Prijetnja zvana Gumblar

Sigurnosne prijetnje koje svojim djelovanjem sistem administratore dovodi u očaj pojavljuju se redovito. Počevši od crva Blaster, Sasser, MyDoom pa sve do najnovijih kao što je Conficker, maliciozni programi najčešće iskorištavaju sigurnosne propuste u operativnim sustavima i programima instaliranim na računala. Međutim, sigurnosni problem u obliku trojanskog konja zvanog Gumblar.cn ili JSRedir uz sigurnosne propuste iskorištava i nemar ili neznanje korisnika. Poznato je da korisnici snimaju lozinke unutar raznih programa. Primjerice, loznika za e-mail korisnički račun je redovito snimljena ili u internet pregledniku ili u e-mail klijentu. Također, lozinke za FTP pristup poslužiteljima spadaju u "tko će svaki put upisivat lozinku" domenu. Ovu potonju sigurnosnu rupu iskorištava Gumblar.

Na poslužitelju po mojim nadzorom problem se počeo manifestirati tako što se na web stranicama nije izvršavala jedna od java skripti. U apache logovima nije bilo ništa neobično, a skripta je uredno postojala u kodu. Detaljniji pregled koda web stranice otkrio je novu skriptu koja je bila na samom dnu stranice, a čiji sadržaj na prvi pogled nije imao smisla. Skripta je izgledala otprilike ovako:

```
/*LGPL*/ try{ window.onload=function(){var M0ls6baqhmn=document.createElement
('s$((c^r)$i!&p^$&t^)'.replace(/\^|#|\)|\!|\$|\(
...
...
...
@^$e#&!/$'.replace(/\)|\(|@|#|\^|&|\$|\!/ig, "));
if (document){document.body.appendChild(Nda8b3m7i8vat);}} }
catch(Bvlu3ghp1mre1o76k9fnb) {}
```

Prvo sam zaključio sam da ovi "hijeroglifi" predstavljaju prilično komplicirane regularne izraze. Daljnjim istraživanjem izraza došao sam do uzroka problema - trojanskog konja iz naslova. Sam način rada ovog trojanskog konja je vrlo zanimljiv. Kad posjetitelj pristupi zaraženoj web stranici, trojan iskoristi jedan od sigurnosnih propusta unutar Acrobat Readera ili Flash playera da se instalira na računalo. Sigurnosni propusti su vezani uz izvršavanje java skripti. Jednom kad se trojan instalira na računalo, pretražuje FTP klijente na računalu (kao što su Filezilla, Total Commander ili Macromedia/AdobeDreamweaver) i podatke za spajanje na web sjedišta koji su snimljeni na računalo. U slučaju da je uz korisničko ime snimljena i pripadajuća lozinka, ti se podaci kradu i onda koriste za FTP pristup dotičnom webu i injektiranje gornje skripte u web stranice. Problem je što se za FTP pristup koriste krivotvorene IP adrese, što daje dojam da se spajanje obavlja s različitih dijelova svijeta. U mom slučaju, jedan od korisnika koji održava web stranice imao je snimljene podatke za spajanje FTP-om u klijentu na svom računalu. Spajanja na poslužitelj je bilo nekoliko u minuti, uvijek s različite IP adrese i svako je trajalo samo par sekundi. Dovoljno da se s poslužitelja skine jedna datoteka, promijeni i vrati na poslužitelj. Sama skripta preusmjerava http promet na nekoliko domena od kojih je prva otkrivena gumblar.cn, po kojoj je trojan i dobio ime. Preusmjeravanje prometa na predodređena web sjedišta dovodi do direktne materijalne koristi vlasnicima istih zbog povećanja broja posjećenosti tih sjedišta. Analizom sam utvrdio da je promijenjeno preko 2000 datoteka, većinom s ekstenzijom .js. Također, zaražene su bile sve html i php datoteke koje imaju index ili default u svom imenu. A razlog za veliki broj zaraženih datoteka jest CMS sustav instaliran na poslužitelju - korišteni CMS ima puno navedenih datoteka po direktorijima.

Prva stvar koju sam napravio jest blokiranje korisničkog računa naredbom

```
# usermod -L korisni?ko_ime
```

Isti efekt postigao bi se i promjenom lozinke. Nakon onemogućavanja pristupa dotičnom korisničkom računu, sljedećih 10-ak sati su se nastavili pokušaji pristupa FTP-om. Brza obrana od ove vrste

napada jest promjena priključne točke (porta) na kojoj FTP poslužitelj "sluša".

Slijedio je popravak štete. Ručno uklanjanje spomenute skripte iz svih zaraženih datoteka bi predugo trajalo pa sam našao rješenje u obliku php skripte koja se pretraži sve datoteke i ukloni malicioznu skriptu. Navedenu skriptu možete pronaći na ovim stranicama [1]. Skripta se jednostavno stavi u root direktorij web sjedišta i pozove se iz web preglednika. Međutim, kako je vrlo vjerojatno da skripta tj. korisnik pod kojim se "vrti" web server nema prava pisanja po svim datotekama, moguće je i ručno pokrenuti skriptu iz ljuske naredbom:

```
# php ime_skripte.php
```

Zbog ogromnog broja zaraženih web sjedišta (neke procjene govore o više od 12000 zaraženih web sjedišta), sigurnosne tvrtke nagađaju da je ovaj trojanski konj veća sigurnosna prijetnja i od ozloglašenog crva Conficker. Iz svih ovih razloga još je jednom potrebno naglasiti da se redovito instaliraju zakrpe operativnih sustava i programa koji se koriste, a možda najveći utjecaj može imati edukacija korisnika.

uto, 2010-01-19 09:40 - Mirko Lovričević**Kategorije:** Sigurnost [2]
Vote: 4

Vaša ocjena: Nema Average: 4 (2 votes)

Source URL: https://sysportal.carnet.hr./node/700

Links
[1] http://justcoded.com/article/gumblar-family-virus-removal-tool/
[2] https://sysportal.carnet.hr./taxonomy/term/30