HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Sobig.a crva

CCERT-PUBDOC-2003-04-17

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

U dokumentu je iznesena analiza Sobig.a Win32 crva, malicioznog programa koji neovlaštenim korisnicima olakšava slanje SPAM poruka. Sobig.a crv posebno je interesantan za analizu, budući da svojim karakteristikama prilično odstupa od ostalih malicioznih programa sličnog tipa.
Većina poznatijih mrežnih crva i virusa redovito dolaze s nekom vrstom *backdoor* programa, koji neovlaštenom korisniku omogućuje kontrolu nad inficiranim sustavom. Ovisno o tipu i namjeni programa, isti se dalje širi na druga ranjiva računala gdje obavlja svoje maliciozne zadaće.
Sobig.a crv specifičan je po tome što na inficiranom sustavu umjesto *backdoor* programa instalira anonimni *open proxy* poslužitelj koji je inicijalno podešen tako da svima omogućuje neautorizirano prosljeđivanje konekcija. Budući da su nezaštićeni *proxy* poslužitelji jedna od primarnih metoda koje *spammeri* koriste za prikrivanje izvora SPAM poruka, mišljenje je kako je ovaj crv razvijen isključivo u tu svrhu.
Širenjem Sobig.a crva stvara se mreža otvorenih *proxy* poslužitelja koji na taj način olakšavaju slanje SPAM poruka te prikrivanje njihovog izvora. Kombiniranjem lažiranja zaglavlja poruka elektroničke pošte i prosljeđivanjem konekcija kroz nekoliko *proxy* poslužitelja, vrlo je teško utvrditi pravi izvor poruke. Budući da je prikrivanje identiteta i lažiranje izvora poruka jedan od važnih zadataka *spammera*, Sobig.a crv idealno je rješenje za distribuiranje SPAM-a.

2. Tehnike distribuiranja neželjene elektroničke pošte

Neželjena elektronička pošta (engl. ***U**nsolicited **C**ommercial **E-**mail –**UCE***), ili popularnije SPAM, danas je jedan od ozbiljnijih problema na Internetu. Brojne poruke, najčešće komercijalnog, odnosno reklamnog sadržaja, svakodnevno popunjavaju korisničke spremnike poruka (engl. *Mailbox*), čime se krajnjem korisniku i davateljima Internet usluga (engl. ***I**nternet **S**ervice **P**rovider*), osim nametnutih novčanih troškova, stvaraju i brojni drugi problemi. Problematika SPAM poruka izlazi van okvira ovog dokumenta i kao takva neće biti dalje razmatrana u kontekstu ovog dokumenta.
U samim počecima distribucije SPAM poruka, njihovi pošiljatelji (u nastavku dokumenta *spammeri*) nisu koristili neke posebne metode za njihovo slanje. Poruke su se slale s vlastitog korisničkog računa, preko lokalnog davatelja Internet usluga, koji je poruke uredno dostavljao na njihovo odredište. Iako vrlo jednostavan i praktičan, ovakav pristup postao je vrlo brzo neprihvatljiv za *spammere*, budući da ne pruža nikakvu mogućnost zaštite od otkrivanja stvarnog izvora poruke. Mrežni administratori i krajnji korisnici su se vrlo brzo organizirali u borbi protiv SPAM-a, što je najčešće rezultiralo blokiranjem korisničkog računa i pristupa Internetu onim korisnicima za koje se pokazalo da sudjeluju u distribuiranju SPAM-a.
Kako bi otežali otkrivanje izvora poruka, *spammmeri* su pribjegli brojnim drugim metodama kojima su nastojali prikriti svoje aktivnosti. U nastavku su opisane neke od popularnijih metoda.

