

Downadup Codex

Vodič kroz mehaniku virusa/pretnje.

Uvod

Još od svoje pojave krajem 2008.g., Downadup worm je postao jedna od najraširenijih pretnji koja je zadesila Internet u zadnjih par godina. Sa složenim zlonamernim kodom, ova pretnja je bila u mogućnosti da preskoči mnoge mrežne zabrane, sakrije se u senci normalnog mrežnog saobraćaja i brani se od uklanjanja na način koji je retko viđen u dosadašnjim pretnjama. Pri svemu tome, sadrži i nekoliko do sada neviđenih mogućnosti. Ipak ono po čemu se definitivno izdvaja je broj trikova "iz rukava" koje ova pretnja sadrži.

Sve je počelo sredinom oktobra 2008.g. kada su primećeni prvi ciljani napadi koji su iskorišćavali tada nepoznatu ranjivost Windows remote procedure call (RPC) servisa. Microsoft je brzo objavio van uobičajenog režima izdavanja sigurnosnih patch-eva, novi patch (MS08-067), naznačavajući ga kao "kritičan" za deo operativnih sistema – što je najviši stepen opasnosti kod Microsoft Security Bulletin-a.

Nije bilo potrebno mnogo vremena da autori malware-a krenu sa zloupotrebom ove ranjivosti u svojim zlonamernim kodovima. Početkom novembra pojavili su se W32.Kernelbot.A i W32.Wecorl, koji su pokazali delimičan uspeh korišćenja MS08-067 ranjivosti.

Onda se krajem Novembra pojavio W32.Downadup (takođe nazvan Conficker od strane dela drugih proizvođača antivirusa). Ova pretnja je postigla skroman uspeh u propagaciji, delom zahvaljujući radu na Metasploit Project, koji je razvijao metode koji su pokazivali kako se ranjivost može iskoristiti.

Broj inficiranih računara sa W32.Downadup je počeo da raste. Ograničavajući faktor za uspeh je bila činjenica da se rutina za propagaciju oslanjala na dostupne GeolP podatke kako bi odredila lokaciju IP adrese. Kada su autori GeolP odlučili da uklone podatke sa lokacije koju je koristio ovaj crv (worm), nepostojanje podataka je onemogućilo dalje brzo širenje infekcije, ograničavajući infekciju samo na lokalnu mrežu u kojoj se nalazio inficirani računar.

Naravno, autori Downadup-a se nisu dali prevariti, spakovali su GeolP podatke u novu varijantu—W32.Downadup.B—zajedno sa kolekcijom trikova ravnom švajcarskom nožiću, nadajući se da će to pomoći širenju crva naširoko i nadaleko.

Ovo je bila jedna od stvari koja je izdvojila Downadup crv od ostatka pretnji koje smo videli tokom zadnjih par godina—njegova tehnička mnogostranost. Ugrađeni trikovi nisu bili novi; samo ih je bilo tako mnogo. Crv je skenirao mrežu tražeći ranjive računare, ali je nije gušio saobraćajem, birajući koje računare skenira u pokušaju da se sakrije. Pokušavao je da iskoristi najčešće korišćenje šifre za mrežni pristup. Koristio je Universal Plug and Play da prođe kroz rutere i mrežne prolaze (gateways). Ako bi se mreža pokazala dovoljno sigurnom, koristio je pametan trik sa AutoPlay mogućnošću da se pokrene sa prenosnih diskova.

Crv je imao i sopstvenu zaštitu od preuzimanja. Prenešeni fajlovi (koje je crv dovlačio) su bili kriptovani, ali i digitalno potpisani i samo su autori Downadup-a imali ključ. Instaliranje patch-a MS08-067 je zaustavljalo dalje korišćenje ranjivosti od strane drugih napadača ili pretnji. Autori crva su čak poklonili posebnu pažnju da spreče buffer overflow u sopstvenom kodu. Niko nije mogao da "otme" potencijalnu mrežu bot-ova ovog crva.

Skrivena opasnost iza svega ovoga jeste potencijalni dodatni teret (payload)—Downadup ima mogućnost da se ažurira ili preuzme dodatne fajlove koje može da izvrši. Ponovo, ne radi se o novoj tehnici, ali u ovom slučaju crv je generisao listu od preko 250 novih domena na koje je mogao da se konektuje i to svaki dan. Svaki od tih domena je mogao da ima novu verziju koja bi dozvolila dalje zlonamerne akcije. Kakve? Bilo šta što autori žele i ne samo to, pretnja sadrži i

sopstveni peer-to-peer (P2P) mehanizam za ažuriranje, omogućavajući da jedan inficiran računar ažurira drugi. Blokiranje pristupa domenima može biti zaštita sa jedne strane, ali blokiranje P2P ažuriranja je potpuno druga priča.

Broj infekcija je počeo da opada sredinom februara, kako su se vesti o ovoj pretnji širile i kako su administratori počeli sa masovnom primenom MS08-067 patch-a kako bi zaštitili svoje mreže. Moguće je da je urok pada i činjenica da je sa uspehom u propagiranju, pretnja dobila prilično pažnje. Domeni koji su trebali da pruže ažuriranje su pažljivo nadgledani od strane security proizvođača, istraživača i medija.

Ovakva pažnja nije iznenađenje imajući u vidu složenost ove pretnje i način na koji koristi mnoštvo oprobanih malicioznih trikova, otkrivajući usput i par novih. Nema sumnje da je Downadup vruća tema za 2009.g., barem do sada, a ovakva pažnja je izazvala i značajan broj istraživanja.

Sve se smirilo po pitanju Downadup do početka marta, kada se pojavio W32.Downadup.C na prethodno inficiranim Downadup kompjuterima. Više se radi o novoj verziji, nego o novom crvu, a ova verzija nije uključivala tehniku propagacije. Novost kod ove verzije je mogućnost da zaustavi niz procesa vezanih za sigurnost. Takođe, dok je prethodna verzija generisala 250 novih domena, ova je generisala 50,000.

Do sredine marta, Symantec Security Response je objavio 14 blog zapisa opisujući detalje različitih mogućnosti Downadup-a od novembra 2008.g do februara 2009.g. uključujući i višestruku analizu mogućnosti ovog crva gde se svaki blog zapis odnosi na određenu mogućnost. Ova analiza objedinjuje sve ove izveštaje i zapise.

Kako su informacije na blogu objavljivanje hronološki, nisu pokrivalo samo tehnički aspekt, već i istorijski kontekst pojave i širenja Downadup crva. Da bi Vam omogućili kompletan pregled, ovaj rad uključuje i nove, do sada neobjavljene informacije od strane Symantec Security Response istraživača.

Kao sveobuhvatnu kolekciju Symantec analize crva, predstavljamo vam Downadup Codex.

U daljem tekstu dajemo prevod objavljenih članaka (za većinu interesantnih, za ostale samo kratak pregled), sa linkovima na potpune verzije. U tekstu se nalazi i članak koji do sada nije objavljen (tiče se propagacije korišćenjem UPnP-a). Dodatno, u ovaj pregled su uključena i poslednja istraživanja koja se tiču nove verzije i motivacije autora Downadup-a.

Increase in exploit attempts against MS08-067

Originally published November 22, 2008 by the Security Intel Analysis Team

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/vulnerabilities_exploits/article-id/178

Ovo je jedan od prvih objavljenih članaka u vezi povećanog korišćenja ranjivosti MS08-067. Ovde izdvajamo samo najinteresantniji deo.

Primećeno je da crv cilja TCP port 445 kako bi iskoristio opisanu ranjivost, te ako uspe, crv kreira HTTP server na inficiranom računaru na slučajno odabranom portu, na primer:

```
http://[EXTERNAL IP ADDRESS OF INFECTED MACHINE]:[RANDOM PORT]/[RANDOM STRING]
```

Zatim crv šalje opisani URL kao deo svog dodatnog tovara udaljenim računarima. Kada u potpunosti uspe, crv se povezuje sa nekim od domena gde ga čeka još pretnji i preuzima novi sadržaj.

