USB kondom, cryptolocker za Linux i ostale ljetne razbibrige

Lutajući bespućima internetske zbiljnosti u ove vruće dane, čovjek naleti na svakojake stvari. Neke od njih su "iz struke", ali na prvi pogled se čini da nisu ozbiljne. Znamo se i mi tekiji zezati, i to ne samo na račun korisnika, zar ne? Jedna od tih veselih vijesti jest da možete kupiti USB kondom. Ne za seks, nego za sigurno punjenje mobitela! O čemu se tu radi?

Svi znamo da je se mobitel može puniti priključivanjem na punjač, ali i na USB port računala, iako takva veza ima dvije funkcije: usput možemo prebaciti podatke na računalo. No dok smo negdje u gradu, na suhom smo kad nam se baterija isprazni. Zato su se ljubazni trgovci pobrinuli da nam na prodajnim mjestima ponude pultove za punjenje USB uređaja. Dok čekate u banci, u salonu telekoma, u trgovačkom centru, kafićima, a od nedavno i kraj Bandićevih fontana, gdje su stavljene klupe naših vrlih mladih kreativaca, sa fotoelektričnim ćelijama na vrhu i USB portovima sa strane - na svim tim čudnim mjestima možete dopuniti baterije svog pametnog telefona, MP3 svirača, tableta... Biti stalno na vezi je naporno, ne samo za vlasnike koje pištanje prekida u poslu i razmišljanju, nego i doslovno iscrpljujuće za baterije. Baš dobro, možeš malo predahnuti i besplatno napuniti baterije, kako vlastite tako i one na uređaju. Ali, da li ste ikad pomislili da možda struju plaćate svojim podacima spremljenim na mobitelu? Tko vam garantira da se istovremeno s punjenjem baterije ne "prazne" podaci s vašeg uređaja?

I tu na scenu stupa USB kondom. Radi se o tome da su "precvikane" žice kroz koje putuju podaci, a one kroz koje ide struja su i dalje tu. Jednostavno, zar ne? Pa sad svi paranoici i sigurnosno osviješteni geekovi, navalite, u svoju zbirku alata za preživljavanje u digitalnom svijetu dodajte i USB kondom. Nije nam namjera da ga ovdje reklamiramo, lako ćete ga sami naći ako vas zaista zanima. Ali oni najspretniji najoprezniji ionako neće odriješiti kesu, već će sami napraviti USB kondom u kućnoj radinosti. Da budu 100% sigurni, zar ne?! :)

Druga zabavna vijest odnosi se na otkriće virusa za Linux. Virusi za Linux su prava rijetkost. Ne tvrdimo da ih nema, ali rijetko se pojave i brzo nestanu, jer se odmah izdaju zakrpe. U svojoj karijeri sistemca godinama sam na svom računalu na poslu koristio Linux bez antivirusnog programa. Kad bih povremeno osjetio potrebu provjeriti da li je sve u redu, instalirao bih i pokrenuo clamav, koji naravno ništa ne bi pronašao. Onaj virus, zapravo crv, kojeg sam jednom prilikom ulovio, našao sam na računalu kolege koji je otišao na godišnji odmor i ostavio upaljeno računalo kako bi cimeri mogli koristiti njegov printer. Tih ljetnih mjeseci nitko se nije sjetio da instalira zakrpe, pa se tako naselila gamad koju sam ulovio kako skenira po lokalnoj mreži i traži drugo ranjivo Linux računalo.

No vratimo se našoj vijesti koju sam našao na linuxblog.darkduck.com. Pripovjedač u prvom licu priča kako je s mreže skinuo virus za Linux. Odzipao ga i, da mu olakša posao, instalirao ga kao root. Virus se nije htio pokrenuti. Istražio je o čemu se radi. Umjesto u /usr/local/bin virus se instalirao u /usr/bin, gdje nema dozvolu za pisanje, pa ne može kreirati datoteke. Na nekom kineskom siteu našao je popravljene .configure i .make datoteke. Prekompajlirao je virus i ponovo ga instalirao. Prilikom pokretanja, virus se žalio da nema biblioteku cmalw-lib-2.0. Guglajući, našao je da se ta bibioteka nalazi na CentOS-u, ali ne na Ubuntuu, koji on koristi. Naš haker/bloger skinuo je izvorni kod te biblioteke, napravio .deb paket i instalirao ga na svoj Ubuntu. Ponovo je pokrenuo virus, ali ovaj je na zvučnik pustio beep i izblesirao se bacivši core dump. Toliko mu pomažeš, a on nikako da proradi! Pregledom logova ustanovio je kako je virus pretpostavio da je datotečni sustav tipa ext4, pa je zvao njegov api kako bi obavio enkripciju diska. Naš bloger koristi btrfs, a ne ext4! :)

Već je bilo kasno, pa je grepao kroz izvorni kod virusa, našao bitcoin wallet na koji treba poslati

ucjenu da bi dobio ključ za dekripciju, te iz čistog sažaljenja poslao 5 dolara u bitcoinima i otišao spavati. L0L! :)

Dok svijetom haraju cryptolockeri koji zaražuju Windows računala, pojava faličnog cryptolokera za Linux čini se tragikomičnom. Jesu li to crnošeširaši pokušali prenijeti cryptolocker za Windowse na Linux? Ili su si dali truda da ga napišu ispočetka? Da li je kod preuzet iz zbirke koja je pobjegla iz lagera NSA? Ostavit ćemo ova pitanja neodgovorenima i nastaviti bezbrižno koristiti Linux.