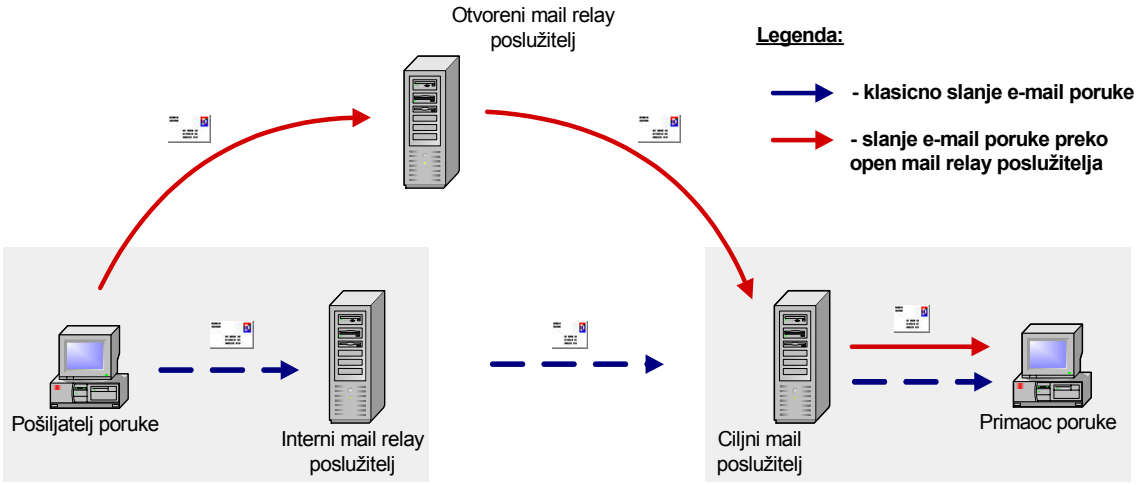
2.1. Privremeni korisnički računi

Jedna od svojevremeno vrlo popularnih metoda sastojala se u otvaranju privremenih korisničkih računa koje bi *spammeri* iskoristili za kratkoročno distribuiranje SPAM poruka. Privremeno otvoreni korisnički račun *spammeri* bi iskoristili za distribuciju SPAM poruka, sve dok netko ne bi prijavio njihove aktivnosti. Dok bi davatelj Internet usluga blokirao prijavljeni korisnički račun s kojeg su detektirane SPAM aktivnosti, isti *spammer* već bi našao drugog davatelja usluga preko kojeg bi nastavio distribuiranje poruka.
Ova metoda je dugo godina bila jedna od osnovnih tehnika distribuiranja SPAM-a, sve dok ISP davatelji usluga nisu počeli kreirati bazu korisnika za koje je poznato da otvaraju ovakve korisničke račune.

2.2. Otvoreni *mail relay* poslužitelji

Sljedeća tehnika koja je još uvijek vrlo popularna za distribuiranje SPAM poruka je iskorištavanje otvorenih *Mail relay* poslužitelja. *Open relay* su oni Mail poslužitelji koji omogućuju procesiranje poruka elektroničke pošte koje nisu niti namijenjene lokalnim korisnicima, niti su poslane od strane

istih. Otvoreni *mail relay* poslužitelji *spammerima* omogućuju jednostavno slanje SPAM poruka, pri čemu se svi troškovi procesiranja poruka prebacuju na organizaciju čiji se *Mail* poslužitelj iskorištava. Na sljedećoj slici dan je primjer slanja poruke elektroničke pošte preko otvorenog *Mail relay* poslužitelja (Slika 1).