Preporučuje se sledeće kako bi se izbegla opasnost:

- Blokiranje pristupa TCP port 139 i 445 na mrežnim obodima
- Obezbediti se da računari u mreži imaju instaliran host-based firewall
- Obezbediti se da je antivirus instaliran i ažuran
- Instalirajte patch MS08-067 što je pre moguće. Microsoft je takođe predložio brojne dodatne načine zaštite u svom biltenu, kao što je isključivanje browser servisa. Savetujemo da pročitate sve navedene sugestije

Symantec IPS će detektovati blokirati sledeće potpise:

- MSRPC Server Service Buffer Overflow
- RPC Server Service B02

W32.Downadup infection statistics

Originally published January 6, 2009 by the Security Intel Analysis Team

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/224

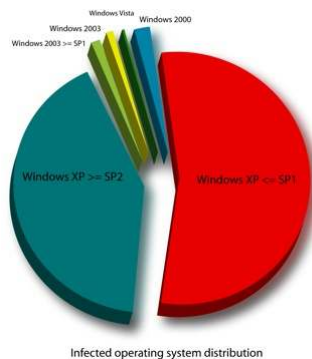
New variants of W32.Downadup.B find new ways to propagate

Originally published January 9, 2009 by Symantec Security Response

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/225

Oba gore navedena članka smo svojevremeno poslali kroz naš bilten našim korisnicima, kada je primećeno da se ovaj crv pojavio i u našim krajevima. Kratak pregled ova dva članka je dat u sledećim redovima.

Crv [W32.Downadup.A](#) je prvi koji je otkriven da uspešno koristi ranjivost [MS08-067](#) u širem smislu. Symantec je izvršio analizu ove pretnje i utvrdio da crv generiše 250 slučajnih domen adresa svaki dan, u nastojanju da ih upotrebi kasnije radi preuzimanja i izvršavanja novih verzija. Ovo je interesantna i sve popularnija tehnika koju koriste autori malicioznog koda. Ono što je takođe interesantno kod metode preuzimanja binarnog ažuriranja za crv jeste da je Symantec iskoristio da proceni širenje infekcije i rasprostranjenost po operativnim sistemima. Tokom jedne nedelje, Symantec je detektovao preko tri miliona jedinstvenih IP adresa u pokušaju da ažuriraju crv. Analizom zahteva došlo se i do distribucije po inficiranim operativnim sistemima. Sledeći grafik prikazuje distribuciju po OS-ovima u periodu posmatranja od 72 sata:

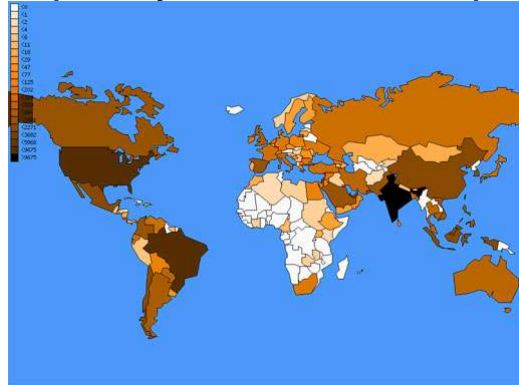


Kao što se na grafiku može videti, najviše je inficiranih Windows XP SP1 i starijih sistema. Preko 500,000 inficiranih računara je upravo sa ovom verzijom OS-a. Odmah iza njega je bio Windows XP SP2 i noviji. Windows 2000 i Windows 2003 imaju sličan broj infekcija.

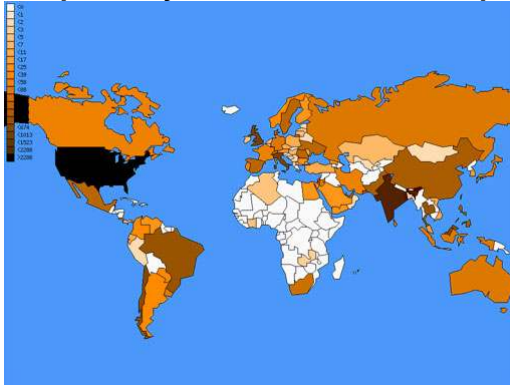
Verujemo da je način propagacije W32.Downadup.A veoma agresivan. Ovaj crv će nastaviti da se širi i dalje, a putem mehanizma ažuriranja moći će da uzima nove oblike i verzije. Symantec je otkrio novu verziju ovog crva 30. decembra 2008.g., označenu kao [W32.Downadup.B](#). Nova verzija sadrži dodatne načine propagacije i izmenjen način generisanja domena. Još novija verzija, [W32.Downadup!autorun](#) se pojavila 7. januara 2009.g. Upravo zahvaljujući načinu preuzimanja novih verzija samog crva, treba očekivati još varijanti. Nova verzija, nazvana [W32.Downadup.B](#), koja se pojavila 30. decembra širi se ne samo korišćenjem ranjivosti Microsoft Windows Server Service RPC Handling Remote Code Execution, već i putem mrežnih deljenih diskova i USB-ova (autorun) i koristeći slabe šifre. Ovi načini propagacije nisu ništa novo; W32.Spybot, W32.Randex i W32.Mytob varijante koriste skoro identične metode za širenje, ali ova varijanta zahteva više napora da se zaštite mreže u preduzećima.

W32.Downadup.B kreira autorun.inf fajl na svim mapiranim diskovima tako da se crv pokrene čim se diskovima pristupi. Dalje, crv prati diskove priključene na zaražen računar kako bi kreirao novi autorun.inf fajl na svaki disk koju mu postane dostupan. Crv takođe prati i DNS zahteve koji sadrže definisane reči i blokira pristup tim domenima tako da izgleda kao da mreža ne radi. Ovo znači da zaraženi korisnici možda neće moći da ažuriraju svoje antivirusne sa tih web sajtova. Ovo može biti problem jer autori crva konstantno kreiraju nove verzije i varijante.

Rasprostranjenost crva W32.Downadup



Rasprostranjenost crva W32.Downadup.B



Neophodno je da što hitnije primenite patch za [Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability](#).

Symantec preporučuje da se svi sistemi osiguraju od Microsoft Windows Server Service RPC Handling Remote Code Execution ranjivosti, da se preuzmu koraci za sprečavanje automatskog pokretanja aplikacija korišćenjem autorun.inf fajlova na prenosnim i mrežnim diskovima i da se sprovede politika složenih šifri za sve računare i servere u mreži. Budući da tokom praznika sistemi verovatno nisu uredno ažurirani (patch-ovani) ovo je doprinelo još bržem širenju ovog crva. U slučaju da već nemate – razmislite o uvođenju automatskog sistema za patch management.

W32.Downadup and W32.Downadup.B statistics

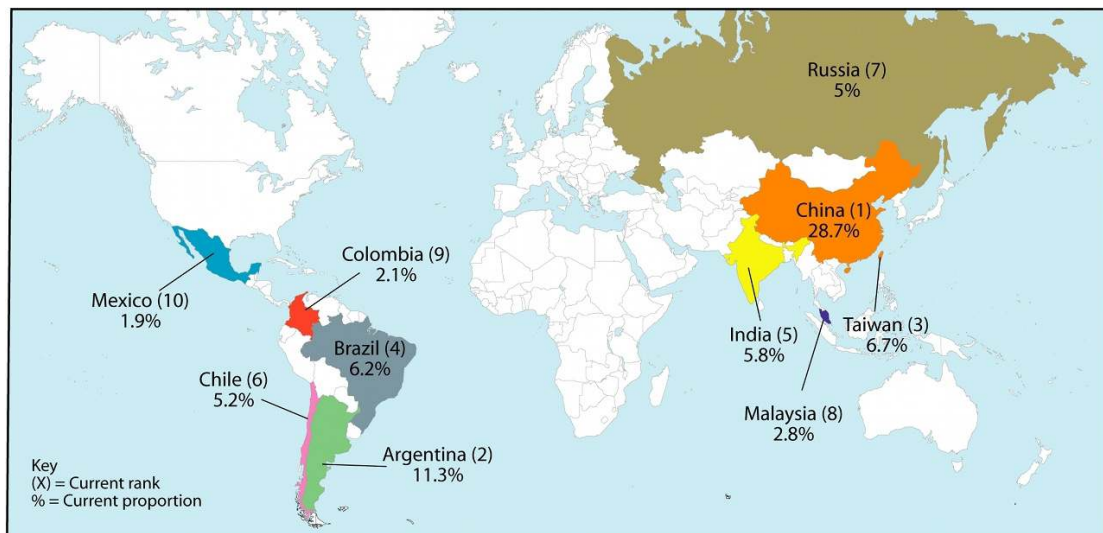
Originally published January 16, 2009 by the Security Intel Analysis Team

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/226

Symantec Intelligence Analysis Team prati infekcije Downadup-a od sredine decembra 2008.g.

