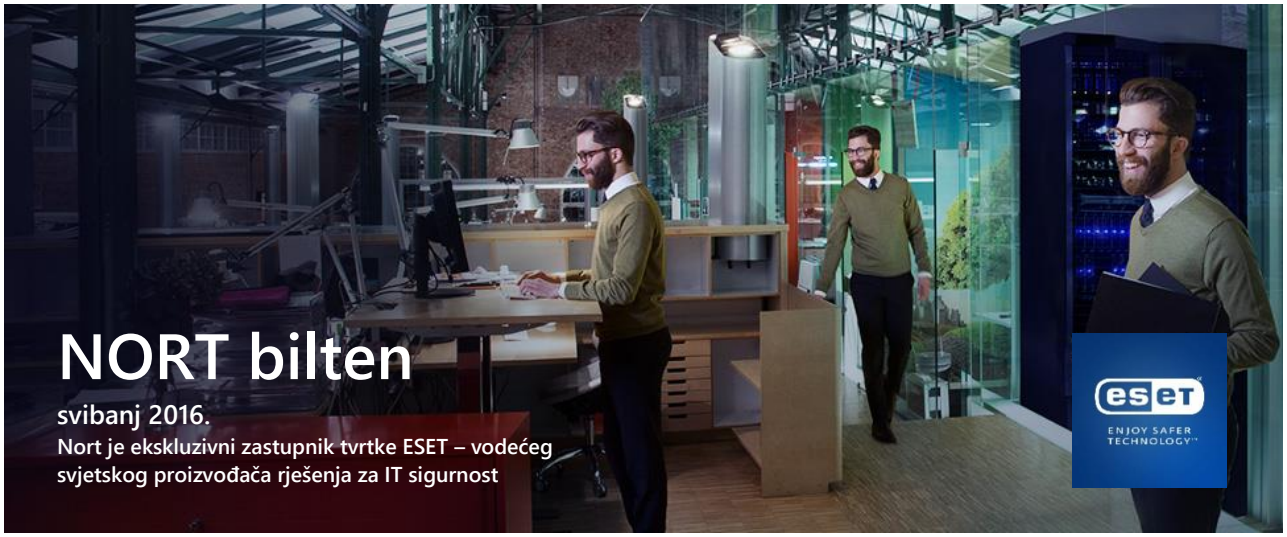


Poštovani partneri i korisnici,

Ovaj bilten posvećujemo temi ransomware-a, iznimno neugodne pojave za sve članove umrežene zajednice. Vjerojatno je barem netko iz vašeg kruga poznanika ili kolega na ekranu svojeg računala imao prilike vidjeti poruku iz noćne more koja ga obaviještava da su podaci na računalu zaključani te da će biti bespovratno izgubljeni ukoliko korisnik ne uplati odgovarajuću sumu anonimnim iznuđivačima. S obzirom na rizik kojeg predstavlja ova vrsta malicioznog koda, prevelik broj korisnika još uvijek prepušta sigurnost svojih podataka slučaju ili se u potpunosti oslanja na antivirusne programe te zanemaruje potrebu kreiranja backup-a. Još prije ere virusa je bilo poznato kako nije pametno držati vrijedne podatke u samo jednom primjerku. Radi pojave nemjerljivog broja prijetnji na internetu (prema nekim procjenama, u 2015. godini je registrirano preko 60 milijuna jedinstvenih primjeraka malicioznog koda), korisnici često gube iz vida banalne prijetnje kao što je fizičko oštećenje računala, od kojeg ne štiti niti jedan antivirusni proizvod. Ovo nas vodi do zaključka kako pouzdana softverska zaštita podataka ne postoji, već je važne podatke potrebno kopirati i držati na odvojenom mjestu.

Ruku na srce, maliciozni kod za vlasnike računala ipak predstavlja veću prijetnju od požara, zemljotresa ili vruće kave. Ransomware predstavlja posebno podlu vrstu malicioznog koda koja, kako joj ime govori, služi za iznuđivanje novaca od vlasnika računala. Samo jedna podvrsta ransomware-a s nazivom Cryptowall je odgovorna za otprilike 325 milijuna dolara štete tijekom 2015. godine. S obzirom da prosječna cijena „otkupa“ iznosi oko 500 dolara, to znači da je oko 650.000 korisnika platilo otkup, dok je broj inficiranih računala vjerojatno mnogostruko veći. Nije loše imati u vidu i procjene nezavisnih analitičara koje govore kako će ukupna šteta od informatičkog kriminala 2019. godine dosegnuti 2,1 trilijun američkih dolara, ili četiri puta više od procijenjene štete u 2015. godini.

