Plače mi se i njegova djeca

WannaCry ransomware je pušten s lanca i, kao što već vjerojatno znate, privremeno je zaustavljen zahvaljujući otkriću kill switcha, no veseli autori odmah su zatim u promet pustili njegovo nasljednika koji nema taj kill switch. Unatoč sigurnosnim zakrpama koje je Microsoft već objavio, očekuje se tsunami novih zaraza i nepoznata količina štete.

Ovaj ransomware u svojoj naravi nije posebno drugačiji od drugih ucjenjivačkih e-zlodjela, ali malo posebnijim čini ga činjenica da iskorištava ranjivost u Microsoftovom OS-u koja je dio arsenala nedavno objavljenih (https://www.bloomberg.com/news/articles/2017-05-04/seriously-beware-the-shadow-brokers [1]) hacking alata NSA, a koju ranjivost je ta agencija, pretpostavlja se, koristila i za provalu unutar SWIFT (https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication [2]) sustava nekih banaka.

Ranjivost se odnosi na SMBv1 protokol u svim verzijama Windowsa od XP nadalje, a omogućuje izvršavanje neautoriziranog koda poslanog s udaljenog mjesta.

Tako se WannaCry ransomware širio na dva načina: klasičnim socijalnim inženjeringom (slanjem e-mail poruka sa zareženim privicima), te potragom za otvorenim SMB portovima na javno dostupnim adresama (i unutar lokalne mreže, čim bi se jedno od njenih računala zarazilo kroz socijalni inženjering).

Jednom zaraženo, računalo prolazi kroz klasični ciklus ucjene: podaci bivaju enkriptirani i zatražena otkupnina u obliku Bitcoina.

No, sistemašima najzanimljiviji aspekti ove epidemije su činjenica da je Microsoft već izdao zakrpe za pronađene propuste (pretpostavlja se, onako potiho, da su dobili odgovarajući mig čim je agencija otkrila krađu svojih alata), te podatak da se ozbiljan broj zaraza ne događa socijalnim inženjeringom, već pronalaženjem izloženih, a nezakrpanih računala na Internetu.

Čudno, zar ne? Posjetite Shodan i uvjerite se sami.

Postoji li neki dobar razlog zašto bi bilo koji stroj imao SMB izložen prema van? Osobno, ne mogu se sjetiti niti jednog razumnog razloga, iako vjerojatno postoji gomila nerazumnih, složenih od strane nestručnih administratora ili projektiranih od strane nestručnih projektanata. I vjerojatno više od jednog korisničkog zahtjeva, jer “njima je tako jednostavnije i navikli su, a i nisu nikome zanimljivi, a i tko će ih naći na tako ogromnoj mreži?”

To, plus činjenica da je Microsoft prije gotovo dva mjeseca(!) izdao zakrpe za navedene propuste, i to ne samo za moderne operacijske sustave već, posve neočekivano, i za Windows XP.

Očito je, mnogi ne samo da nerazumno ostavljaju javno izložene portove protokola koji nisu nikad niti bili namijenjeni takvoj upotrebi, već i nisu pretjerano ažurni sa sigurnosnim zakrpama. Donekle je razumljivo biti na oprezu u korporativnim okruženjima gdje su stvari osjetljive, kompleksne i ponekad sliče kuli od karata, ali u slučaju ovako ozbiljne zaraze jedini ispravan korak je bez odlaganja instalirati sigurnosne zakrpe i nadati se da će sve biti u redu; posljedice ignoriranja ili otezanja mogu biti značajno skuplje od poteškoća u radu sustava.

I ne samo to, jer uvijek ima više: ranjivost se odnosi na SMBv1 protokol koji će još malo pa proslaviti

svoj trideseti rođendan. To je star, star, star protokol. Nakon njega nastali su SMBv2 i SMBv3. Nitko ne bi trebao koristiti SMBv1. Gotovo ništa više ne ovisi o tom protokolu, osim uistinu starog softvera i hardvera: postoje, primjerice, modeli starih mrežnih pisača još uvijek u upotrebi, a koji ne znaju komunicirati na novijim SMB protokolima; potreba za kompatibilnošću unazad nagovorit će drugu stranu da odustane od novijih verzija tog protokola radi ostvarivanja ikakve komunikacije sa strojem koji priča samo staroslavenski.