W32.Downadup je izuzetno interesantan zlonamerni kod i jedan od aktivnijih u poslednje vreme. Zaslužni za to su većinom korisnici Windows XP SP2 i Windows 2003 SP1 sistema koji nemaju instaliran MS08-067 patch.

Symantec Intelligence Analysis Team je pratio rasprostranjenost i poreklo i u ovom članku možete naći grafički predstavljenu rasprostranjenost virusa i top 10 zemalja po broji inficiranih računara.



Peer-to-peer payload distribution

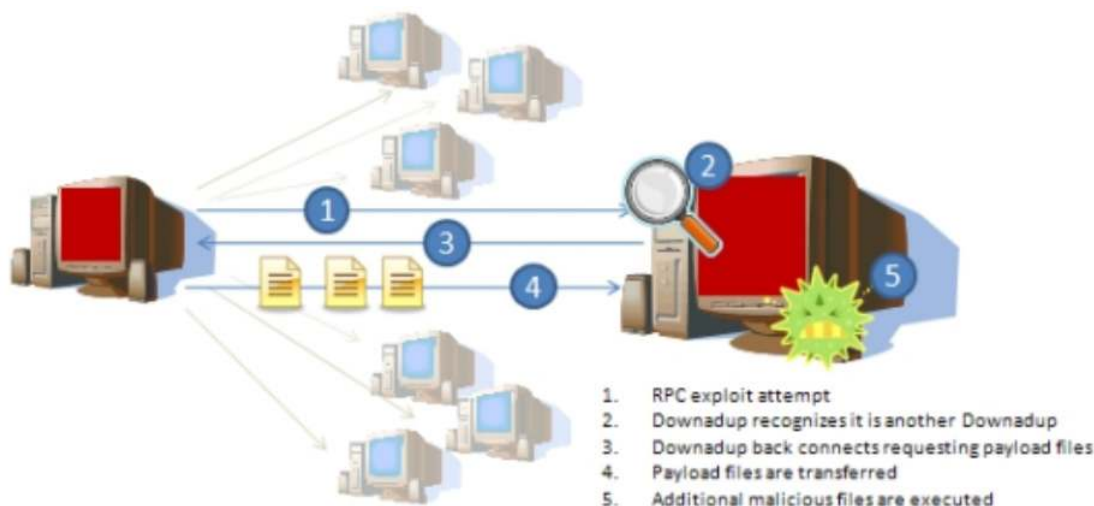
Originally published January 19, 2009 by Eric Chien

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/227

Dok se deo istraživača bavi procenama rasprostranjenosti Downadup (tj. Conficker) crva, očekujemo da se pojave i novi oblici. U ovom trenutku, Downadup se replicirao na više od 4-5 miliona mašina – za sada bez očekivanog dodatnog tereta. Pre deset godina, sama replikacija je bila dovoljna motivacija za većinu pretnji, dok se kod današnjih pretnji motivacija svodi na novac. Na osnovu prethodnih varijanti i karakteristika koda, verujemo da je crv u vezi sa dobro poznatom grupom pisaca zlonamernog koda koja je prethodno distribuirala mnoštvo adware-a i lažnih aplikacija (tj. lažnih antispyware proizvoda).

Crv ima dva mehanizma za preuzimanje dodatnog tereta - sadržaja (payload). Jedan je već poznat, gde se generiše lista domena svaki dan koji se kontaktiraju radi ažuriranja. Na kraju, jedan od tih domena će biti registrovan od strane autora i tu će postaviti dodatne pretnje/kod. Ipak, proizvođači kao što je Symantec takođe prate ove domene, što ih čini manje idealnim kandidatom za autore pretnje, posebno ako domen bude brzo zatvoren.

Zbog toga, postoji drugi mehanizam za distribuciju dodatnih fajlova koji je teže pratiti i koji je jednako teško ugasiti. Crv koristi (potencijalno neefikasni) peer-to-peer (P2P) mehanizam koji mu dozvoljava da deli fajlove među zaraženim računarima. Mehanizam je prikazan na slici:



Tokom gore prikazanog procesa, Downadup ne samo da patch-uje RPC ranjivost u memoriji, već koristi i taj patch da prepozna pokušaj iskorišćenja ranjivosti od drugih zaraženih računara. Crv je sposoban da analizira dolazeći shellcode i proveriti da li odgovara sopstvenom. Ako odgovara, na osnovu podataka izvučenih iz shellcode može se povezati sa drugom inficiranom mašinom. Ovo "back connect" povezivanje koristi HTTP protocol, ali na slučajno odabranom portu. Druge inficirane mašine onda odgovaraju tako što šalju podatke koji sadrže dodatni sadržaj/kod.

Downadup može prenositi istovremeno više ovakvih fajlova koristeći ovaj mehanizam. Svaki od fajlova može biti kriptovan (ili barem digitalno potpisan) i sadrži header koji ima u sebi identifikator fajla i datum. Identifikator fajla dozvoljava crvu da proveriti da li mu je taj fajl već poznat i da odredi da li treba da ga ažurira. Datum se koristi kao datum isteka i ako je trenutni datum nakon datuma isteka, fajl se odbacuje. Fajlovi se stalno proveravaju i oni koji isteknu se odbacuju. Ovi fajlovi se snimaju u registry i nude se ostalim peer računarima kada ih traže, istovremeno ih zadržavajući pri restartovanju.

Kasnije se ovi fajlovi mogu snimiti na disk i pokrenuti ili učitati direktno u memoriju. Na taj način, dodatni zlonamerni kod se može pokrenuti bez potrebe da sam fajl bude zabeležen na disk.

Geo-location, fingerprinting, and piracy

Originally published January 20, 2009 by Patrick Fitzgerald

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/228

U ovom članku se piše o zemljama u kojima se najviše raširio ovaj crv i izvodi se poređenje sa stopom piraterije u tim zemljama. Deo članka govori i o iskorišćenju MS08-067 ranjivosti i operativnim sistemima koji su najviše pogođeni.

A lock with no key

Originally published January 21, 2009 by Ka Chun Leung

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/229

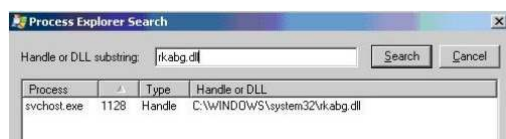
Poznato je da je W32.Downadup.B vrlo agresivan pri inficiranju računara. Pogledajmo neke od trikova koje koristi da bi ostao na inficiranom računaru. Jedan od Symantec test računara je inficiran sa W32.Downadup.B. Pri skeniranju sa starom, originalnom verzijom Norton Antivirus 2006 pojavila se sledeća greška:



Proces je "zaključao" fajl i time sprečio pristup istom. Budući da antivirus ima više načina da se izbori sa ovim, zašto to nije tako i u ovom slučaju?

Kada W32.Downadup.B inficira računar, vidimo novi fajl C:\WINDOWS\system32\rkabg.dll, a zatim i kako se instalira kao servis (u ovom slučaju kao "bmumwkv") u netsvcs servis grupi. Dakle, zaustavljanjem ovog servisa, moći će da se "oključa" fajl.

Ipak, kada se pogleda, izgleda kao da je servis već zaustavljen. Bliži pogled na servise i procese na računaru ne otkriva ništa sumljivo, ali nešto mora da drži taj fajl zaključanim. Process Explorer od Sysinternals (koji je sada deo Microsoft-a) ima mogućnost da pronade koji proces pristupa fajlu:



Svchost.exe—proces koji je ugostio servis koji je kreirao W32.Downadup.B—drži zaključanim i pokrenutim, čak i kada je W32.Downadup.B servis nije pokrenut. Dodatna analiza pokazuje da se W32.Downadup.B servis pokreće pri podizanju

računara, a zatim ubacuje kod u service host pre nego što se sam zaustavi. Ovaj trik pali kod iznenađujućeg velikog broja antivirusnog softvera.