Koliko je ransomware opasan? Možda je najbolje pitati predstavnika FBI-a, koji je na konferenciji Cyber Security Summit 2015 izjavio: “Da budem iskren, često savjetujemo ljudima da jednostavno plate otkupninu.” Iako većina antivirusnih programa štiti od velike većine malicioznih kodova, dovoljno je da jedan jedini cryptolocker „prođe“ kako bi se korisnik našao u poziciji da mora prihvatiti savjet FBI-a. Ljudi u takvim slučajevima često kažu „to se samo meni može dogoditi“. Naravno da to nije istina. To se može dogoditi svakome tko zanemaruje osnovna pravila održavanja sigurnosti podataka. Nekome se silno kopiranje podataka i ograničavanje funkcija određenih korisničkih programa može učiniti suvišnom gnjavažom, pa čak i simptomom zasebne vrste IT-paranoje. Međutim, ukoliko se budete pridržavali osnovnih pravila sigurnosti, svaka ružna priča o gubitku podataka koju čujete će na vašem licu izazvati tek zagonetan osmijeh.

Čuvajte svoje podatke.

Vaš NORT

Nort d.o.o. je ekskluzivni distributer antivirusnog programa NOD32 za Hrvatsku, Srbiju, Bosnu i Hercegovinu, Crnu Goru, Makedoniju, Kosovo i Albaniju

SADRŽAJ

Fenomen ransomware-a i što mi mislimo o tome

Rješenja za IT sigurnost tvrtke ESET spadaju među najpouzdanije proizvode na tržištu i štite korisnike od gotovo svih „kripto virusa“ koji služe za iznuđivanje novaca od vlasnika „zaključanih“ podataka. Međutim, u stvarnom svijetu ne postoji stopostotna zaštita. Danas postoje platforme za izradu malicioznog koda, što znači da proizvodnja virusa više ne zahtjeva visoku razinu informatičke pismenosti. Ova činjenica se odražava u ogromnom broju novih vrsta i podvrsta malicioznih kodova koji se pojavljuju na dnevnoj bazi – nezavisni njemački institut za informatičku sigurnost AV Test registrira preko 390.000 novih uzoraka štetnih kodova dnevno. Uz pretpostavku o uspješnosti detekcije određenog antivirusnog programa od 99,99%, još uvijek će preostati neprimijećeno 39 prijetnji dnevno. Za gubitak podataka je dovoljna jedna.

Načini napada i zašto antivirus ne može zaustaviti sav ransomware

Maliciozni program koji šifrira podatke na računalima najčešće stiže – ne biste vjerovali – putem e-pošte. Među rizičnim kanalima su i inficirani web serveri i Remote Desktop Protocol. U prvom slučaju se napad

oslanja na naivnost prosječnog korisnika koji će teško odoljeti iskušenju da otvori link na neku zanimljivu vijest ili privitak namijenjen upravo njemu, pa je neophodno neprestano upozoravati korisnike na mogućnost zaraze ovim putem. Pod udarom je niz raznih datoteka na svim odredištima na kojima napadnuti korisnik ima pravo pisanja/brisanja (lokalni i vanjski diskovi, USB memorije, mapirani mrežni diskovi, mapirani *cloud* diskovi,…).

Razlog iz kojeg antivirusni programi nisu savršeno pouzdani u otkrivanju ransomeware-a je u tome što ransomware nakon obavljanja svojeg prljavog posla na računalu nestane te je nemoguće pronaći njegov trag i poslati ga proizvođaču antivirusnih rješenja kako bi ovaj „naučio“ svoje proizvode da ga ubuduće prepoznaju. Čak i antivirusni programi koji imaju razvijenu tzv. heuristiku, to jest algoritam koji maliciozne kodove prepoznaje po njihovom karakterističnom ponašanju, ne mogu uvijek razlikovati ponašanje ransomeware-a od ponašanja savršeno dobroćudnog programa. Antivirusni program je moguće konfigurirati tako da proširi definiciju „rizičnog“ ponašanja programa, ali pretjerano osjetljiv antivirusni program bi zatrpao korisnika „false-positive“ upozorenjima i vrlo brzo doveo do frustracije.

