CARNET

Analiza WannaCry *ransomwarea*

NCERT-PUBDOC-2018-1-354

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

12. svibnja 2017. godine preko 75.000 računala diljem svijeta zaražena su *ransomwareom* – vrstom zlonamjernog softvera (eng. *malware*) koja šifrira datoteke na žrtvinom računalu te traži otkupninu za njihovo dešifriranje. Pogođeni su između ostaloga:

- *National Health Service* – sustav javnog zdravstva u Ujedinjenom Kraljevstvu (uključujući bolnice),
- *Deutche Bahn* – tvrtka koja upravlja željezničkom infrastrukturom u Njemačkoj,
- *Telefónica* – multinacionalni pružatelj telekomunikacijskih usluga,
- *FedEx* – multinacionalna tvrtka koja pruža usluge dostave,
- Ministarstvo unutarnjih poslova Ruske Federacije

i još brojni drugi. Zbog napada je u navedenim organizacijama bio otežan rad. Primjerice u nekim bolnicama u Ujedinjenom Kraljevstvu su i otkazivane operacije. Slika 1 prikazuje poruku sa zahtjevom za otkupninu na ekranu na glavnom željezničkom kolodvoru u njemačkom gradu Chemnitzu. Napad se nastavio i nakon 12. svibnja te je u konačnici bilo oko 200.000 žrtva u preko 150 zemalja (1).

Slika 1 – poruka sa zahtjevom za otkupninu na ekranu na glavnom željezničkom kolodvoru u njemačkom gradu Chemnitzu (izvor)

Napad je prouzročio zlonamjerni softver poznat pod nazivom **WannaCry** (poznat još i kao: WanaCrypt0r, WanaDecrypt0r, WCry itd.).

1.1 Kratka povijest WannaCrya

Ime WannCry zapravo se odnosi na cijelu „obitelj" zlonamjernog softvera (eng. *malware family*). Drugim riječima, ono obuhvaća više različitih inačica istog zlonamjernog softvera.

To je značajno zbog toga što napad u svibnju 2017. zapravo nije bio prvi napad WannaCrya, već samo najveći. Ranije inačice viđene su još u veljači i ožujku 2017. te su kasnije prozvane **WannaCry 1.0**. Slika 2 prikazuje poruku sa zahtjevom za otkupninu iz WannaCry inačice 1.0 viđene u veljači 2017.

Slika 2 – poruku sa zahtjevom za otkupninu iz WannaCry inačice 1.0 viđene u veljači 2017. (izvor)

Prije svibnja 2017., WannaCry bio je prilično nepoznat. U usporedbi s drugim *ransomwareom*, inačica 1.0 nije bila niti posebna, niti široko raširena. Nakon toga, u inačicu 2.0 autori WannaCrya dodaju mogućnost **automatskog širenja zaraze** na druga računala. Drugim riječima, u novoj inačici WannaCry poprima karakteristike računalnog crva (eng. *computer worm*).

12. svibanja 2017. oko 8 ujutro (UTC) pojavljuju se prve zaraze novom inačicom WannaCrya. Nova inačica izrazito se brzo širila – do kraja dana zaraženo je najmanje 75.000 računala.

2 Pozadina napada

Prema riječima Europola, veličina WannaCry napada u svibnju 2017. godine bila je bez presedana (2). Postavljaju se pitanja:

- Tko stoji iza napada?
- Kako se zaraza tako brzo proširila?
- Koji su motivi napadača?

Naredna poglavlja pokazat će koliko je pozadina ovog napada zapravo bila složena.

2.1 Equation grupa, Shadow Brokers

Kako bi bilo moguće razumjeti pozadinu WannaCry napada, prvo je potrebno upoznati se s grupama zvanima *Equation* i *Shadow Brokers*.

National Security Agency (NSA) jedna je od obavještajnih agencija SAD-a zaduženih za nacionalnu sigurnost. *Office of Tailored Access Operations* (TAO) je navodni tajni dio NSA-a koji aktivno napada računalne sustave i mreže te na taj način prikuplja informacije (3) (4). **Equation grupa** kodno je ime za naprednu „hakersku" grupu koju sigurnosni stručnjaci povezuju upravo s agencijom NSA odnosno s TAO-om (5) (6) (7).