Slika 1: Distribuiranje SPAM poruka preko open mail relay poslužitelja

Uvidjevši problem otvorenih *mail relay* poslužitelja, organizirane su brojne akcije s ciljem pronalaženja istih, kako bi se na taj način suzbilo distribuiranje SPAM-a. Danas postoji velik broj Web stranica na kojima je moguće provjeriti da li je neki Mail poslužitelj *open relay* ili nije. Ovakve stranice najčešće koriste mrežni administratori u svrhu blokiranja SMTP konekcija s tih poslužitelja.
Danas postoje i javni automatizirani alati koji periodički provjeravaju nasumce odabrane *Mail* poslužitelje kako bi utvrdili da li su *open relay* ili ne. Ukoliko jesu, poslužitelji bi se automatski dodavali na "crnu" listu otvorenih *relay* poslužitelja, kako bi se naglasila mogućnost njihove zlouporabe u svrhu distribuiranja SPAM poruka.
Iako korištenje otvorenih *mail relay* poslužitelja u određenoj mjeri omogućuje djelomično prikrivanje izvora poruka, detaljnijom analizom zaglavlja poruke moguće je prilično jednostavno utvrditi njezino pravo podrijetlo. Kako bi se u što većoj mjeri otežala identifikacija izvora poruke, *spammeri* su počeli lažirati zaglavlja istih. Postoje različite tehnike lažiranja zaglavlja, s boljim ili lošijim rezultatima, ovisno o vještini i iskustvu *spammera*.
Također treba napomenuti kako je detaljnijom analizom log zapisa na Mail poslužitelju koji je iskorišten za distribuiranje SPAM-a uvijek moguće doći do podataka o korisničkom računu koji je iskorišten za prosljeđivanje SPAM poruka (ukoliko log zapisi postoje). Identificiranim korisnicima redovito bi se blokirali korisnički računi, što bi zahtijevalo daljnje pronalaženje načina za distribuciju SPAM-a.

2.3. Otvoreni *proxy* poslužitelji

Pojavom tehnologija kao što su xDSL, kabelski modemi (engl. *Cable modem*) i sl, koje i kućnim korisnicima omogućuju relativno brzi pristup Internetu, dodatno se olakšalo distribuiranje SPAM sadržaja. Jedini problem bio je u činjenici što svega par davatelja Internet usluga (engl ***I**nternet **S**ervice **P**rovider*) u pojedinim zemljama svojim korisnicima nudi takve usluge. Identifikacija korisnika koji pristup Internetu koriste u svrhu distribuiranja SPAM sadržaja najčešće bi podrazumijevala ukidanje njihovih korisničkih prava, što bi istima otežalo pronalaženje novih korisničkih računa s bržim pristupom Internetu.
Kako bi prikrili svoje IP adrese, odnosno izvor SPAM poruka, te na taj način izbjegli ukidanje Internet pristupa, *spammeri* su pribjegli jednoj od dobro poznatih tehnika koju neovlašteni korisnici vrlo često koriste za prikrivanje konekcija. Radi se o otvorenim *proxy* poslužiteljima.
Proxy poslužitelji u svojoj legitimnoj primijeni korisnicima omogućuju brži pristup Web sadržajima na Internetu te eventualnu autentikaciju prilikom pristupa različitim Internet resursima (npr. Web, FTP i