Uspješan napad ransomeware-om na računalu korisnika kreira šifrirane kopije izvornih dokumenata koje je nemoguće „otključati“ bez pomoći napadača, koji u pravilu traže između 300 i 2000 američkih dolara za „ključ“. Šifrirane kopije obično nose specifične ekstenzije („*.omg“, „*india.com“, „*anointernet.com“, „*lycos.com“, „*nonpartisan.com_IQ*“, itd.).

Što činiti kako bi se napad spriječio?

Iako smatramo da je proizvod kojeg zastupamo izuzetno pouzdan u detekciji prijetnji, nikada ne bismo tvrdili da je instalacija antivirusnog software-a sve što trebate napraviti za sigurnost svojih podataka. Uostalom, i sam ESET je nedavno u obitelj svojih proizvoda dodao proizvode za backup i povrat podataka tvrtke StorageCraft, čime je pokazao da u ovom poslu nema mjesta aroganciji. Ukoliko je naš cilj zaštita podataka korisnika, tada je potrebno napraviti **apsolutno sve** da bi se rizik od njihovog gubitka sveo na minimum, a ne samo ono što mi vjerujemo da je dovoljno.

Dakle, čak i u našoj ulozi zastupnika izuzetno pouzdanih antivirusnih rješenja mi svojim korisnicima savjetujemo da poduzmu sljedeće mjere za zaštitu svojih podataka:

1. **Backup.** Mi smo pobornici najstrože definicije ovog termina, koja ne priznaje jednostavno kopiranje podataka na bilo koji mrežni disk ili uređaj koji ostaje spojen na isti sistem kao i nosač originala podataka. Backup označava redovito presnimavanje važnih podataka na medij koji se nakon stvaranja kopije iskapča i **fizički odvaja** od nositelja originala podataka. U idealnoj situaciji ćete koristiti najmanje dva diska / USB memorije naizmjenično. Više o temi backup-a možete pronaći u našoj bazi znanja.

2. **Korištenje antivirusnog software-a i drugih sigurnosnih tehnologija.** Sva računala na mreži jednostavno moraju imati antivirusni program, ali uvijek imajte u vidu da antivirusni programi nikada nisu bili namijenjeni zaštiti od apsolutno svih vrsta napada.

3. **Nadogradnja i sve sigurnosne zakrpe i nadopune operacijskih sustava, kao i nadogradnja svih aplikacija na računalima, uključujući i antivirusni program, na najnovije verzije.** Korištenje zastarjelih računalnih sustava koji više nisu podržani od strane proizvođača povećava rizik od uspješnog napada virusom. Preporučujemo da redovito preuzimate i instalirate **sve sigurnosne zakrpe i nadopune operacijskog sustava** kao i **svih aplikacija** koje imate instalirane na računalu. Prema našim iskustvima s terena, većina uspješno napadnutih korisnika je imala instaliran Windows XP i staru ili pogrešno konfiguriranu verziju ESET-ovog programa. Microsoft je napustio Windows XP još u travnju 2014 te sigurnosni propusti tog operativnog sistema nikada neće biti ispravljeni. Svakako nadogradite ESET proizvod na najnoviju dostupnu verziju i provjerite da li je aktivna funkcija *ESET Live Grid*.

Što učiniti u slučaju uspješnog napada ransomware-om?

Ovo je trenutak kada počinju stizati loše vijesti – podatke „zaključane“ ransomware-om je trenutno praktički nemoguće dešifrirati bez ključa, pa žrtvi napada u slučaju da nema backup podataka u pravilu preostaje samo plaćanje „otkupnine“. Pri tome imajte na umu riječi ESET-ovog stručnjaka za sigurnost i glavnog urednika portala We Live Security Raphaela Labaca Castro: „Zapamtite, ovo nije uslužna djelatnost, to su cyber-kriminalci“. Drugim riječima, ne postoje nikakve garancije da ćete nakon plaćanja vratiti podatke, kao što nema garancije da nakon plaćanja nećete biti podvrgnuti ponovnom napadu.