U tom grmu leži ranjivi zec: ako ste neko računalo otvorili prema Internetu, WannaCry će pokušati spustiti protokol na razinu SMBv1 i tako iskoristiti sigurnosne propuste kako bi zarazio računalo.

Zato, provjerite i pogasite sve portove koji ne moraju apsolutno nužno biti izloženi jednom tako prijateljskom okruženju kao što je Internet.

Koristite li moderne operacijske sustave (Win10, WS 2016), možete uključiti audit za SMB1 protokol pomoću ove jednostavne PowerShell naredbice:

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

Event log će zabilježiti ako tko pokušava pristupiti zastarjelim protokolom. Pregledajte log, nabavite čekić i posjetite krivca/e, te mu/im pod prijetnjom upotrebe čekića na prstićima isključite SMBv1. Imate li neki od onih gore navedenih starih pisača možete (i trebate) ih bez puno milosti zatući spomenutim čekićem jer vjerojatno ne postoji softverska nadogradnja za njih, a oni sve dok su “živi” predstavljaju sigurnosnu prijetnju cijeloj mreži.

Kad ste to obavili, isključite SMBv1 na svim ostalim računalima i poslužiteljima. Naime, upravo zbog problema kompatibilnosti sa opskurnim komadima softvera i hardvera SMBv1 nije automatski isključen čak ni na najnovijim Microsftovim operacijskim sustavima. Tako je barem bilo do ovog napada, nadajmo se da će se praksa promjeniti: modernom svijetu SMBv1 potreban je koliko i UUCP protokol.

Informacije radi, Microsoftova sigurnosna zakrpa riješila je ove probleme:

CVE-2017-0143

CVE-2017-0144

CVE-2017-0145

CVE-2017-0146

CVE-2017-0148

Napad originalnim WannaCry softverom usporen je zanimljivim otkrićem: kako na blogu spominje MalwareTech (https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html [3]), ransomware bi prilikom aktivacije tražio pristup adresi http://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ [4] i ako bi se nešto odazvalo (tj. ako bi netko aktivirao tu domenu), program bi se deaktivirao. Bilo je, dakle, dovoljno registrirati tu domenu da u vrlo kratkom vremenu značajno uspori broj novih infekcija: svako zaraženo računalo koje bi moglo pristupiti navedenoj adresi ne bi bilo napadnuto; nažalost, računala koja ne mogu pristupiti domeni jer su, primjerice, zabranjene sve adrese osim onih potrebnih za obavljanje posla i dalje su osjetljiva na napad jer malware ne može pristupiti navedenoj adresi i zbog toga uredno aktivira maliciozni kod.

Unatoč činjenici da je ovo slučajno otkriće usporilo izvorni napad, zlonamjerni su autori u opticaj pustili nekoliko mutacija koje imaju drugačiji “kill switch” - ili ga uopće nemaju. Sinovi WannaCry zlodjela zato su još opasniji, ali ne zaboravimo da su i oni jednako tako ovisni o ljudskoj gluposti:

otvaranju sumnjivih e-mail privitaka i šlampavoj sistemskoj administraciji.

Da ponovim: unatoč apokaliptičnom vrištanju medija, zaštititi se vrlo je jednostavno, barem sistemašima: valja instalirati sve sigurnosne zakrpe. Ne škodi potom niti posvuda isključiti SMBv1.

Korisnici? Njih treba uporno i iznova educirati o sigurnosti sustava, paziti da imaju redovito osvježavane antiviruse i sve sigurnosne zakrpe, te povremeno i preventivno prijetiti čekićem po prstićima.

P.S. jeste li provjerili što na sve to kaže vaš vatrozid?

pon, 2017-05-15 14:08 - Radoslav Dejanović**Vijesti:** CERT [5]
Windows [6]
Sigurnosni propusti [7]
Kategorije: Operacijski sustavi [8]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: wannacry [9]
cryptolocker [10]

Source URL: https://sysportal.carnet.hr./node/1740

Links
[1] https://www.bloomberg.com/news/articles/2017-05-04/seriously-beware-the-shadow-brokers
[2] https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication
[3] https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
[4] http://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/
[5] https://sysportal.carnet.hr./taxonomy/term/9
[6] https://sysportal.carnet.hr./taxonomy/term/12
[7] https://sysportal.carnet.hr./taxonomy/term/14
[8] https://sysportal.carnet.hr./taxonomy/term/26
[9] https://sysportal.carnet.hr./taxonomy/term/102
[10] https://sysportal.carnet.hr./taxonomy/term/103