Shadow Brokers grupa je nepoznatog sastava koja se prvi put pojavila u javnosti objavom u kolovozu 2016. godine. Tada su objavili da su ukrali kibernetička oružja (alate za kompromitaciju računala) od Equation grupe te da otvaraju aukciju za njihovu prodaju. Slika 3 prikazuje početni dio te objave.

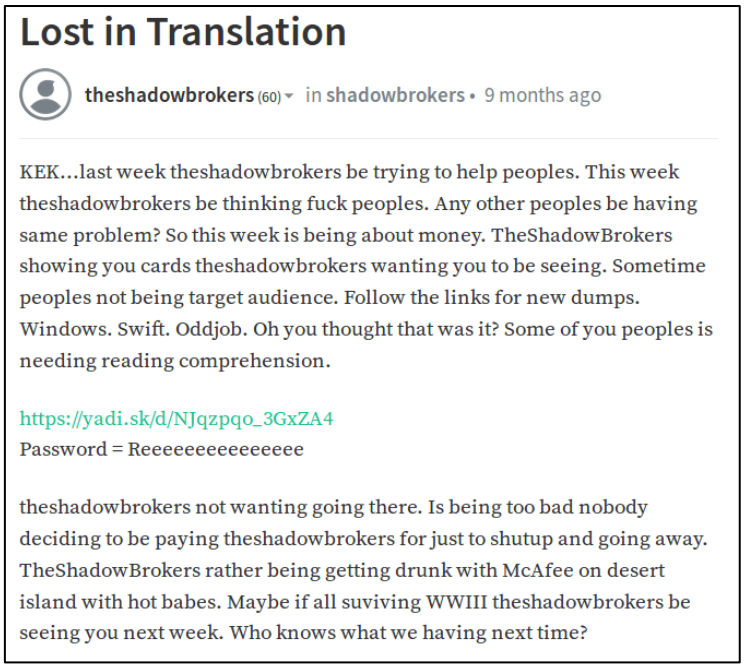
```
Equation Group Cyber Weapons Auction - Invitation
- ------------------------------------------------


!!! Attention government sponsors of cyber warfare and those who profit from it !!!!

How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? We
find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find
Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you
some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You
write many words. But not all, we are auction the best files.
```

Slika 3 – Početni dio objave Shadow Brokers grupe iz kolovoza 2016. (izvor)

Kroz još nekoliko objava u narednih pola godine pokušavaju prodati ukradeno, no naizgled bez puno uspjeha. Zatim, 14. travnja 2017. **javno objavljuju** niz ukradenih kibernetičkih oružja. U tom trenutku napredni, moćni alati za kompromitaciju računala postaju **dostupni svima**. Na slici 4 prikazana je ta objava.



Lost in Translation

theshadowbrokers (60) in shadowbrokers • 9 months ago

KEK...last week theshadowbrokers be trying to help peoples. This week theshadowbrokers be thinking fuck peoples. Any other peoples be having same problem? So this week is being about money. TheShadowBrokers showing you cards theshadowbrokers wanting you to be seeing. Sometime peoples not being target audience. Follow the links for new dumps. Windows. Swift. Oddjob. Oh you thought that was it? Some of you peoples is needing reading comprehension.

https://yadi.sk/d/NJqzpqo_3GxZA4
Password = Reeeeeeeeeeeeee

theshadowbrokers not wanting going there. Is being too bad nobody deciding to be paying theshadowbrokers for just to shutup and going away. TheShadowBrokers rather being getting drunk with McAfee on desert island with hot babes. Maybe if all suviving WWIII theshadowbrokers be seeing you next week. Who knows what we having next time?

Slika 4 – objava grupe Shadow Brokers iz 14. travnja 2017. (izvor)

U CNN-ovom članku o ovom događaju, Matthew Hickey, osnivač sigurnosne tvrtke Hacker House, rekao je „Ovo je vjerojatno najopasnija stvar koju sam vidio u zadnjih nekoliko godina. Ovo stavlja snažan alat za napadanje u ruke bilo koga tko ga želi preuzeti i započeti napadati poslužitelje.“ (8)

Od objavljenih alata, u kontekstu ovog dokumenta, posebno su značajni alati s kodnim imenom EternalBlue i DoublePulsar.