Kada se zatvori file handle u Process Explorer-u, skeniranje nastavlja kako je i očekivano:



Dakle, dok ovo može predstavljati problem u verziji 2006, ali novije verzije Symantec proizvoda više nemaju ovaj problem.

Ne zaboravite, ako mislite da ste inficirani sa Downadup i imate problema da ga detektujete i uklonite, uvek možete da preuzmete

Symantec alat za uklanjanje ovog crva sa:

http://www.symantec.com/content/en/us/global/removal_tool/threat_writeups/FixDwndp.exe

Small improvements yield big returns

Originally published January 22, 2009 by Elia Florio

<https://forums2.symantec.com/t5/Malicious-Code/Downadup-Small-Improvements-Yield-Big>Returns/ba-p/381717>

U ovom članku se opisuju unapređenja koja donosi W32.Downadup.B verzija u odnosu na prethodnu.

Attempts at smart network scanning

Originally published January 23, 2009 by Eric Chien

<https://forums2.symantec.com/t5/Malicious-Code/Downadup-Attempts-at-Smart-Network-Scanning/ba-p/382114>

Mogućnost pretnje da se proširi naširoko često zavisi od algoritma pronalaženja drugih računara na Internet-u, koji su predstavljeni svojom IP adresom. Downadup koristi niz tehnika da skenira nove mašine kako bi povećao mogućnosti širenja, a istovremeno smanjujući šansu da bude primećen.

Skeniranje mreže samo golom silom (brute-force) može dovesti do primetnog usporenja i problema u radu mreže kod inficirane mašine. Downadup pokušava da ograniči svoj uticaj na dva načina. Prvo, crv kontaktira dva poznata web sajta i računa prosečnu brzinu veze i raspoloživ propusni opseg, a zatim koristeći ove vrednosti konfiguriše koliko istovremenih pokušaja remote procedure poziva (RPC) mu je dozvoljeno. Drugo, nakon svakog skeniranja, pauzira—od 100 milisekundi do dve sekunde—zavisno od tipa skeniranja i da li se računar koristi ili ne. (Downadup proverava korišćenje računara određujući da je neko koristio tastaturu u prethodnih 5 minura.)

Downadup pokušava na četiri različita načina skeniranje, koje se ponavlja u beskonačnoj petlji. Prvo skenira mašine koje su na istoj podmreži - subnet, mašine koje je prethodno uspešno inficirao, mašine koje su u blizini - takođe prethodno inficirane i slučajno izabrane mašine.

Prvo, Downadup sekvencijalno skenira sve IP adrese iz istog opsega u kom je i inficirana mašina, počinjući od prve IP adrese u podopsegu. Uključeno je više podopsega ako mašina ima više IP adresa iz različitih opsega.

Dalje, Downadup pokušava da iskoristi ranjivost prethodno inficiranih mašina. Ovo radi iz dva razloga—prvi, da ponovo inficira mašinu koja je možda očišćena i drugo, da inicira peer-to-peer (P2P) komunikaciju kako bi primio novi sadržaj (payload) kao što je opisano u članku: Peer-to-Peer Payload Distribution. Crv pamti samo poslednjih 100 uspešno inficiranih mašina.

Zatim, Downadup počinje sa generisanjem slučajnih IP adresa za napad. Moguće da su pojedine IP adrese izostavljene zbog bug-a, što delimično ograničava napad. Downadup može da generiše samo oko četvrtine od ukupnog broja IP adresa, što ograničava mogućnost da dođe do dela IP adresa sa RPC ranjivošću.

Konačno, paralelno, Downadup će skenirati i mašine koje su blizu ostalih mašina koje su uspešno iskorišćene. Za svaku inficiranu mašinu, Downadup skenira klasu C (/24) bloka IP adresa i prethodnih 10 klasa C (/24) blokova. Na primer, ako je uspešno iskorišćena mašina sa IP adresom 208.77.188.166, Downadup će skenirati opseg od 208.77.178.1 do 208.77.188.255.

```

; Avira
<0, 104, 199, 91> ; Bitdefender
<255, 104, 199, 91>
<0, 209, 88, 192> ; Computer Emergency Respo
<255, 209, 88, 192>
<0, 88, 242, 207> ; Computer Associates
<255, 88, 242, 207>
<192. 43. 42. 12> : Computer Associates

```

Pored toga, Downadup ne skenira svaku IP adresu iz izračunatog opsega. Na primer, IP opseg kao što je 127.x.x.x ili 169.254.x.x se preskače. Ono što je još važnije, Downadup sadrži veliku crnu listu IP opsega koji pripadaju proizvođačima sigurnosnog softvera. Deo liste možete videti na slici pored.

Ne pokušavajući da se skenira proizvođače sigurnosnog softvera, Downadup izbegava honeypot sisteme. Ova crna lista se koristi i da odbije konekcije koje dolaze sa nje, sprečavajući proizvođače sigurnosnog softvera da dobiju novi payload radi analize.

Downadup će na kraju obnoviti listu IP adresa konfigurisanih na lokalnoj mašini. Ako je bilo koja promenjena od kako je skeniranje počelo, skeniranje će se prekinuti jer je exploit dizajniran da se konektuje nazad na prethodno konfigurisanu IP adresu.

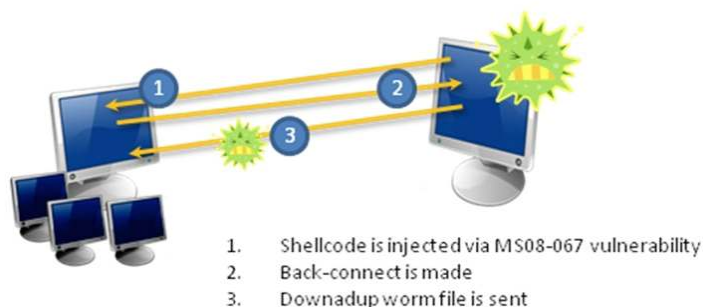
Znajući IP adresu na koju treba da se konektuje ponovo, pokreće još jedan problem kod Downadup-a. Sa mnogim kućnim korisnicima iza wireless rutera, firewall-ova i onih koji koriste NAT, mnoge inficirane mašine se ne mogu kontaktirati sa spoljašnjih mašina. Downadup pokušava da prevaziđe ovo ograničenje – o tome više u nastavku.

Playing with Universal Plug and Play

Originally published January 28, 2009 by Eric Chien

<https://forums2.symantec.com/t5/Malicious-Code/Downadup-Playing-with-Universal-Plug-and-Play/ba-p/383244>

Pored ostalih metoda, Downadup inficira druge mašine putem remote procedure call (RPC) ranjivosti MS08-067. Korišćenjem ove ranjivosti, crv ubacuje shellcode koje se konektuje nazad na inficiranu mašinu. Ovo je poznato kao back-connect. Back-connect radi preko HTTP-a na slučajno izabranom portu, a inficirana mašina odgovara slanjem crva. Shellcode prima ovaj fajl i izvršava ga, inficirajući tako drugi računar.



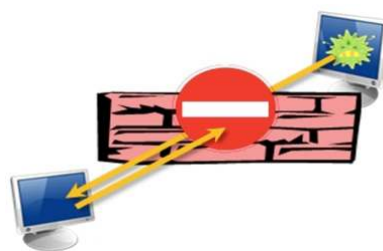
Ipak, mnogi korisnici danas koriste rutere ili druge Internet gateway uređaje koji sprečavaju mašine spolja da se povežu sa računarima unutra uz korišćenje NAT-a. Ovo bi u normalnim okolnostima sprečilo Downadup-ov shellcode da uspešno obavi inficiranje jer back-connect ne bi uspeo.