U vrlo rijetkim slučajevima je moguće vratiti podatke pomoću sitnih trikova kao što je korištenje opcija *File History* ili *System Protection* u Windows-ima koje omogućuju povrat prethodne verzije zaključanih datoteka (više o svim mogućnostima vraćanja podataka u slučaju zaključavanja od strane ransomware-a pogledajte u našoj bazi znanja).

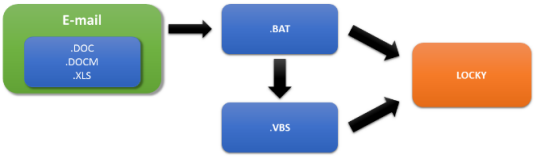
Zaključak

Isključivo oslanjanje na antivirusni program radi zaštite podataka na vašem računalu predstavlja prilično rizičnu igru. Opasnosti od ransomware-a su tolike da agencije kao što su američki Department of Homeland Security (DHS) i kanadski Canadian Cyber Incident Response Centre (CCIRC) izdaju upozorenja kako bi pojedinci i poduzeća postali svjesni prijetnje. Nadamo se da svima koji su pročitali ovaj članak nikakva dodatna upozorenja neće biti potrebna.

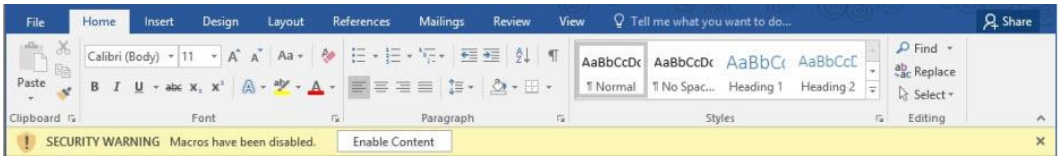
Analiza infekcije Locky ransomeware-om

Članak preuzet s portala www.welivesecurity.com
Autor: Diego Perez, ESET Research Lab, Latinska Amerika

Posljednjih mjeseci je zabilježen značajan porast korisnika zaraženih ransomware-om poznatim pod nazivom Locky, koji se koristi kako bi zaključao korisnikove podatke i zatim iznudio otkupninu u bitcoin-ima. Ali kako ova prijetnja uspijeva prodrijeti u računalne sisteme i oteti podatke? Dijagram niže prikazuje postupak zaraze koji vodi do isporuke malicioznog koda. Korisnik prima e-mail u vezi raznih tema koji može biti na raznim jezicima. Ovaj email u privitku sadrži Microsoft Office dokument (.DOC, .DOCM ili .XLS). Dokument kreira BAT datoteku, koja zatim kreira novu datoteku pisanu VBScript-om. Ove dvije datoteke će kasnije isporučiti glavnu prijetnju, koju je ESET identificirao pod nazivom Win32/Filecoder.Locky.



Navedeni Office dokument sadrži maliciozne makro naredbe koje se izvršavaju kada korisnik klikne na gumb „Enable Content“ u Office dokumentu. Nakon što su makro naredbe omogućene, maliciozni kod se izvršava automatski.



Tri specifične linije koda kreiraju BAT datoteku s nazivom “Ugfdxafff.bat”. Zadatak ove datoteke je kreiranje nove .exe datoteke u VBScript-u i URL adrese s koje će se učitati maliciozni kod. Nakon pokretanja, BAT datoteka će obrisati VBScript kod i samu sebe kako bi uklonila sve tragove sa sistema. Ovaj proces se vidi na sljedećoj slici:

Ovaj niz međukoraka omogućuje da se napad zaustavi prije nego što stigne do vašeg inbox-a ili prije pokretanja makro naredbi. Uzrok ulaska ove prijetnje u sistem je prihvaćanje neželjenih „spam“ poruka od strane korisnika ili zaposlenika kompanije, nakon čega dolazi do „otmice“ podataka koja može prouzročiti velike probleme. Stoga je neophodno imati na umu rizike povezane s korištenjem makro naredbi u Microsoft Office dokumentima. Iz tog razloga je ključno da svi korisnici budu upoznati s trendovima u računalnom kriminalu i posljedicama malicioznog koda kao što je ransomware te da uvedu visoke standarde računalne sigurnosti. Naravno, važno je da koriste ispravno konfiguriranu najnoviju verziju antivirusnog programa.