2.2 EternalBlue i DoublePulsar

EternalBlue, jedan od objavljenih alata, služi za preuzimanje kontrole nad računalom (eng. *exploit*). On omogućava napadaču udaljeno (mrežno) preuzimanje kontrole nad računalima s operacijskim sustavom Windows iskorištavanjem ranjivosti u implementaciji SMB protokola.

EternalBlue izrazito je opasan iz nekoliko razloga:

- Moguće je **napasti** računala udaljeno, **preko mreže** (eng. *remote*). To ne znači da je moguće napasti računala samo na lokalnoj mreži (primjerice unutar organizacije), već i preko Interneta ako SMB priključak nije zaštićen vatrozidom.

- Za iskorištavanje ranjivosti **nije potrebno znati nikakvo korisničko ime niti lozinku** (eng. *unauthenticated*).

- Ranjivost se nalazi u jezgri (eng. *kernel*) operacijskog sustava. Posljedica toga je da se prilikom iskorištavanja ranjivosti napadačev kod izvršava s najvišim privilegijama, u tzv. nultom prstenu (eng. *ring 0*). Drugim riječima, pomoću EternalBluea moguće je preuzeti **potpunu kontrolu** nad računalom.

- Ranjivost je **prisutna u Windows instalacijama s početnim postavkama** (eng. *default*).

14. ožujka 2017., mjesec dana **prije** javne objave Shadow Brokers grupe (koja je sadržavala EternalBlue), Microsoft objavljuje sigurnosnu nadogradnju MS17-010. Ona sadrži niz sigurnosnih zakrpa, između ostaloga i zakrpu za ranjivost koju EternalBlue iskorištava (CVE-2017-0144). To znači da su već **mjesec dana prije objave EternalBluea, ažurirana računala zaštićena od njegovog pokušaja napada**. No mnoga računala **nisu** redovito ažurirana, zbog čega je čak i danas, deset mjeseci nakon sigurnosne zakrpe, EternalBlue opasan.

Još jedan objavljeni alat značajan u kontekstu ovog dokumenta je **DoublePulsar**. DoublePulsar su tzv. „tajna vrata" za prikriveno kontroliranje računala (eng. *backdoor*). Drugim riječima, DoublePulsar je alat koji osigurava da napadač ostane prikriven nakon što preuzme kontrolu nad računalom.

Između ostaloga, DoublePulsar moguće je ugraditi u kompromitirano računalo pomoću EternalBluea. Jednom kada je ugrađen, skriva se u jezgri operacijskog sustava (eng. *kernel*) zbog čega je izrazito teško primijetiti napad.

12. svibnja 2017., mjesec dana nakon što je grupa Shadow Broker javno objavila alate, pojavljuju se prve zaraze WannaCry inačice 2.0 **s mogućnošću automatskog širenja mrežom pomoću EternalBluea i DoublePulsara**. Upravo pomoću njih se WannaCry 2.0 tako brzo i destruktivno proširio.

Žrtve WannaCrya 2.0 su računala koja nisu ažurirana sigurnosnom nadogradnjom MS17-010. Iako je nadogradnja objavljena dva mjeseca prije napada, **brojna računala nisu bila ažurirana te je šteta bila ogromna**.

Operacijski sustav **Windows XP** i ranije inačice Windows operacijskih sustava više uopće nisu bili podržani niti su postojale ikakve sigurnosne nadogradnje za njih. No i dalje, **brojna računala s važnim funkcijama (primjerice računala u bolnicama) su koristila uprave te zastarjele i nesigurne operacijske sustave** pa su zbog toga bila i ranjiva. Dan nakon napada, Microsoft je iznimno izdao i sigurnosnu nadogradnju za zaštitu operacijskog sustava Windows XP od EternalBluea, no za mnoge organizacije to je bilo prekasno.

3 Kako WannaCry radi?

Distribucija i zaraza WannaCry 2.0 *ransomwarea* odvija se u dvije faze:

1. „Crv" (eng. *worm*) – zadužen za **automatsko širenje mrežom** (lokalno i globalno)
2. *Ransomware* – zadužen za **šifriranje datoteka na zaraženom računalu**

Zbog takvih karakteristika dvije klase zlonamjernog softvera, WannaCry znaju klasificirati kao kriptocrv (eng. *cryptoworm*).