Da bi prevazišao ovo, Downadup mora da izvede tri akcije; da utvrdi da li se mašina nalazi iza gateway uređaja, da dođe do spoljašnje IP adrese i da se obezbedi da dolazeće konekcije spolja budu prosleđene ka mašini/računaru unutra. Ovo je poznato kao port forwarding. Downadup koristi Universal Plug-and-Play (UPnP) protokol da postigne ovaj zadatak.

UPnP protokol podržava većina uobičajenih gateway uređaja koji se koriste u kućnim okruženjima. Da postigne prvi zadatak, Downadup koristi UPnP-ov discovery protocol, koji je zasnovan na Simple Service Discovery Protocol (SSDP). Ovaj protokol omogućava mašinama na mreži da otkriju druge gateway uređaje na mreži.

Kao deo SSDP, Downadup šalje jedan M-SEARCH zahtev na multicast adresu 239.255.255.250 na portu 1900/udp i zatim sluša odgovore. M-SEARCH zahev traži heder poznat kao cilj pretrage (predstavljen sa "ST") koji predstavlja tipove uređaja ili servisa koje Downadup traži. Oni su predstavljeni sa tzv. universal resource identifiers (URI). Downadup traži jedan od sledećih četiri uređaja ili servisa:

urn:schemas-upnp-org:device:InternetGatewayDevice:11.
 urn:schemas-upnp-org:service:WANIPConnection:12.
 urn:schemas-upnp-org:service:WANPPConnection:13.
 upnp:rootdevice (represents all UPnP devices)4.



Ovde je i primer sadržaja jednog paketa koji sadrži M-SEARCH zahtev:

```
M-SEARCH * HTTP/1.1HOST: 239.255.255.250:1900ST: urn:schemas-upnp-
org:device:InternetGatewayDevice:1MAN: "ssdp:discover"MX: 3
```

Ako odgovarajući uređaj postoji na mreži, uređaj će odgovoriti sa porukom koja sadrži dodatni URI koji daje informacije o uređaju i servisima koje uređaj podržava. Nakon provere da li je uređaj odgovarajući, Downadup šalje UPnP GetStatusInfo zahtev da se uveri da je uređaj trenutno povezan na mrežu sa WAN interfejsom (Internet-om). Ovim se završava prva faza određivanja da li se mašina nalazi iza gateway uređaja.

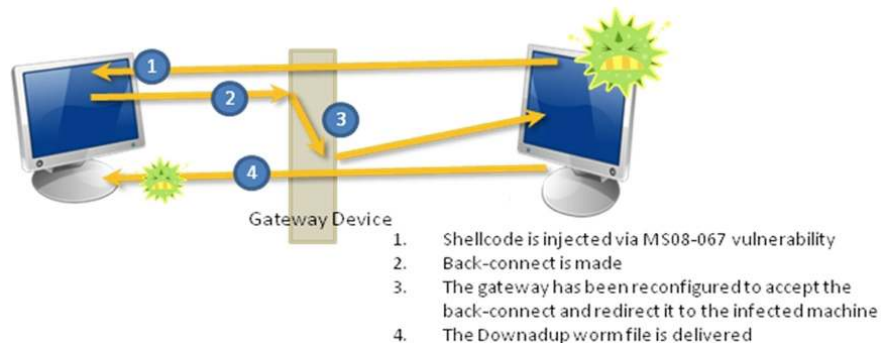
Dalje, šalje se UPnP GetExternalIPAddress komanda uređaju da bi se dobila spoljašnja IP adresa čime se završava i drugi korak. Ovo je IP adresa koja je vidljiva spolja, ostalim mašinama na Internet-u.

Konačno, Downadup treba port za prosleđivanje dolaznih zahteva kroz gateway do inficirane mašine. Zahtev za prosleđivanje portova traži nekoliko parametara; u ovom slučaju su relevantni oni koji se tiču opisa, spoljašnjeg porta na kome se sluša, interne IP adrese i porta na koji se prosleđuje dolazni saobraćaj.

Opis polje se generiše iz Volume Serial Number i naziva računara koji je inficiran. Ovim se kreira prilično jedinstven opis. Downadup šalje GetGenericPortMappingEntry komandu gateway uređaju da označi postojeće zapise za prosleđivanje portova kako bi se videlo da li neki već odgovara generisanom opisu. Ako se podudaraju, crv pretpostavlja da se radi o prethodnim zapisima koje je generisao i koje je obrisao korišćenjem UPnP DeletePortMapping komande.

Zatim se dodaje novi zapis za prosleđivanje portova sa AddPortMapping komandom. Downadup pokušava da upotrebí port 80 za spoljašnji port, a interni port je slučajno generisan. Ako promena konfiguracije ne uspe, pokušava se još dva puta, ali sa slučajno generisanim spoljašnjim portom između brojeva 1024 i 10000.

Ovim je proces kompletiran, omogućavajući da back-connect bude prosleđen sa spoljašnje mreže na unutrašnju mrežu. Ovako Downadup uspešno može da inficira računare iza kućnih gateway uređaja.



Pažljivi čitaoci mogu da primete da dok ova procedura dozvoljava Downadup-u da inficira ostale mašine kada se nalazi iza gateway uređaja, mašine iza sopstvenih

gateway uređaja su i dalje zaštićene (ako zaustavljaju RPC i ostali mrežni saobraćaj). Na žalost, Downadup se može širiti privatnim mrežama drugim načinima, a jednom u mreži njegove raznovrsne tehnike omogućavaju mu da inficira celu lokalnu mrežu.

Napredni korisnici mogu proveriti njihove uređaje da utvrde da li je moguće da se onemogući UPnP da se spreče neželjene modifikacije u sigurnosti njihovih gateway uređaja.

Locking itself out

Originally published February 18, 2009 by Eric Chien

<https://forums2.symantec.com/t5/Malicious-Code/Downadup-Locking-Itself-Out/ba-p/389837>

Jedan od potencijalno opasnih metoda širenja Downadup je preko mrežnih diskova, što predstavlja opasnost, posebno u preduzećima.

Downadup pokušava da se kopira na ostale mašine korišćenjem administrativnog mrežnog deljenja (ADMIN\$) koji podrazumevano postoji na Microsoft Windows mašinama. Ipak, kopiranje

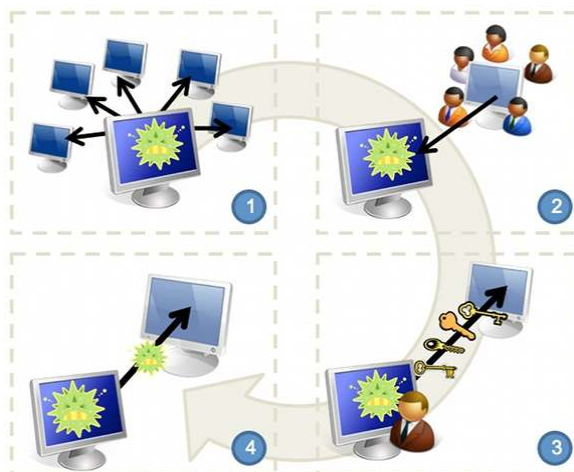
na deljeni disk, zahteva autentifikaciju. Ovaj uslov vodi do određenih primetnih neželjenih efekata.

Downadup prvo prebrojava sve servere u mreži korišćenjem NetServerEnum zahteva, koji vraća sve vidljive Windows mašine na mreži. Downadup zatim pokušava da zarazi svaku od ovih mašina.

Da bi se autentifikovao, prvo se pokušava sa podacima od lokalnog korisnika. Ako pak to ne radi, Downadup pokušava sa različitim user name i password parovima.

Od udaljene mašine se traže svi dostupni nalozi (user name). Srećom, većina Windows XP i novijih sistema ne šalje ove informacije, a i kada pošalje radi se o lokalnim korisnicima.

Obogaćen sa imenima naloga, Downadup pokušava da se konektuje do mašina sa svakim nalogom i mnoštvom šifri, uključujući tu:



1. All machines are found on the network
2. Usernames are obtained from each machine
3. Different passwords are guessed for each user
4. Once authenticated, Downadup is copied to the remote machine

- user name
- dvostruko nastavljenim user name-om (na pr. perapericperaperic)
- naopakim user name-om (na pr. cireparep)

Upotrebiće preko 250 uobičajenih šifri kao što su "password", "123" i "admin".