Koliko je ransomware opasan za prosječnog korisnika i zašto novinar časopisa Wired danas ima tri backup-a

Tijekom posljednje dvije godine primjetno je porastao broj napada ransomware-om, malicioznim kodom koji je stvoren s prvenstvenom namjenom iznuđivanja. Nakon što je pokrenut, ovaj maliciozni kod šifrira podatke, kao i čitave uređaje. Pristup podacima je moguć samo nakon što žrtva napada plati otkupninu (tako bi barem trebalo biti – ovdje ne postoje garancije). Naravno, ovo predstavlja vrlo efikasan oblik cyber kriminala.

Iako ransomware nije nova pojava, mnogi stručnjaci njegovu evoluciju u 21. stoljeću smatraju zabrinjavajućom. Ova rastuća prijetnja je u stanju nanijeti ozbiljnu financijsku, materijalnu i psihološku štetu žrtvama. I to nije sve. Do nedavnog vremena se većina poslovnih i privatnih korisnika mogla smatrati sigurnom od ovakvih napada. To danas nije slučaj, jer napadi ransomware-om više ne predstavljaju rijetkost, već su se pretvorili u masovnu pojavu.

“Šteta koju je ransomware u stanju nanijeti korisnicima time što ih sprječava da pristupe podacima predstavlja sve veći razlog za zabrinutost,“ izjavio je Camilo Gutiérrez Amaya u ESET-ovom istraživanju o cyber kriminalu objavljenom 2016. godine. “Ovo je jedna od najopasnijih sigurnosnih prijetnji pošto iskorištava nedostatak odgovarajućih backup procedura i neodgovarajuće sigurnosne prakse u kompanijama [što se odnosi i na privatne korisnike].”

Ne podcijenjujte prijetnju

Gutiérrez Amaya ističe važnost pravovremene izrade kopija vaših podataka kao što su fotografije, poslovni dokumenti ili vaša kolekcija glazbe, istovremeno naglašavajući kako izrada kopija ostaje zanemareni aspekt sigurnosti. Prema nalazima ekipe koja se nalazi iza inicijative World Backup Day (koji se obilježava 31. ožujka, www.worldbackupday.com), 30 posto korisnika nikada nije napravilo backup.

Svi su „slučajna“ meta

Relativno nedavni slučaj s novinarom portala Wired Mat Honan-om pokazuje rizike neodgovornog ponašanja. 2012. godine, „unutar jednog sata, sav [njegov] digitalni život je uništen”. Njegov slučaj ne otkriva samo nedostatke u njegovom odnosu prema sigurnosti, već i u čitavom tehnološkom ekosistemu.

Vrijedi istaknuti neke zanimljive činjenice u vezi s njegovim slučajem. G. Honan je iskusan novinar koji se bavi temom visokih tehnologija. Iako nije savršen, njegov pristup online sigurnosti je vjerojatno bolji nego u slučaju prosječnog korisnika. Pored toga, razlog napada na g. Honana nema veze s bilo kakvim privatnim sukobom ili ostvarenjem financijske koristi. Zapravo, njegov slučaj čak niti ne spada pod temu ransomeware-a, pošto su hakeri koji su preoteli njegove e-mail račune i profile na društvenim mrežama to učinili samo da bi „gledali kako stvari gore". Kao što mu je jedan od napadača rekao: „Zaista nisam osjećao nikakvu mržnju prema tebi prije ovoga. Jednostavno mi se svidjela tvoja lozinka…"