3.1 Automatsko širenje mrežom

Onaj dio po kojemu se WannaCry razlikuje od većine ostalog *ransomwarea* i zlonamjernog softvera je upravo automatsko širenje mrežom. Mehanizam širenja WannaCrya moguće je raščlaniti na sljedeći način:

1. **Širenje pomoću EternalBluea**

   Glavni mehanizam širenja WannaCrya je EternalBlue – javno objavljeno kibernetičko oružje ukradeno Equation grupi. Nakon uspješnog napada EternalBlueom, WannaCry na računalo ugrađuje DoublePulsar te preko njega pokreće svoje ostale dijelove. WannaCry se pomoću EternalBluea širi:

   a) **Lokalnom mrežom**

      Širenjem unutar lokalne mreže u pravilu se postiže zaraza računala unutar iste organizacije, primjerice bolnice. Unutar lokalne mreže, širenje je izrazito efektivno jer lokalni promet zbog implicitnog povjerenja najčešće ne prolazi kroz vatrozide i slična sigurnosna rješenja.

   b) **Internetom**

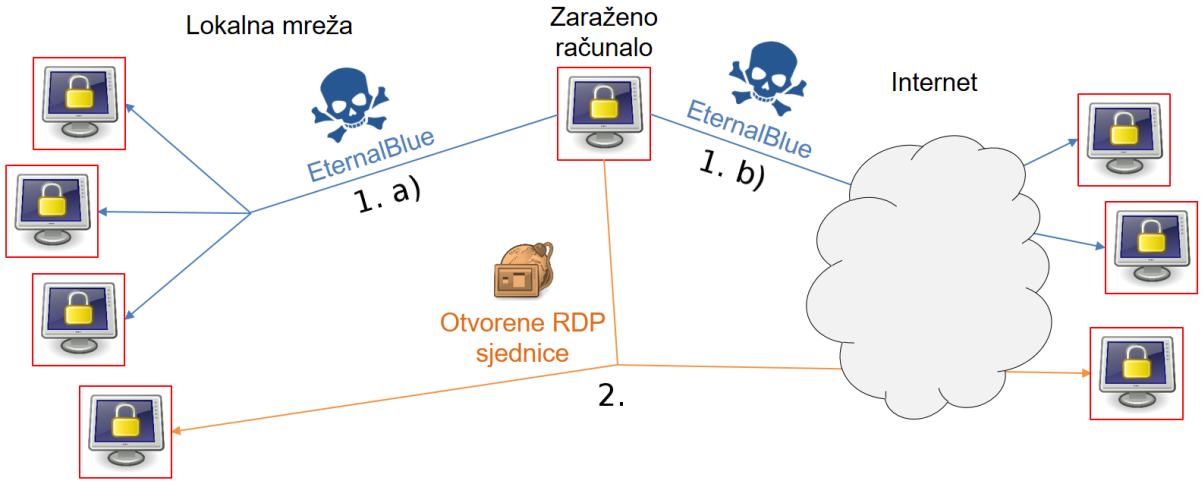
      Uz širenje lokalnom mrežom, WannaCry odabire nasumična računala na Internetu te se pokušava proširiti na njih. Na ovaj način postiže se širenje zaraze i izvan digitalnih zidova organizacija, no za razliku od širenja unutar lokalne mreže, u ovom će slučaju WannaCry češće naići na vatrozide i ostale sigurnosne prepreke te će u konačnici zaraza rjeđe biti uspješna.

2. **Širenje kroz otvorene RDP sjednice**

   Iako je za glavni dio širenja WannaCrya odgovoran EternalBlue, WannCry se širi još i kroz otvorene RDP (eng. *Remote Desktop Protocol*) sjednice. Primjerice, ako WannaCry zarazi računalo sistemskog administratora koji u tom trenutku upravlja nekim udaljenim računalima preko RDP protokola, WannaCry će se proširiti i na njih. Razumljivo, ovaj dio je u gotovo svim analizama u manjem fokusu, no bitno je spomenuti kako WannaCry ima i ovu mogućnost.

