SANS Telekom Srbija

OUCH! | June 2017

Mesečni bilten za podizanje svesti o bezbednosti informacija

OUCH!

U OVOM BROJU...

- Primena ispravki
- Bekap
- Sajber pecanje

Šta smo naučili iz WannaCry napada

Uvod

Gost urednik

Dr. Johannes Ullrich je dekan Istraživanja za SANS tehnološki institut i osnivač veb sajta DShield.org. Odgovoran je za **SANS Internet Storm Center** koji nadgleda aktuelne sajber pretnje po IT bezbednost. Takođe je i predavač na kursevima Web Application Security (**DEV522**), Intrusion Detection (**SEC503**) i IPv6 (**SEC546**).

Nedavno ste sigurno bili svedoci velike medijske pažnje posvećene novom sajber napadu pod imenom "WannaCry". "WannaCry" je zarazio preko 200 000 računara i onemogućio različite organizacije, uključujući bolnice u Velikoj Britaniji, da pristupe svojim podacima. Nekoliko je razloga koji su doprineli da ovaj napad dobije tako veliku pažnju. Prvo, brzo se širio od računara do računara iskorišćavajući poznatu ranjivost Windows računara. Drugo, ovaj tip napada izveden je pomoću malvera (virusa) poznatog pod imenom "Ransomware", što znači da jednom kada zarazi vaš računar malver enkriptuje sve vaše podatke i time onemogućava da im pristupite. Jedini način da ponovo pristupite vašim podacima je da ih vratite iz bekapa ili da platite napadaču otkupninu u iznosu od 300 USD da bi ih dekriptovao. Treće, i najvažnije, ovaj napad nikada nije trebalo da se desi. Ranjivost koju je "WannaCry" iskorišćavao na Windows računarima bila je već dobro poznata Microsoft-u, koji je ispravku za nju objavio nekoliko meseci ranije. Nažalost, veliki broj organizacija nije na vreme primenio ispravku, ili još uvek koristi operativne sisteme poput Windows XP koji su toliko stari da ispravka za njih nije ni bila dostupna. U nastavku predstavljamo tri jednostavna koraka koja možete preduzeti kako biste osigurali da vas napadi poput "WannaCry" nikada neće ugroziti.

Primena ispravki

Pre svega, obezbedite da vaši računari, mobilni uređaji, aplikacije i sve drugo što je povezano na Internet budu ažurni. Sajber kriminalci neprestano traže nove ranjivosti u softveru na vašim uređajima. Kada otkriju ranjivosti oni koriste posebne programe da hakuju uređaje koje koristite. U međuvremenu, kompanije koje su kreirale softver za vaše uređaje vredno rade na ispravci tih ranjivosti i objavljivanju ispravki. Ako obezbedite da vaši računari ili mobilni uređaji instaliraju te ispravke značajno ćete otežati posao nekome ko želi da vas hakuje. Upravo ova činjenica je ono što najviše frustrira kod širenja WannaCry. Ispravke za onemogućavanje i zaustavljanje ovog napada Microsoft je objavio skoro dva meseca ranije. Da su organizacije ažurirale svoje računare, napad nikada ne bi uspeo. Kako biste obezbedili da vaši uređaji ostanu ažurni, omogućite automatsko ažuriranje kad god je to moguće. Ovo pravilo se odnosi ne samo na računare i

Šta smo naučili iz WannaCry napada

mobilne uređaje već i na skoro sve tehnološke uređaje povezane na mrežu kao što su televizori povezani na Internet, kućni ruteri, konzole za igrice, a jednog dana verovatno i vaš automobil. Ako su vaši operativni sistemi ili uređaji toliko stari da više nisu podržani bezbednosnim ispravkama, kao što je slučaj sa Windows XP, zamenite ih novim koji su podržani.

Tri jednostavna, ali ključna koraka za zaštitu od napada poput WannaCry su: neka vaši računari uvek imaju primenjene najnovije ispravke, pazite se napada putem elektronske pošte (pecanje) i kreirajte bekape za vaše sisteme.