sl.). Pohranjivanjem češće posjećivanih Web stranica (engl. *Caching*), *proxy* poslužitelji osim boljih performansi korisnicima nude i novčanu uštedu, što su osnovni razlozi njihovog korištenja.
IP adrese klijenta koji Internet resursima pristupaju preko *proxy* poslužitelja prepisuju se u IP adresu njegovog javnog sučelja, tako da se odredišnom poslužitelju čini kao da konekcija dolazi s *proxy* poslužitelja, a ne od klijenta koji je zaista inicirao konekciju. Upravo spomenuto svojstvo *proxy* servisa neovlašteni korisnici vrlo često koriste u svrhu prikrivanja konekcija s kojih provode napade.
Dodatni problem predstavlja spoznaja da većina *proxy* poslužitelja u svojoj inicijalnoj konfiguraciji omogućuje prosljeđivanje konekcija bez obzira na njihovo podrijetlo (*open proxy* poslužitelji). Ovaj, vrlo česti sigurnosni propust u konfiguraciji *proxy* sustava, neovlaštenim korisnicima omogućuje jednostavno prikrivanje podrijetla konekcija, što su i distributeri SPAM sadržaja iskoristili u svoju korist. Prosljeđivanje SMTP konekcija kroz HTTP, WinGate, SOCKS i druge *open proxy* poslužitelje postala je uobičajena praksa *spammera* prilikom distribuiranja SPAM sadržaja. Kombiniranjem otvorenih *proxy* i otvorenih *mail relay* poslužitelja te lažiranjem zaglavlja poruka moguće je vrlo efikasno prikrivanje izvora poruke.
Slično kao i kod otvorenih *mail relay* poslužitelja, liste otvorenih *proxy* poslužitelja dostupne su na Internetu. *Spammeri* ovakve liste koriste u svrhu pronalaženja novih resursa za distribuciju SPAM-a, dok neki mrežni administratori vrlo često ovakve liste koriste za određivanje IP adresa s kojih blokiraju SMTP konekcije.
Vrlo brzo razvijene su brojne metode u svrhu suzbijanja SPAM sadržaja distribuiranih putem *open proxy* poslužitelja. S obzirom da su poznati mrežni portovi na kojima su najčešće pokrenuti *proxy* servisi, jedna od metoda uključivala je provjeru da li je neki od takvih portova otvoren na računalu koje inicira SMTP konekciju. Ukoliko se pokaže da je konekcija inicirana s poslužitelja na kojem je pokrenut *proxy* servis, ista se prekida, čime se djelomično eliminira mogućnost primanja SPAM poruka.
Danas je dostupan i velik broj javnih lista otvorenih *proxy* poslužitelja za koje je poznato da se intenzivno koriste u svrhu distribucije SPAM sadržaja. Blokiranje konekcija s tih IP adresa u kombinaciji s ostalim metodama u velikoj mjeri pomaže u borbi protiv SPAM-a.
U siječnju 2003. godine prvi se puta pojavio crv za Windows operacijske sustave pod imenom Sobig.a. Nakon infekcije sustava, crv s Interneta dohvaća i instalira *proxy* poslužitelj koji će se kasnije iskoristiti za prikrivanje konekcija neovlaštenih korisnika (u ovom slučaju *spammera*). Provedena analize pokazale su da su maliciozne datoteke crva vrlo vješto prikrivene na sustavu što prilično otežava njegovu detekciju i analizu.
Maliciozni *proxy* poslužitelj pokrenut je na posve nestandardnim mrežnim portovima i ne bilježi nikakve podatke o proslijeđenim konekcijama.. Ovakav pristup gotovo je idealan za distribuiranje SPAM sadržaja, što upućuje da se radi o malicioznom programu razvijenom isključivo u tu svrhu.

3. Metamorfni trojanski konj

Sigurnosni stručnjaci, na temelju provedenih analiza, smatraju kako maliciozni *proxy* poslužitelj koji dolazi kao dio Sobig.a virusa nije prvi puta viđen. Slično ponašanje uočeno je i kod nekih drugih mrežnih crva (engl. *Worm*) i *trojana* (engl. *Trojan horse*), primijećenih u kolovozu 2002. godine. Iako ova povezanost nikada nije potvrđena, smatra se da je programer Sobig.a crva već ranije eksperimentalno razvijao maliciozne programe sličnih karakteristika.
Povezivanje Sobig.a crva s eventualnim prethodnikom dodatno je otežano, budući da se crv, zajedno sa svojom *trojan* komponentom, vrlo vješto prikriva na sustavu, pri čemu koristi napredne tehnike širenja i inficiranja sustava. Prema svojim karakteristikama, stručnjaci su Sobig.a crv sa njegovim komponentama proglasili kao metamorfni trojanski konj (engl. *Metamorphic trojan horse*). Ovakav zaključak izveden je iz činjenice da se infekcija sustava odvija u fazama koje ponekada traju i do nekoliko dana, pri čemu nerijetko sljedeća faza u potpunosti zamjenjuje prethodnu. Nakon nekoliko faza komponenta crva se uklanja iz programa i program se više ne širi na druga računala. U tom trenutku je virus u potpunosti evoluirao u *trojan* aplikaciju.
U nastavku slijedi kratki opis pojedinih faza razvoja Sobig.a crva.

3.1. Faza 1: Sobig.a

Sobig.a crv širi se putem e-mail servisa, gdje sam crv dolazi kao privitak poruke (engl. *Attachment*) prepoznatljive po *From:* polju sa sadržajem big@boss.com.

Karakteristike e-mail poruke sa Sobig.a virusom dane su u sljedećoj tablici (*Tablica 1*).