Dijagram na slici 5 prikazuje kako se WannaCry širi s jednog na drugo računalo. Sukladno prethodnom tekstu, *1. a)* na dijagramu prikazuje širenje lokalnom mrežom pomoću

EternalBluea, *1. b)* prikazuje širenje Internetom pomoću EternalBluea i *2.* prikazuje širenje kroz otvorene RDP sjednice.



Slika 5 – dijagram koji vizualno prikazuje kako se WannaCry širi s jednog na drugo računalo.

Uz navedeno, iako bi to trebalo biti izrazito rijetko, WannaCry se može proširiti i na računalo koje nije ranjivo na EternalBlue, ali mu je već prethodno, na neki drugi način, ugrađen DoublePulsar.

3.2 Prve zaraze

Prethodno poglavlje odgovara na pitanje kako se WannaCry širi sa zaraženog računala na druga računala, no to i dalje ne odgovara na pitanje: „Kako su prva računala bila zaražena?“ Odgovor na to pitanje i dalje nije poznat, za sada postoje samo hipoteze.

Intuitivan, glavni sumnjivac za prve zaraze bio bi **EternalBlue** – ako se pomoću njega WannaCry širi, zašto on ne bi bio odgovoran i za početnu zarazu? EternalBlue je izrazito efektivan unutar lokalne mreže te nema sumnje kako je odgovoran za širenje WannaCrya unutar organizacija. **No djelotvornost EternalBluea je upitna kada se radi o udaljenim računalima na Internetu.** Kako bi napad WannaCryom bio uspješan, SMB priključak računala mora biti dostupan, a to je rijeđe slučaj na Internetu gdje je takav dolazni promet obično zaustavljen vatrozidom. EternalBlue svakako može objasniti jedan dio globalne zaraze, no pitanje je je li on zaista samostalno odgovoran za tako široki doseg WannaCrya.

Druga hipoteza o početnoj zarazi uključuje **DoublePulsar**. Konkretnije, zaraza WannaCryem možda je započela s računalima koja su nekako prethodno bila zaražena te im je bio ugrađen DoublePulsar. Tu hipotezu podržavaju podaci sigurnosne tvrtke Fortinet. U često postavljenim pitanjima o WannaCryu na Fortinet-ovom blogu piše kako je Fortinet „detektirao oko 6.000 pokušaja iskorištavanja ili ispitivanja DoublePulsar tajnih vrata 27. travnja. te 16.000 pokušaja 28. travnja“ (9). Piše i kako se čini da je „DoublePulsar skrovito distribuiran tjednima [ranije] te da je onda korišten kao glavni vektor napada za WannaCry jer su deseci tisuća strojeva već čekali s otvorenim tajnim vratima“ (9).

Još jedna hipoteza je da je WananCry inicijalno raširen ***phishing* napadima**. Ova hipoteza podržana je time što su *phishing* napadi danas uobičajeni način zaraze *ransomwareom* i drugim zlonamjernim softverom. No izvan toga, nema nikakvih konkretnih tragova koji bi upućivali na *phishing* kao inicijalni vektor zaraze WannaCrya.

3.3 Prekidač za gašenje (eng. *kill switch*)

Uz automatsko širenje, WannaCry sadrži još jedan zanimljivi mehanizam. Prilikom pokretanja, prije nego išta drugo učini, WannaCry obavlja jednu provjeru:

1. **Pokuša kontaktirati** Web stranicu na domeni *www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com,*

2. Ako uspije, **zaustavlja se**. Ne širi se dalje niti šifrira podatke na računalu!

Upravo zbog toga, ovaj mehanizam prozvan je „prekidačem" za gašenje (eng. *kill switch*). Postavlja se pitanje: „Zašto su autori ugradili takav mehanizam za zaustavljanje zaraze?"

Za razumijevanje potencijalnih objašnjenja, potrebno je pozadinsko znanje o **tehnikama otkrivanja zlonamjernog softvera**. Brojni alati za otkrivanje zlonamjernog softvera, softver koji ispituju/analiziraju pokreću unutar izolirane okoline (eng. *sandbox*). Zatim, na temelju ponašanja softvera unutar te okoline, procjenjuju je li on zlonamjeran ili nije.