Mada je ovo pametan način, neželjeni efekat pogađanja šifri je povećan broj korisnika koji se žali na zaključane naloge zbog pravila zaključavanja nakon određenog broja neuspešnih autentifikacija. Ovaj efekat može postati još problematičniji jer Downadup ne označava sve postojeće naloge; zbog toga je moguće da svi nalozi budu zaključani u preduzeću,

čak i ako je zaražen samo jedan računar.

Ako Downadup ispravno pogodi šifru pre zaključavanja naloga, kopiraće se u System32 folder na udaljenoj mašini preko ADMIN\$ share-a sa slučajnim nazivom fajla i slučajnom ekstenzijom. (Kasnije, kada se pokrene, ukloniće se i kopiraće se sa slučajnim nazivom i ekstenzijom "DLL".) Zatim se menja vreme fajla na isto kao i od kernel32.dll da bi se sprečila sumnja.

Jednom kada se fajl nađe na računaru, potrebno je i da se pokrene. Kreira se zakazani posao (scheduled job) koji će pokrenuti fajl u sledećem satu, prema lokalnom vremenu na mašini. Tako, ako je vreme inficiranja bilo 14:36, mašina će kroz zakazan posao pokrenuti fajl u 15:00. Pokretanje fajla se vrši kroz rundll32.exe jer je kopirani fajl sa DLL nastavkom.

Nakon što se svi računari, nalozi i šifre provere, Downadup će čekati 40 minuta i zatim pokušati ponovo. Ovo može izazvati ponovno zaključavanje naloga, rezultujući u još većem broju žalbi korisnika.

A new Downadup variant?

Originally published February 23, 2009 by Patrick Fitzgerald

<https://forums2.symantec.com/t5/Malicious-Code/A-New-Downadup-Variant/ba-p/391186>

Tokom nekoliko zadnjih dana pojavili su se mnogi izveštaji o mogućoj novoj varijanti Downadup (ili Conficker), koja je nazvana Downadup.B++ ili Conficker.C. Dok neko može da kategorizuje Downadup u tri varijante (ili čak više), Symantec proizvodi će detektovati sve poznate varijante kao W32.Downadup ili W32.Downadup.B.

Na žalost, pored razlike u imenu, postoje i razlike u definicijama između proizvođača antivirusa. Neki proizvođači svaki različit binarni kod—sa drugim MD5 hash—vide kao drugu verziju, što rezultuje sa više od 30 različitih Downadup "varijanti". Neki drugi proizvođači ne prave nikakvu razliku i imaju jedno ime za sve razlike u verzijama.

Ipak, ono što je važno nije da li je ovo još jedna varijanta, već da li je ovo nova varijanta; tj. da li se pojavila nedavno. Srećom, Downadup.B++ / Conficker.C nije nova varijanta. Ova verzija postoji već neko vreme od pojavljivanja Downadup i skoro svi proizvođači je detektuju.

Glavni razlog koji je doveo do toga da deo industrije nazove ovaj uzorak novom varijantom je pojava peer-to-peer ponašanja. Ovo ponašanje je već analizirano detaljnije od strane Eric Chien u članku: Peer-to-Peer Payload Distribution. Symantec korisnici su zaštićeni od ove verzije Downadup.B++ / Conficker.C već neko vreme, ukoliko su im virus definicije ažurne.

Advanced crypto protection

Originally published February 23, 2009 by Elia Florio

<https://forums2.symantec.com/t5/Malicious-Code/Downadup-Advanced-Crypto-Protection/ba-p/391311>

Ovaj članak detaljno opisuje kriptografiju koji Downadup koristi za kriptovanje dodatnog sadržaja (payload) koji donosi i razmenjuje kao i digitalni potpis koji koristi.

Propagation by AutoPlay

Written by Ben Nahorney and John Park

(nije do sada objavljen)

Kao i mnoge druge pretnje pre njega, W32.Downadup.B koristi prednosti AutoPlay mogućnosti koja postoji kod Windows operativnih sistema (OS). Ipak, crv ispoljava nekoliko varijacija tradicionalnih AutoPlay trikova tako često viđenih kod ostalih pretnji.



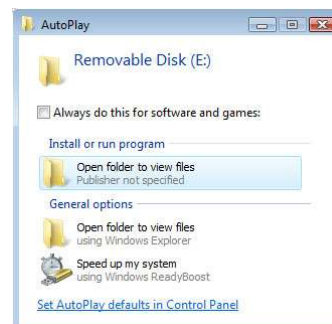
Prvi iz ove grupe trikova spada u domen socijalnog inženjeringa. Recimo da vi imate USB disk inficiran sa W32.Downadup.B i priključite ga na USB port računara sa Windows XP-om. Kada se AutoPlay pokrene (pod pretpostavkom da nije već onemogućen) možete videti dijalog nalik ovom na slici.

Brz pogled na dijalog daje utisak da će prvi izbor biti otvaranje foldera na disku kako bi videli fajlove. Pogled izbliza pokazuje tri stvari koje odskaču. Za početak, prva rečenica kaže šta želite da uradite sa *fajlom* koji ćete otvoriti. Drugo, tip fajla je *program*, što se vidi po ikonici ispod prve rečenice. Konačno, prva opcija koja se nudi je "open the folder to view files using the *program provided on the device*". Windows ne nudi da ga otvorite sa ugrađenim alatima—pita vas da li želite da

pokrenete program sa USB uređaja.

Možda početnik ili srednje iskusni korisnik neće razumeti šta ga to Windows pita u ovom slučaju, čak i ako čitaju detaljno šta piše. Da odamo čast Microsoft-u, ovim problemom su se pozabavili u Windows Vista i budućim verzijama operativnog. Ako isti USB priključite na računar sa Vistom, videće AutoPlay dijalog kao na slici desno.

Opcija za pokretanje malicioznog programa se sada nalazi ispod **Install or run program**, odvojena od standardnih Windows mogućnosti koji su pod **General options**. Još jedan trag je opcija "Always do this for *software and games*".



Ovde je problem to što mnogo ljudi ne čita na šta AutoPlay pažljivo upozorava. Downadup autori znaju za to i pokušavaju to da iskoriste, tako što su napravili svoj autorun.inf fajl na taj način da izgleda kao da birate opciju da otvorite folder. Naravno, radi se o prevari, pažljivo predstavljenoj da bi pokrenuli maliciozni kod sa USB uređaja.

Da bi demonstrirali kako je ovo urađeno, pogledajmo tekst koji se nalazi u autorun.inf fajlu koji koristi crv:

```
[autorun]
Action=Open folder to view files
Icon=%systemroot%\system32\shell32.dll,4
Shellexecute=RUNDLL32.EXE .\RECYCLER\[RANDOM NUMBERS]\[5-8 RANDOM LETTERS].[RANDOM EXTENSION]
UseAutoPlay=1
```

Dve linije koje su odgovorne za ovaj trik socijalnog inženjeringa su `Action=` i `Icon=` linije. Prva prikazuje tekst “Open folder to view files”— isti koji koristi Windows da otvori folder u Windows Explorer-u.

Linija sa `Icon=` pomaže dodatno prikazujući 5. Ikonu iz shell32.dll fajla—ikonu Windows foldera. U kombinaciji ove dve linije u autorun.inf fajlu daju utisak da birate opciju koja otvara folder.

Linija sa `Shellexecute=` je ona koja pokreće maliciozni udarac. Kada se W32.Downadup.B iskopira na prenosni disk, snima maliciozni DLL u skriveni folder `%DriveLetter%\RECYCLER—Recycle Bin` za disk koji je u pitanju.

Brzim pogledom na USB disk možda nećete uočiti njegovo prisustvo, budući da je folder skriven. Čak i ako pažljivo pogledate disk, primetićete još jedan skriveni folder u Recycle Bin-u sa imenom tipa “S-n-n-nn-nnnnnnnnnn-nnnnnnnnnn-nnnnnnnnnn-nnnn”, gde je svako "n" slučajna cifra. Ovo ima za cilj da imitira foldere koje koristi Security Identifiers (SIDs)—jedinstven broj dodeljen od strane OS-a da identifikuje korisnika ili grupu u okviru mreže Windows računara. Folderi bazirani na SID-ovi nisu neuobičajen prizor kada se pogleda skriveni sadržaj `%DriveLetter%\RECYCLER` foldera. Imitiranjem ovih foldera, pretnja izgleda kao da joj je tu mesto.