Polje e-mail poruke	Vrijednost
From:	big@boss.cim
Subject:	Jedna od sljedećih vrijednosti: Re: Movies Re: Sample Re: Document Re: Here is that sample
Datoteka u privitku:	Jedna od sljedećih vrijednosti: Document003.pif Sample.pif Untitled1.pif Movie_0074.mpeg.pif

Tablica 1: Karakteristike poruke sa Sobig.a virusom

Crv je pisan u Visual C++ programskom jeziku, a izvršna verzija programa kriptirana je Telock 0.98 programskim paketom, kako bi se otežala njegova analiza. Telock 0.98 omogućuje enkripciju i kompresiju većinu `dll`, `exe` i `ocx` datoteka kako bi se smanjila njihova veličina te otežala njihova analiza.

Nakon pokretanja datoteke u privitku poruke elektroničke pošte sa Sobig.a crvom, maliciozni program `Winmgm32.exe` kopira se u Windows direktorij gdje se i pokreće.

Crv ima dvije osnovne zadaće. Prva je da se dalje širi kako bi se zarazila druga računala, a druga je da dobavi `reteral.txt` datoteku s adrese http://www.geocities.com/reteras/. `Reteral.txt` datoteka sadrži listu drugih URL adresa s kojih će se dobaviti sljedeće datoteke važne za širenje virusa. Tipično ova datoteka sadrži nelegitimnu http://www.blahblahblahblah.com/ Internet adresu koja je postavljena s razlogom da korisnika navede na krivi put prilikom analize načina rada i razvoja virusa. U određenim trenucima autor Sobig.a crva lažiranu vrijednost zamjenjuje s pravom URL adresom, koju vrlo brzo ponovno uklanja. U trenutku analize virusa, legitimna URL adresa glasila je http://www.loricoshop.com/users/serak/txtfile.txt.

S ove adrese virus dohvaća maliciozni *trojan* program, koji se pokreće u sljedećoj fazi razvoja virusa.

3.2. Faza 2: Lala trojan

Drugu fazu razvoja crva trenutno ne prepoznaje niti jedan antivirusni program. Budući da programer virusa koristi ranije opisano zamjenjivanje URL adresa, analiza ove faze razvoja dodatno je otežana. Osim promjene URL adrese s koje se dobavlja maliciozni program, primijećene su i periodičke promjene na samom programu, što otežava prepoznavanje virusa postojećim antivirusnim programima.

Trojan pod nazivom *Lala* (`Mptask.exe`) pisan je u Delphi programskom jeziku i također je zaštićen TeLock 0.98 programskim paketom.

Program sadrži nekoliko komponenti uključujući i onu koja vrši obavješćivanje HTTP protokolom preko CGI skripte na adresi http://www.banking-concern.com/cgi-bin/index7.cgi. Prethodne inačice programa su u istu svrhu koristile CGI skriptu pod nazivom index6.html. Na temelju ovakvih činjenica razumno je pretpostaviti da se u trenutku analize radi o sedmoj inačici trojanske komponente Sobig.a crva. CGI skripte koje se spominju u ovom kontekstu najvjerojatnije se nalaze na Web poslužiteljima nedužnih organizacija na kojima je programer crva prethodno ostvario neautorizirani pristup.

Posljednja inačica *Lala* trojanskog programa instalira i *keylogger* program zajedno s *Lithium* trojanskim programom, koji neovlaštenom korisniku omogućuje udaljeni pristup inficiranom sustavu. Pristup *Lithium* programu moguć je jedino odgovarajućim klijentskim programom sa zaporkom `adm123`.

Lala program na identičan način, kao i u fazi jedan, dobavlja maliciozne datoteke potrebne za treću, finalnu fazu razvoja virusa. U trenutku analize pisanja dokumenta maliciozna URL adresa glasila je http://www.loricoshop.com/users/serak/g5aa.txt.

Navedena datoteka sadrži `g5aa.exe` program koji se smješta u standardni Windows direktorij (npr. WINNT i sl.). Analize su pokazale da se radi o instalacijskom programu poznatog WinGate *proxy* poslužitelja, pri čemu su naravno prekršena prava licenciranja ovog, inače komercijalnog, programa.