Glavni zaključak: izradite kopiju vaših podataka

Između ostalog, jedna od glavnih poruka ovog slučaja je neosporna važnost izrade backup-a. Kao što je Honan istaknuo u članku napisanom nakon proživljenog iskustva, u kojem je izložio koliko ga je napora i novaca koštao povratak dijela njegovog digitalnog života, backup za njega danas predstavlja dio životne filozofije: "Kada kontrolirate svoje podatke na lokalnoj razini i spremate ih na zaseban medij, nitko vam ih ne može oduzeti. Barem ne trajno. Danas imam lokalno i online backup rješenje i spremam se uvesti dodatno backup rješenje na izdvojenoj lokaciji. To znači da ću imati četiri kopije svih podataka koje smatram vrijednima. Pretjerivanje? Vjerojatno. Ali jednom sam se opekao." Većina profesionalaca u području informatičke sigurnosti bi se složila s g. Honanom. Niti jedno rješenje za backup nije 100% pouzdano, što znači da vrijedi pratiti primjer novinara i redovno održavati nekoliko kopija vrijednih podataka.

Detaljne upute za zaštitu od gubitka podataka koje je 2011. godine sastavio ESET-ov stručnjak Aryeh Goretsky još uvijek mogu poslužiti kao dobar vodič za backup. Video „Što je ransomware i kako se zaštititi" je dostupan na sljedećem linku: http://www.welivesecurity.com/videos/what-is-ransomware-and-how-can-i-protect-myself/

Novi Trojan virus koji se širi putem USB-a u stanju izbjeći detekciju

Članak preuzet s portala www.welivesecurity.com
Autor: Tomaš Gardon, analitičar ESET-a

Na USB uređajima je nedavno otkriven jedinstveni Trojan virus koji krade podatke i razlikuje se od tipičnih malicioznih kodova s istom namjenom. Svi tipovi ovog virusa se oslanjaju na USB uređaj na kojem se nalaze i ne ostavljaju tragove na kompromitiranom računalu. Štoviše, virus koristi poseban mehanizam kako bi se zaštitio od kopiranja, što ga čini još težim za otkrivanje.

Dok drugi maliciozni kodovi za pokretanje koriste dobre stare načine kao što su Autorun datoteke, ovaj novi USB maliciozni kod koristi još jedan način. Ova metoda se oslanja na sve češću praksu spremanja prijenosnih verzija popularnih aplikacija kao što su Firefox, NotePad++ ili TrueCrypt na USB nosačima. Maliciozni kod koristi ovu praksu tako što se ubacuje u lanac izvršnih programa tih aplikacija u obliku plugin-a ili DLL-a. Sukladno tome, pri svakom pokretanju neke od navedenih aplikacija, u pozadini se pokreće i maliciozni kod. Međutim, ono što čini ovaj maliciozni kod posebnim je njegov mehanizam zaštite.

Virus se sastoji od šest datoteka. Četiri datoteke su izvršne, dok preostale dvije sadrže podatke za konfiguraciju. Kako bi se zaštitio od kopiranja ili obratnog inženjeringa, virus koristi dvije tehnike: prvo, neke od datoteka su zaštićene AES128 enkripcijom; drugo, njihovi nazivi se stvaraju od kriptiranih elemenata. Pošto je ključ enkripcije sastavljen u ovisnosti od ID broja USB uređaja, virus je moguće pokrenuti samo s tog uređaja. Ova povezanost s USB uređajem, kao i sofisticirana višeslojna enkripcija koja je također povezana s pojedinim USB uređajem, čini ovaj virus vrlo otpornim na detekciju i analizu

(pošto ga je nemoguće odvojiti od USB uređaja, nije moguće poslati njegov „uzorak“ na analizu putem interneta). Drugim riječima, ovaj virus može obaviti krađu podataka s računala putem USB-a bez da bude primijećen.

ESET-ov analitičar Tomaš Gardon kaže kako je ovaj virus očigledno napravljen radi provođenja ciljanih napada te kako je unatoč teškoj detekciji rizik od sličnih virusa moguće smanjiti isključivanjem USB port-ova koji nisu nužni te edukacijom zaposlenika kako bi bili u stanju prepoznati rizične USB uređaje.

ESET alati za IT sigurnost

NORT je ekskluzivni distributer proizvoda tvrtke ESET u Hrvatskoj, Bosni i Hercegovini, Srbiji, Crnoj Gori, Makedoniji, Kosovu i Albaniji

www.nod32.com.hr
nod32@nort.hr
Tel: +385 1 3691 986
Fax: +385 1 3691 987