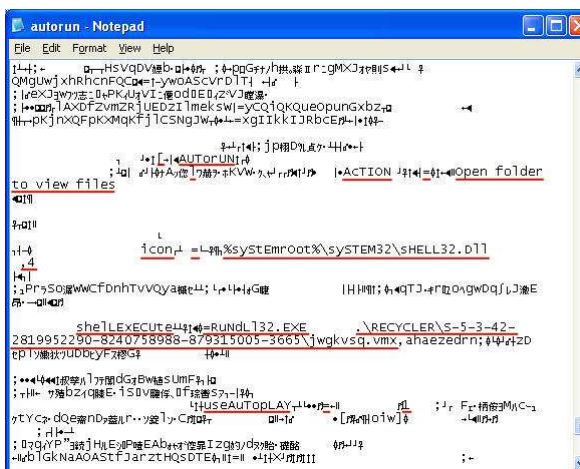
Kao konačnu zaštitu od otkrivanja, aktuelni W32.Downadup.B fajl koji je iskopiran u ovaj folder ima ime koje je slučajno, sa slučajnom ekstenzijom. Na kraju, bez tragova u autorun.inf fajlu, maliciozni .dll fajl izgleda samo kao đubre u okviru SID foldera u Recycle Bin-u diska.

Dolazimo do mesta gde stvari postaju ozbiljne: kada se izvrši linija `Shellexecute=`, poziva se `rundll32.exe`— proces koji je zadužen za pokretanje i izvršavanje DLL-ova i učitavanje njihovih biblioteka u sistemsku memoriju. U ovom slučaju to su biblioteke malicioznog W32.Downadup.B i računar postaje inficiran crvom.

Zadnja linija `UseAutoPlay=1` pokušava da pokrene kod bez obaveštavanja korisnika sa AutoPlay dialogom. Osim ako ova mogućnost nije onemogućena, rezultat će biti automatsko izvršavanje DLL na Windows XP SP2 ili starijim operativnim sistemima.

Ove funkcionalnosti su ukratko o tome kako AutoPlay radi, ali W32.Downadup.B ima još trikova u rukavu—dodaje đubre u autorun.inf fajl i to ne malo đubreta, već većinu onoga što čini ovaj fajl.

Ipak AutoPlay uspeva da izvrši instrukcije u fajlu. Ovo je zato što kada Windows prepozna autorun.inf fajl, prati tačno određene instrukcije koje očekuje da nađe. Prvo traži očekivani `[autorun]` heder, zatim tekst koji spada u ograničen skup komandi koje su ispravne samo autorun.inf fajlu. Bilo koji znaci osim onih koji se očekuju u AutoPlay komandama se ignorišu u potpunosti. Ne samo to, već same komande mogu biti isprekidane sa nizom znakova koje će Windows ignorisati, a koji su ubačeni u sredinu ispravnog AutoPlay stringa, kao što je prikazano na slici.



Cilj ovoga je da fajl autorun.inf izgleda nekome ko ga otvori da ga pregleda kao nefunkcionalno đubre. (Prave AutoPlay instrukcije su smeštene na dno fajla.) Ovo nije ništa drugo nego još jedan

trik socijalnog inženjeringa koji treba da prevari iskusnije korisnike koji su možda svesni potencijalne opasnosti koju nosi neočekivani autorun.inf fajl na mrežnim deljenim diskovima ili prenosnim diskovima.

Gledano van konteksta prenosnih diskova, ovi trikovi se mogu upotrebiti jednako uspešno i na mrežne diskove. AutoPlay funkcioniše na isti način i u ovom slučaju te pristup mrežnom disku nosi jednako opasnosti ako je AutoPlay omogućen.

Još jedan trik koji koristi W32.Downadup.B je način na koji traži prenosne i mapirane diskove. Kada se ovakva pretnja pokrene, proverava sve diskove da bi utvrdila koji su prenosni, a koji mrežni mapirani i zatim ih inficira. W32.Downadup.B radi isto to, ali takođe i registruje Windows objekat koji prati WM_DEVICECHANGE poruke. Kada se ova poruka pojavi, to obično znači da je napravljena nova konekcija ili ka prenosnom ili ka mapiranom disku, te onda pretnja ponovo pokreće pretraživanje pokušavajući da inficira novi uređaj. Ukratko, ova pretnja može da inficira nove diskove u realnom vremenu, u sekundi čim ih priključite.

Sve u svemu, W32.Downadup.B ima par trikova kako bi se lakše širio korišćenjem AutoPlay-a. Kao i uvek, preporučujemo da isključite/onemogućite AutoPlay na vašim računarima i vašoj mreži kako bi izbegli potencijalnu infekciju sa W32.Downadup.B ili drugim pretnjama koje se šire korišćenjem ovih tehnika.

W32.Downadup.C Digs in Deeper

Originally published March 6, 2009 by Peter Coogan

<https://forums2.symantec.com/t5/Malicious-Code/W32-Downadup-C-Digs-in-Deeper/ba-p/393245>

Symantec-ovo stalno praćenje Downadup (ili. Conficker) crva je danas rezultovalo u detekciji kompletno nove verzije koja se širi na sisteme koji su već inficirani sa Downadup. Symantec je ovu verziju nazvao W32.Downadup.C.

Analiza novog uzorka još traje i u ranoj je fazi, ali inicijalni rezultati pokazuju neke interesantne stvari. Izgleda da nova verzija ne koristi niti stare niti nove načine za širenje na nove mašine. Cilj su joj antivirus softver i alati za analizu sigurnosti sa ciljem da ih onemogući. Svaki proces na inficiranoj mašini koji se pronade, a sadrži neki od naziva u donjoj listi biće uklonjen:

wireshark	unlocker
tcpview	sysclean
scct_	regmon
procmon	procexp
ms08-06	,rtstub
mrt.	mbsa.
klwk	kido
kb958	kb890
hotfix	gmer
filemon	downad
confick	avenger
autoruns	

Takođe, kao odgovor na uspešno praćenje i "razbijanje" algoritma za generisanje domena od strane proizvođača sigurnosnog softvera u verziji W32.Downadup.B, autori Downadup-a su sada prešli sa 250 domena na dan na algoritam koji generiše novih 50.000 domena na dan. Novi algoritam za generisanje domena takođe koristi jedan od mogućih 116 sufiksa za nazive domena.

Ova prva otkrića govore da autori Downadup-a sada pokušavaju da povećaju životni vek postojećih Downadup pretnji na inficiranim mašinama. Umesto da nastave sa pokušajima daljeg širenja, izgleda da žele da zaštite trenutno inficirane mašine sa Downadup-om od antivirus softvera i alata za uklanjanje. Takođe, trenutno se ne primećuje povećanje broja infekcija računara sa ovom pretnjom, ali je ipak držimo na oku.

W32.Downadup.C Bolsters P2P

Originally published March 20, 2008 by the Security Intel Analysis Team

(<https://forums2.symantec.com/t5/Malicious-Code/W32-Downadup-C-Bolsters-P2P/ba-p/393331>)

U ovom članku se poredje varijante Downadup crva, sa naglaskom na C verziju.

Downadup Motivations

Originally published March 23, 2009 by Eric Chien

(<https://forums2.symantec.com/t5/Malicious-Code/Downadup-Motivations/ba-p/393335>)

Kako se bliži 1. april kao datum za isporuku neženjenog dodatnog sadržaja pretnje [W32.Downadup.C](#) (takođe poznate i kao Conficker) nastavljaju se spekulacije da li će taj neželjeni sadržaj biti jedna od najvećih prvoaprilskih šala ili će biti nevolja jednaka cyber Pearl Harbor-u. Ne možemo sa sigurnošću da predvidimo budućnost, ali možemo da pogledamo motivacije prethodnih varijanti Downadup-a i da pretpostavimo kakav će to teret doneti i da će on verovatno biti između ova dve ekstrema.