3.3. Faza 3: WinGate

Kako je spomenuto u prethodnom poglavlju, Wingate (inačica 5.0.2) *proxy* poslužitelj zapakiran je u spomenutu `g5aa.exe` malicioznu datoteku koju *Lala* program dohvaća kao zadnji korak duge faze. U odnosu na legitimnu inačicu istog poslužitelja, program dolazi s nešto izmijenjenom konfiguracijom, s podrškom za sljedeće TCP servise:

- Port 555 - RTSP Streaming Media Proxy;
- Port 608 - Remote Control Service servis;
- Port 1180 - SOCKS Proxy poslužitelj;
- Port 1181 - Telnet Proxy poslužitelj;
- Port 1182 - WWW Proxy poslužitelj;
- Port 1183 - FTP Proxy poslužitelj;
- Port 1184 - POP3 Proxy poslužitelj;
- Port 1185 - SMTP poslužitelj.

Remote Control Service servis (TCP port 608), neovlaštenom korisniku omogućuje pristup instaliranom *proxy* poslužitelju uz pomoć Wingate Gatekeeper klijentskog programa. Uz pomoć spomenutog klijentskog programa i odgovarajuće zaporke moguće je nadzirati i upravljati radom *proxy* poslužitelja. Inicijalna zaporka koju koristi maliciozna inačica programa glasi `zaq123`.
Mogućnost udaljenog upravljanja i nadzora malicioznog *open proxy* Wingate poslužitelja može se iskoristiti u svrhu praćenja i analize postupaka *spammera*, pogotovo onih manje iskusnih koji su uvjereni da njihove aktivnosti u ovom slučaju ostaju potpuno anonimne.

4. Preporuke za uklanjanje crva

Ukoliko je sustav zaražen Sobig.a crvom, a maliciozni program iz druge faze još nije aktiviran, crv je moguće odstraniti uklanjanjem sljedećeg *registry* ključa:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WindowsMGM=C:\%WI
NDOWS%\Winmgm32.exe
```

Također je potrebno provjeriti da li postoji još koja veza (engl. S*hortcut*) koja će omogućiti pokretanje programa kod pokretanja sustava (*Startup* direktorij i sl.). Ukoliko takva ne postoji, potrebno je iznova pokrenuti operacijski sustav (engl. *Restart*) te ukloniti `Winmgm32.exe` program iz Windows direktorija. Ukoliko je širenje crva doseglo drugu fazu njegovog razvoja, biti će potrebno ukloniti i ostale *registry* zapise, odnosno datoteke uključene u njegovo daljnje širenje.
Maliciozni programi uključeni u drugu fazu razvoja crva pokreću se putem sljedećih *registry* vrijednosti:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MPtaskServices=C:\%WINDOW
S%\%SYSTEM%\mptask.exe
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MPtaskServices=C:\%WINDOW
S%\%SYSTEM%\pntask.exe
```

Za pokretanje programa treće faze zadužen je sljedeći *registry* ključ:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MMtaskService=mmtask.exe
```

Uklanjanjem navedenih *registry* zapisa te pripadajućih malicioznih datoteka ukloniti će sve komponente Sobig.a crva sa sustava.
Manje iskusnim korisnicima može se preporučiti korištenje gotovih programa koji će obaviti analizu sustava te ukloniti komponente virusa, ukoliko je isti detektiran. Jedan od takvih programa moguće je naći na adresi:

http://securityresponse.symantec.com/avcenter/ venc/data/w32.sobig.a@mm.removal.tool.html

5. Zaključak

U ovom dokumentu iznesena je analiza Sobig.a crva, specifičnog po nekoliko elemenata. Za razliku od većine drugih crva, program na zaraženom sustavu instalira modificiranu inačicu Wingate *proxy* poslužitelja što upućuje na činjenicu da je program razvijen isključivo u svrhu lakšeg distribuiranja SPAM sadržaja. Analiziran je način širenja crva prema pojedinim fazama zajedno s malicioznim komponentama koje sadrži.