25.000 inficiranih Linux servera

Kako se čini, jedan od uspješnijih cyber napada na Linux servere u tijeku je, potiho, već dvije godine. Prema izvješću [1] tvrtke Eset, grupa malicioznih osoba potiho već dvije godine inficira servere diljem svijeta, pretvarajući ih u strojeve za plasiranje spam poruka/reklama i preusmjeravanje korisnika na maliciozni sadržaj.

Tehnički, riječ je o grupi alata koji svaki ima svoju zasebnu funkciju:

- Linux/Ebury je malware koji omogućuje backdoor shell i krade ssh akreditacije;
- Linux/Cdorked omogućuje backdoor shell i preusmjerava Windows korisnike na "drive-by" malware (zadnje dvije stavke u ovom popisu);
- Linux/Onimiki presreće DNS zahtjeve;
- Perl/Calfbot je spam bot koji radi na svim platformama koje imaju instaliran perl;
- Win32/Boaxxe.G je click fraud malware za Windows;
- Win32/Glubteta.M je generički proxy za inficirana računala

Promatrana kao cjelina, ta grupa alata zarazit će Linux server, nakon čega stroj može biti iskorišten kao:

- točka napada na druge servere;
- spam bot;
- ako na serveru postoji Web servis, on će biti kompromitiran tako da posjetiteljima nudi "drive-by" malware.

Kako nije riječ o nužno Linux-specifičnom kodu, moguće je zaraziti servere pod FreeBSD-om (SSH backdoor), ali i OS X-om, pa čak i Windows strojeve koji na sebi imaju instaliran Cygwin, te naravno sve strojeve koji imaju instaliran perl.

U opasnosti su i klijenti pod Windows OS-om, jer zaraženi web servisi upućuju posjetitelje na za Windows specifične zloćudne datoteke.

Možda najzanimljivija priča jest ona o najslabijoj sigurnosnoj karici, onoj koja omogućuje širenje ove digitalne pošasti: neadekvatno rukovanje administratorskim lozinkama. Naime, u ovom slučaju napadači ne koriste niti zero-day sigurnosne propuste niti stare, nepatchirane servere – napadi se fokusiraju na slabe lozinke koje je lako pogoditi brute force metodom i odgovarajućim rječnicima, što se ovim primjerom (25.000 inficiranih servera) pokazalo sporom, ali lukrativnom strategijom.

U osnovi ovog napada jest, dakle – ljudska glupost: napadač bi jednostavno pokušao pogoditi administratorovu lozinku. Jednom provaljen, server zatim postaje dijelom maliciozne mreže i čini nekoliko opasnih stvari: krađom ssh akreditacija pokušava se proširiti na druga dostupna računala, ali isto tako i krade ssh lozinke korisnika zaraženog servera, te pokušava "uvaliti" malware slučajnim

web prolaznicima.

Autori teksta daju i jednostavne testove kojima je moguće provjeriti je li server zaražen nekim od zloćudnih programa:

Linux/Ebury će promjeniti ssh datoteku tako da neće vraćati ispravnu poruku o grešci: ako na zadanu naredbu "ssh -G" ne dobijete nazad poruku o grešci ("illegal option" ili "unknown option") već samo uputu o upotrebi, riječ je o zaraženoj datoteci:

```
$ ssh -G 2>&1 | grep -e illegal -e unknown > /dev/null && echo “System clean” || echo
 “System infected”
```

Linux/Cdorked će preusmjeriti sve zahtjeve za favicon.iso (ne .ico) na google.com, pa ako vas ovakav zahtjev:

```
$ curl -i http://myserver/favicon.iso | grep “Location:”
```

odvede ravno na http://google.com/ - inficirani ste.

Linux/Onimiki je malo zapetljanije tražiti, pa autori predlažu korištenje Yara [2] pravila za ispitivanje je li named datoteka inficirana.

Perl/Calfbot možete otkriti ako potražite /tmp/... lock datoteku:

```
$ flock --nb /tmp/... echo “System clean” || echo “System infected”
```

Za više detalja i kompleksnije tehnike potrage pročitajte izvorni dokument.

Za uklanjanje zlonamjernog koda autori preporučuju drastične korake: serveri na kojima je potvrđena infekcija trebali bi biti potpuno "pregaženi" i na njih bi trebalo iznova instalirati servise.

Što se, pak, prevencije tiče, autori preporučuju ove korake:

- onemogućiti root login: "PermitRootLogin no" u /etc/ssh/sshd_config (ovo zbilja spada u osnove osnova zaštite sustava);
- onemogućiti prijavu lozinkama i forsirati prijavu ssh ključevima;
- koristiti SSH Agent Forwarding umjesto kopiranja ssh ključa sa servera na server;
- koristiti dvofaktornu autentikaciju.

Naravno, kako su autori dokumenta djelatnici tvrtke koja se bavi antivirusima, toplo su preporučili i korištenje odgovarajućeg antivirusa. :-)

sri, 2014-03-19 20:04 - Radoslav Dejanović**Vijesti:** Linux [3]
Kategorije: Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1369?page=0

Links
[1] http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf
[2] http://plusvic.github.io/yara/
[3] https://sysportal.carnet.hr./taxonomy/term/11
[4] https://sysportal.carnet.hr./taxonomy/term/30