Prva varijanta Downadup-a (.A) nudi najviše dokaza o motivacijama autora. Slično kao i nedavna varijanta, Downadup.A je imao datum za isporučivanje dodatnog tereta postavljen na 1. decembar 2008.g. Downadup.A je pokušavao da preuzme teret sa lokacije `hxxp://trafficconverter.biz/4vir/antispyware/loadadv.exe`. Downadup.A was nikada nije uspeo da isporuči teret jer je ovaj sajt bio zatvoren, a vlasnik sajta trafficconverter.biz bio je uveliko uključen u isporuku [misleading applications](#) – lažnih aplikacija (takođe poznatih i kao lažni – prevarantski antispyware proizvodi) na mašine korisnika. Lažne aplikacije se pretvaraju da skeniraju računar od malicioznih pretnji i pokušavaju da uplaše korisnika da poveruje kako je računar zaražen, kada u stvari nije i da za uklanjanje nepostojećih pretnji pokušavaju da ubede korisnika da plati od \$50-\$100 da kupi “softver”.

Svrha trafficconverter.biz (koji je isti kao i traffic-converter.biz, a kasnije i trafficconverter2.biz) bila je da regrutuje preprodavce da pomognu u instaliranju lažnih aplikacija. Njihovim sopstvenim rečima:

"What is Traffic Converter?"

Traffic Converter is affiliate program that helps webmasters to convert their traffic into cash.

How it works?

We are selling popular antispyware and security software products to surfers which you send to us. You receive \$30 for each sale of our products.

Why does it work so good?

With our direct-marketing approach, aggressive promotion materials and advanced software products you can earn much more than with other affiliate or advertising programs."

Prijavlivanjem na Traffic Converter, dobićete URL-ove sa kojih se mogu preuzeti i instalirati lažne aplikacije kao što je [XP AntiVirus](#). Vlasnik Traffic Converter je isporučivao ove lažne aplikacije i kroz ostale, svoje domene kao što su xpantivirus.com, antispyguard.com, antivirus2009online.com i systemscanner2009.com. Prethodno je većina ovih sajtova bila registrovana preko Estdomains i Directi, oba poznata po tome što su vršila registracije u ime i za slične sajtove. Inače, lažne aplikacije, kao što je XP AntiVirus, izgleda da su poticale od druge strane poznate kao Innovagest 2000, koja je poznata i po kreiranju mnoštva sličnih klonova kao što su AlfaCleaner i AntiMalware 2009.

Sa ovakvom istorijom, originalna motivacija Downadup-a se čini prilično jasnom—da isporuči lažne aplikacije. Ipak, tipičan metod isporuke lažnih aplikacija kroz Traffic Converter dešavao se kroz preprodavce koji su generisali saobraćaj ka Traffic Converter-u svojim metodama, kao što su drive-by downloads ili exploit-ima postavljenim na oglase kroz mreže oglašavača. Da bi preprodavcu bila priznata instalacija obično je potrebno da dodaju jedinstven ID u zahtevu za preuzimanje (download) ili instalaciju. Neki od primera ovakvih URL-ova koji su generisali saobraćaj ka Traffic Converter domenima su:

hxxp://seamastersoft.com/soft.php?aid=0135&d-1&product=XPA&refer=3e6376a25
hxxp://onlineprivatescan.com/2009/1/freescan.php?id=880135
hxxp://traffic-converter.biz/s.php?nick=8801931355&group=880193&os=Windows

U svakom od ovih primera, "aid", "id" i "nick" predstavljaju preprodavce koji su zaslužni. Ovi preprodavci su [zarađivali hiljade dolara mesečno](#).

U slučaju Downadup, ipak se pretnja direktno preuzima sa Traffic Converter domena kao hxxp://trafficconverter.biz/4vir/antispymware/loadadv.exe bez parametara preprodavca; moguće značenje je da su vlasnici Traffic Converter-a ili veoma bliski partneri ili ljudi koji se nalaze iza Downadup-a, pre nego preprodavci. Čak šta više, direktorijum "4vir" je možda skraćena od "for virus", označavajući Downadup. Suprotno tome, dodatan direktorijum "antispymware" samo ponovo potvrđuje poznatu činjenicu da je Traffic Converter uključen u download lažnih aplikacija. Pored toga, naziv fajla je isti kao i prethodno korišćen naziv za IFrameBiz i/ili IFrameCash koji je nudio sličan servis plati-po-instalaciji. Da li postoji veza sa ovom prethodnom grupom ili je naziv fajla samo koincidencija nije potpuno jasno. Nedugo pošto je trafficconverter.biz nestao, vlasnici su se vratili sa novim sajtom, trafficconverter2.biz. Ipak, nakon svega nekoliko dana rada, ponovo su nestali; ovoga puta su tvrdili da ih je blokirao procesor plaćanja karticama i da oni nemaju nikakve veze sa Downadup-om.

I dok uživamo u čitanju scenarija korišćenja Downadup-a za kreiranje "[Mračnog Google-a](#)" koji će pretraživati podatke na svim inficiranim računarima, ako se autori Downadup-a drže svojih originalnih namera, verovatniji scenario je da će autori pokušati da nadoknade ono što su investirali u instaliranje lažnih aplikacija ili drugim plati-po-instalaciji programima kao što su razni tipovi adware-a. Ipak, imajući u vidu značajan broj očiju koje budno prate svaki potez Downadup-a, ne smemo da podcenimo šansu da se autori predomisle i odustanu od početnih motiva.

Zaključak

Do danas, Downadup je jedan od najsloženijih crva u istoriji malicioznog koda. Sa tako mnogo lica, interesantan je za analizu. Proučavanje njegovih tehnika propagacije (širenja), neobičnih načina zaštite i sigurnih sistema za ažuriranje su izazovi za svakoga u security profesiji. Iako se ovi faktori u kombinaciji mogu smatrati zaslužnim za široko rasprostranjen uspeh, istina je da je razlog uspeha prozaičan—popustljivost.

Kao što je pomenuto, u ovoj pretnji nema ničega što do sada nije već viđeno u jednog ili drugog formi. Dok neki od trikova uzimaju novi oblik stare teme, malo je stvari koje bi Downadup mogao da uradi u dobro obezbeđenoj mreži.

Korišćenje MS08-067 ranjivosti je daleko najviše korišćeno za tehniku propagacije crva kroz mrežu. Ipak, pojava W32.Downadup je došla skoro mesec dana od objavljivanja patch-a. U većini IT okruženja ovo je više nego dovoljno vremena da se testira i instalira patch, posebno ovakav koji je označen kao "kritičan" u Microsoft Security Bulletin.

Nisu ni RPC ranjivosti nešto novo. Neki po poznatih crva, kao što je W32.Blaster iz 2004.g., koristili su propuste u ovom servisu da izazovu masovnu infekciju—mnogo veću nego što je to uspeo Downadup. Vidimo da i stare, postojeće pretnje kao što je porodica Spybot crva, nastavljaju da iskorišćavaju stare, na izgled zastarele RPC ranjivosti.

Pravilno administriranje mrežnih i prenosnih diskova je podjednako važno. Nalik slatkišima, tvrdim spolja, a sa mekom unutrašnošću, Downadup je često koristio MS08-067 da uđe u mrežu, a jednom kada je bio unutra, uspešno se širio korišćenjem drugih tehnika. Sve što je bilo potrebno jeste jedan ranjivi računar kako bi se probila tvrda spoljašnjost i došlo do slatke i meke unutrašnjosti intraneta.

Ključni element za zaštitu vaših računara i mreža od ovakvih pretnji je proaktivno primenjivanje patch-eva. Isključivanje AutoPlay mogućnosti i sprovođenje politike složenih šifri za mrežne diskove su dodatna dva, tri udarca koja bi oborili ovakve pretnje kao što je Downadup. Dodatno, kao prevenciju, blokirajte na mrežnim obodima portove koje ova pretnja koristi—u ovom slučaju to su portovi 139 i 445. Kao što je slučaj sa svim današnjim pretnjama, dobro upravljana mreža je sigurna mreža.