šteta koju je naneo ne kaska mnogo za onom koju je izazvala kraljica svih virusa, MELISSA. Za razliku od MELISSE u pitanju nije bio word dokument koji je posedovao makroe zle namere već se radilo o e-mail poruci na koju je prikačen attachment a u čijem subject-u piše ILOVEYOU. U pitanju je svakako najnežgodnija ljubavna poruka koju možete primiti.

Kako virusi deluju?

Ovaj deo priče o virusima može lako da se predstavi kao neinteresantan za autora virusa. Ono što fascinira svakog ko se bavi računarskim virusima je brzina kojom se on širi i način na koji izvrši radnju gotovo uvek fatalnu za korisnika zaraženog sistema. Međutim, kada virus pređe sve zamke anti-virusnih programa i zaštita operativnog sistema i aplikacija ono što na kraju uradi je uglavnom razočaravajuće. Uglavnom se radi o nekoj jednostavnoj radnji poput brisanja fajlova ili

formatiranja *boot* sektora tako da posle restarta sistema vaš sistem više ne može da se podigne, a nekada se radi o nezlonamernom virusu koji vas npr. maltretira sa malom animacijom ovčice koja prolazi preko vašeg ekrana dok nešto radite. Koliko god se trudili ovčica će vas redovno posećivati i verovatno reći nešto sasvim glupo. Nekada će padati padobranom, nekad igrati fudbal a nekada će samo čučati u ćošku i zvižducati. U početku se smejete ali verujte mi da nakon par dana ovčica nije ni malo zanimljiva. Počnete da je iznervirano bacate kursorom u ćošak ekrana a nakon samo nekoliko sekundi iz suprotnog ćoška ovčicina glava kreće da se pomalja i da vas priupituje nešto još gluplje od onoga što ste prvi put čuli od nje. Mada, ruku na srce, bolje dosadna ovčica nego formatiran hard disk.

Kao jedno od indirektnih delovanja e-mail virusa može se pomenuti zagušenje Internet saobraćaja. Poznato je da u prvim danima virusa, danima navale, Internet saobraćaj ume da bude fatalno usporen što je i sasvim logično sa obzirom na tehniku kojom se širi e-mail virus.

Vrednost koja zapravo označi momenat kada virus treba da se izvrši naziva se *trigger* (okidač). *Trigger* je nekada momenat izvršenja zaraženog fajla, nekad dostignuti broj replikacija virusa a nekada unapred određen datum. U svakom slučaju desiće se a da to najverovatnije ni ne znate.

Kako je moguće da virus nanese baš toliko štete?!

Siguran sam da su bar neki od vas rekli "Ma ajde!"...

Siguran sam da su bar neki od vas rekli "Ma ajde!" kada su pročitali informaciju o milijardama dolara vrednoj šteti koju virus može da nanese. Možda zvuči previše ali na zapadu šteta nanescena virusom, kao i bilo koja druga, ne meri se samo direktno izgubljenim novcem. Ako je izvesna kompanija koja ima 500.000

korisnika dnevno, kao što je slučaj sa kompanijama mobilne telefonije, prinuđena da obori svoje servere na 6 sati onda samo zamislite koliko je nenaplaćenih sms poruka, poziva vremenskoj prognozi ili mejl poruka. Isto tako, dešava se da "bezobrazniji" virusi izbrišu podatke čija vrednost često ne može da se meri samo novcem već su u pitanju podaci bitni za poslovanje firme. Neretko provajderi Internet i mejl usluga "gase" svoje servere i iz već pomenutog razloga zagušenja saobraćaja. Ponekad e-mail virus toliko optereti javnu mrežu da je jedini način da se Internet rastereti da provajderi koji poseduju e-mail sisteme jednostavno obustave saobraćaj pošte. U zapadnim zemljama *down-time* je najgore što može da se desi jednoj velikoj kompaniji. Setite se samo koliko je avio-kompanija propalo posle 11. septembra 2001. godine jer im je poslovanje samo privremeno bilo prepolovljeno. Skoro nijedna od tih kompanija nije izgubila novac ili avion posle terorističkog napada u New York-u ali su mnoge propale. U našoj zemlji je suprotna priča jer se dešava da kompanija posluje ispod svake norme a da i dalje postoji u narednim godinama. U Americi, ako niste "u igri" mesec dana vi ste prošlost i treba vam mnogo vremena da se oporavite, a to je upravo ono što elektronski virus radi, natera vas da obustavite deo poslovanja, da uradite najgore po sebe. Otuda zapravo tolika šteta koju virus nanosi, on pogada najosetljiviji deo zapadnog sistema jer na zapadu ako stojite onda i propadate.

Zaključak

Kakvi god da su razlozi iz kojih pojedinci ili manje organizacije prave viruse, ono što je sigurno je da će oni postojati dok god postoje i računari. Koliko god se stručnjaci trudili da naprave idealnu zaštitu od virusa, najbolje što mogu da urade je da preventivno umanje štetu nanescenu širenjem elektronskih infekcija ili da autorima virusa otežaju bavljenje ovakvim zanimanjima. Microsoft je još prošle godine najavio poboljšanje zaštite od virusa digitalnom autentifikacijom procesa koji pokušavaju da se izvrše u operativnom sistemu. Ova prednost .NET tehnologije zaista zvuči ohrabrujuće ali ako je čovek napravio tu tehnologiju onda će je čovek i probiti i u to nema mnogo



sumnje. Iz ovih razloga je bitno da se svako od nas malo bolje upozna sa načinom širenja i delovanja virusa kako bi stekao sposobnost da ga prepozna i da se efikasno od njega odbrani.

U narednim brojevima Omega magazina govorićemo o tehnikama odbrane od virusa kao i drugim vrstama elektronskih infekcija koje mogu da pogode računare. Završićemo priču o podeli virusa a moćićete i da pročitate nešto više o prvim zabeleženim primerima virusa. Do tada pozdrav svim čitaocima...