Bekap

U nekim slučajevima, sajber napadi poput Ransomware-a mogu zaraziti i ažurne sisteme. Zato je drugi način da se zaštitite taj da kreirate bekap vaših podataka. Bekapi su rezervne kopije vaših informacija koje čuvate negde drugde osim na vašem računaru ili mobilnom uređaju. Kada izgubite važne podatke možete ih oporaviti korišćenjem bekapa. Nažalost, veliki broj ljudi ne kreira redovno rezervne kopije iako je taj postupak jednostavan i jeftin. Postoje dva načina za izradu bekapa: na fizičkom medijumu ili korišćenjem Cloud-a. Oba pristupa imaju svoje prednosti i mane. Ako niste sigurni koji način da koristite možete istovremeno koristiti oba.

Fizički medijumi su uređaji nad kojima vi imate kontrolu, poput eksternih USB diskova ili mrežno dostupnih diskova, kod vaše kuće ili na poslu. Prednost u slučaju korišćenja vaših sopstvenih fizičkih medijuma je u tome što vam oni omogućavaju da veoma brzo kreirate rezervne kopije velikih količina podataka i isto tako brzo te podatke oporavite. Mana ovakvog pristupa je što ako se desi da budete zaraženi malverom poput Ransomware-a postoji mogućnost da se zaraza proširi i na vaš bekap. Ako koristite fizičke medijume za izradu bekapa pobrinite se da rezervne kopije vaših podataka ne budu mrežno dostupne i budu na bezbednoj lokaciji. Vodite računa da sve rezervne kopije jasno obeležite. Cloud rešenja predstavljaju online servise koji kreiraju rezervne kopije i čuvaju vaše podatke na Internetu. Najčešće je dovoljno da na vašem računaru instalirate softver koji se stara o svemu. Prednost Cloud rešenja za bekap je u njihovoj jednostavnosti. Dodatno, ako se zarazite Ransomware-om malver obično ne može da pristupi vašem bekapu u Cloud-u. Mana je u tome što bekap i oporavak velikih količina podataka može dugo da traje. Ne zaboravite da proverite pravila privatnosti i bezbednosti bekapa u Cloud-u. Proverite da li servis za izradu bekapa nudi odgovarajuće metode zaštite kao što su enkripcija vaših podataka i jake metode za autentifikaciju.

Šta smo naučili iz WannaCry napada

Sajber pecanje

Konačno, loši momci neprestano unapređuju i menjaju svoje metode za napad. Sajber kriminalci često koriste metod poznat pod imenom pecanje (phishing) da izvrše napad i zaraze žrtvu. Pecanje se sprovodi tako što vam sajber kriminalci pošalju elektronsku poruku (mejl) sa ciljem da vas navedu da otvorite inficirani prilog ili posetite maliciozni veb sajt. I u jednom i u drugom slučaju vaš računar se može zaraziti. Iako "WannaCry" nije koristio ovaj metod napada, on se često koristi u mnogim drugim tipovima napada, uključujući većinu tipova Ransomware-a. Pritom, sajber kriminalci koji su razvili WannaCry će u nastupajućim mesecima bez sumnje unaprediti načine na koje napadaju i upotrebiti nove tehnike poput pecanja, a sve sa ciljem da inficiraju još više računara. Kako biste se zaštitili od ovakvih napada putem elektronske pošte najvažniji je zdrav razum. Ako poruka deluje čudno, sumnjivo ili suviše dobro da bi bila istinita, najverovatnije je u pitanju napad.

Saznajte više

Prijavite se na OUCH! mesečni bilten za podizanje svesti o bezbednosti informacija namenjen svima, pročitajte prethodne brojeve OUCH!-a i saznajte više o SANS-ovim rešenjima za unapređenje svesti o bezbednosti informacija na našoj internet prezentaciji securingthehuman.sans.org/ouch/archives.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Dodatne informacije

Šta je malver:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Bekap:	https://securingthehuman.sans.org/ouch/2015#august2015
Sajber pecanje:	https://securingthehuman.sans.org/ouch/2015#december2015
Bezbedno korišćenje Cloud-a:	https://securingthehuman.sans.org/ouch/2016#november2016

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Кэти Клик, Cheryl Conley
Preveli: Dragan Ristić i Gordana Živanović