Mumblehard – Perl babuška koja napada Linux i BSD poslužitelje

Kvalitetan malware prepoznat ćemo i po tome što dugo vremena ostaje neotkriven. Mumblehard je jedan od takvih primjera jer je u pogonu od 2009. godine. Ovaj malware otkriven je tek nedavno, gotovo slučajno, a jedan od razloga njegove dugovječnosti je neobičan način skrivanja izvršivih datoteka i činjenica da svoju potvrđenu (i jedinu?) aktivnost – slanje spam poruka – obavlja na diskretan način, zbog čega nema vršnog opterećenja zaraženog poslužitelja, niti ga blokiraju blacklisting servisi.

Priča o otkriću i analizi Mumbleharda čita se poput zabavnog i fantastičnog krimića, sa dijelovima koji su genijalni i dijelovima u koje je teško povjerovati. Uistinu, Mumblehard je mješavina sofisticiranih i posve primitivnih (time, vjerojatno, efikasnih) metoda koje rezultiraju perzistentnom zarazom koja je neprimjećena trajala šest godina.

Ovaj malware otkiven je gotovo slučajno, kad su istraživači iz ESET-a analizirali potencijalni malware na jednom od poslužitelja koji je završio na crnoj listi zbog širenja spam poruka. Ispostavilo se da na sustavu postoje procesi koji su u suštini neočekivani Perl interpreteri. Daljnje istraživanje otkrilo je izvršive datoteke u /tmp direktoriju.

Analiza datoteka otkrila je sofisticirani način infekcije: datoteke u sebi sadrže pakirani Perl kod, koji pak u sebi može sadržavati pakirani binary (koji u sebi onda ima još malo zapakiranog Perl koda).

Analiza je otkrila i kako je malware u stanju zaraziti Linux i BSD poslužitelje, unatoč činjenici da te dvije platforme baš i nisu identične: kod je kratak, nekompliciran i napisan u asembleru, te koristi jednostavan trik – aktiviranjem sistemskog poziva koji vraća različite rezultate ovisno o verziji operacijskog sustava malware prepoznaje na kojoj se arhitekturi izvršava i sukladno tome prilagođava svoje ponašanje.

Jednom zaražen, poslužitelj će se povremeno aktivirati i pokušati uspostaviti vezu sa C&C adresama koje su statički definirane kao deset nepromjenjivih IP adresa ili domena, što se pokazalo kobnom pogreškom: istraživači su uspjeli preuzeti kontrolu nad jednom od domena kojoj je istekla registracija. Preuzevši domenu, istraživači su došli u priliku na poslužitelj pod svojom kontrolom dobivati komunikaciju zaraženih računala.

Nadzorom komunikacije koji je trajao duže od pola godine, bili su u stanju identificirati više od 8.000 zaraženih poslužitelja širom svijeta.

No, kako se infekcija širi? Pretpostavlja se da postoje dva vektora širenja: jedan je iskorištavanje poznatih propusta u Joomla i WordPress aplikacijama ("booooring", rekao bi svaki iskusan sistemaš), ali je drugi posve Montypythonovski i upravo brutalno glup: istraživači su otkrili da adrese C&C poslužitelja vode do ukrajinske tvrtke Yellsoft koja prodaje – pazite sad – softver za masovno spamiranje elektroničke pošte.

Igrom slučaja softver te tvrtke pisan je (i) za Linux, pisan je u Perlu i prodaje se za 240$ po licenci.

U načelu ne bismo mogli puno prigovoriti tvrtci koja se bavi poslom koji je na rubu legalnog i koja sasvim sigurno ima svoju klijentelu, ljude koji vide profit u nečemu što drugi vide kao naporno dosađivanje. Sve bi to bilo više ili manje etično poslovanje da nije – pazite sad – linka na stranici tvrtke koji vodi na – zvuk fanfara – piratiziranu verziju njihovog softvera!

Nije riječ o provali na sustav, tvrtka sama od sebe nudi link na piratiziranu verziju softvera kojeg inače prodaje za 240$, tek uz napomenu kako u tom slučaju korisnici ne mogu od njih dobiti podršku.

Piratska verzija je, naravno, zaražena Mumblehard malwareom.

Što bi, Linusa mu, navelo neku tvrtku na piratiziranje vlastitog softvera? Odgovora ima mnogo, ali naivne možemo odmah odbaciti; najvjerojatniji odgovor je da tvrtka ima prste u izradi malware aplikacije, ili barem zarađuje u drugoj ruci. Računajući na gramzivost svojih klijenata (koji po naravi stvari ne mogu biti pretjerano moralne osobe, stoga instant karma), tvrtka ostvaruje posrednu ili neposrednu zaradu od apsolutno svih korisnika njenog softvera.

Je li i vaš poslužitelj zaražen Mumblehardom možete provjeriti na jednostavan način: kako malware svakih petnaestak minuta kontaktira C&C poslužitelje, provjerite postoji li kakav neočekivan cron job koji se izvršava u tom intervalu i pritom poziva skripte koje se nalaze u /tmp ili /var/tmp direktoriju.

Također, primjećeno je da od deset C&C poslužitelja, samo jedan uistinu šalje naredbe zaraženim poslužiteljima, i to samo povremeno; poslužitelj na adresi 194.54.81.163 "otvara se" tek kad ima nove zadatke za zaražena računala, nakon čega se portovi zatvaraju i poslužitelj ide u period hibernacije, u kojem ne odgovara na podražaje s Interneta. No, to nam omogućuje da na jednostavan i bezbolan način onemogućimo funkcioniranje malwarea: jednostavna zabrana pristupa toj IP adresi na firewallu onemogućit će malware čak i u slučaju da je poslužitelj već zaražen.

Najzad, malware je moguće onesposobiti i korištenjem "noexec" opcije na /tmp u fstab-u, što je i inače dobra praksa – pa ako do sad niste, a u mogućnosti ste...

Što možemo zaključiti o ovom komadu zločestog softvera? S jedne strane je nestandardno dobro rješenje koje pokazuje da autori znaju svoj posao (korištenje asemblera, ugnježđavanje Perl skripti), s druge je strane neobjašnjivo šlampavo (klijenti vraćaju rezultat izvršavanja svim C&C poslužiteljima indiskriminatorno, umjesto da ga vraćaju samo onom poslužitelju koji je naredbu i poslao), a s treće strane koriste krajnje naivan ali očito efektan socijalni inženjering, što bi bilo na rubu apsurda da nije činjenice da tvrtka sama daje link na zaraženu, piratiziranu verziju vlastitog softvera - što obilno prelazi rub apsurda, pa i zdravog razuma. I sve to uspjevaju činiti neopazice već šest godina!

Za više detalja pročitajte izvorni dokument ovdje (http://www.welivesecurity.com/wp-content/uploads/2015/04/mumblehard.pdf [1]).

sri, 2015-05-06 13:40 - Radoslav Dejanović**Vijesti:** Sigurnost [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1547

Links
[1] http://www.welivesecurity.com/wp-content/uploads/2015/04/mumblehard.pdf
[2] https://sysportal.carnet.hr/taxonomy/term/13