Barem još neko vrijeme, dok se crnošeširaši ne izvješte, ne nauče razliku između /usr/bin i /usr/local/bin, shvate da Linux nema samo jedan zadan datotečni sustav kao Windowsi, itd. its. Priča zvuči komično, koliko je truda čovjek uložio da pomogne virusu da proradi na Linuxu, pa opet ništa od toga!

Linux drži oko 95 posto tržišta servera, ali na desktopu je još sporedan igrač. Doduše, u blagom je porastu, netmarketshare.com kaže da je na 2,36% i raste, za razliku od Appleovog OSX-a koji je na 3,49%, ali mu se broj korisnika zadnjih godinu dana smanjuje. Ostatak čine razne verzije Windowsa. To je svakako jedan od razloga zašto nema mnogo virusa za Linux. No postoje i drugi razlozi, tehničke naravi, ali to ćemo ostaviti za neku drugu priliku. Iako bi zapravo, barem u teoriji, trebalo biti obrnuto. Zar nije lakše napraviti virus za softver otvorenog koda, kad već imaš na raspolaganju izvorni kod, koji možeš proučiti, pronaći ranjivosti?

Paranoični smo po prirodi, jer znamo kako svijet funkcionira. Velika riba jede malu ribu, pod krinkom slobodnog tržišta. Kad mali ojačaju i pokušaju se uključiti u utrku, tada se vraća protekcionizam, a konkurenti proglašavaju "zločestima". Veliki igrači nameću svoja pravila i u svijetu informatike, a softver i hardver otvorenog koda još se pušta i podnosi radi kreativnosti koja se tu rađa, a koja se može iskoristiti i u komercijalnom svijetu. No mi paranoici uvjereni smo da će se stvari u budućnosti promijeniti, da će od 1984. godine nadalje smjeti programirati samo certificirani i uniformirani, strogo nadzirani programeri, koji će raditi samo ono što im se kaže. :)))

Dakle, dok još možete birati, ako ste odlučili nabaviti/napraviti USB kondom, red je da na Linux instalirate antivirus. Naravno, open source i besplatan. Evo, ja ću prvi. Instalirao sam i pokrenuo ClamAV:

```
$ clamscan -r .
----------- SCAN SUMMARY -----------
Known viruses: 6300275
Engine version: 0.99.2
Scanned directories: 2422
Scanned files: 55719
Infected files: 0
Total errors: 0
Data scanned: 17513.27 MB
Data read: 38973.16 MB (ratio 0.45:1)
Time: 1874.466 sec (31 m 14 s)
```

Nema virusa, čak ni onih za Windowse. :)

I naravno, backup, backup, backup... Nema veze da li koristite Windowse, Linux ili nešto treće. Ne mora vas naciljati cryptolocker, može se dogoditi i običan hardverski kvar. Sad je vrijeme ljetnih oluja, blizu vas može udariti grom i spržiti vam hladnjak, TV, računalo. :(

A što se tiče kriptiranja datotečnog sustava, kriptirajte ga sami! Za svaki slučaj. Ako ste paranoični, ne treba vam ni razlog ni opravdanje. Just do it! :)

I na kraju, dok na ovim paklenim vrućinama dišete na škrge i razmišljate kako vam se teško koncentrirati na teže zadatke jer vam moždani valovi sve više nalikuju na ravne crte, pogledajte ovu mapu svijeta [1] koju su napravili kolege iz Kasperskog. Uživo možete pratiti, gotovo u realnom vremenu, gdje se trenutno u svijetu događaju cyber napadi. Usput ćete dobiti i statistiku, na primjer koje su države pod najvećim udarom, koji su trenutno najčešći virusi itd. Statistiku prikupljaju brojni

zaštitni alati koje je Kasperski prodao kupcima širom svijeta. Gore desno čeka vas gumbić na kojem piše "Am I Infected?" Ako se odvažite kliknuti na njega, neće vam se skenirati računalo, već će vam ponuditi da besplatno isprobate njihove proizvode na raznim OS-ovima. Naravno, nema Linuxa, osim ako Android ne smatrate jednom njegovom verzijom.

čet, 2017-07-13 19:46 - Aco Dmitrović**Vote:** 5

Vaša ocjena: Nema Average: 5 (2 votes)

story_tag: kolumna informacijska sigurnost [2]

Source URL: https://sysportal.carnet.hr/node/1749

Links
[1] https://cybermap.kaspersky.com
[2] https://sysportal.carnet.hr/taxonomy/term/110