Takve okoline u pravilu nisu spojene na pravu mrežu, kako zlonamjerni softver unutar njih ne bi mogao napraviti štetu drugim računalima na mreži. Umjesto toga, okolina je spojena na „lažni" Internet. Unutar njega, često su **sve domene i Web stranice prividno dostupne** – čak i one koje ne postoje na stvarnoj mreži. One su prividno dostupne kako bi alati mogli vidjeti što analizirani softver pokušava poslati mrežom te iskoristiti i tu informaciju za analizu.

Vjerojatno objašnjenje „prekidača" za gašenje je sljedeće – kontaktiranjem domene koja ne postoji na stvarnom Internetu, **WannaCry pokušava saznati je li pokrenut unutar izolirane okoline**. Izvan izolirane okoline kontaktiranje će biti neuspješno jer domena ne postoji, no unutar izolirane okoline, ono bi trebalo biti uspješno upravo zbog navedenog „lažnog" Interneta. Ako smatra da se nalazi unutar izolirane okoline, WannaCry se zaustavlja kako navedeni alati **ne bi otkrili da se radi o zlonamjernom softveru**. Općenito, kod zlonamjernog softvera uobičajene su slične tehnike za zaobilaženje detekcije u izoliranim okolinama (eng. *anti-sandbox techniques*).

No taj pristup ima i manu iz perspektive autora WannaCrya. Čim netko analizira WannaCry i otkrije taj mehanizam, može registrirati tu, do sada nepostojeću, domenu i na taj način **zaustaviti daljnje zaraze**. Upravo to je i učinjeno – istog dana kada je zaraza započela, domena je registrirana i daljnja zaraza je bila zaustavljena. No i dalje, ukupna šteta bila je ogromna.

3.4 Šifriranje datoteka na računalu

Ransomware dio WannaCrya zapravo je uobičajen – nije značajno drugačiji od drugih *ransomwarea* i zlonamjernog softvera općenito.

WananCry pretražuje datoteke na diskovima računala te šifrira one s određenim nastavcima. U popisu ima preko 100 nastavaka (*.docx, .pptx, .jpeg, .png, .zip*…) koje šifrira, a koji bi trebali pokriti datoteke koje su značajne žrtvi, tj. za koje bi žrtva platila otkupninu. Međutim, datoteke s nastavcima kao što su *.dll* i *.exe* neće biti šifrirane kako bi računalo i dalje radilo nakon postupka šifriranja.

Prije šifriranja, WannaCry gasi određene programe, konkretnije Microsoft Exchange i Microsoft SQL Server, kako bi mogao šifrirati i njihove datoteke.

Uz šifriranje, *ransomware* komponenta WannaCry briše sigurnosne kopije datoteka (eng. *shadow copies*) kako ih žrtve ne bi mogle lako vratiti bez plaćanja otkupnine.

3.5 Poruka

Kada je gotov sa šifriranjem datoteka, WannaCry prikazuje poruku sa zahtjevom za otkupninu (eng. *ransom note*). Poruka ukratko objašnjava što se dogodilo računalu te traži novac u zamjenu za dešifriranje datoteka. Slika 6 prikazuje WannaCry poruku sa zahtjevom za otkupninu na engleskom jeziku.

Slika 6 – WannaCry poruka sa zahtjevom za otkupninu na engleskom jeziku

Poruka je prevedena na 28 jezika, uključujući hrvatski. Analitičari tvrtke Flashpoint proveli su lingvističku analizu prijevoda poruke te su utvrdili da, uz iznimku engleske i kineskih inačica, poruke su vrlo vjerojatno prevedene pomoću usluge *Google Translate* (10). Na temelju te činjenice i analize engleske i kineskih inačica poruke, zaključuju s

visokom vjerojatnošću da autor poruke tečno govori kineski te da ima znanje engleskog jezika, ali da mu on nije materinji (10).

Po pitanju otkupnine, napadači za dešifriranje datoteka traže $300 u Bitcoin-ima. Korištenje Bitcoin-a uobičajeno je za *ransomware* i druge kriminalne aktivnosti na Internetu zbog više razine anonimnosti u usporedbi s konvencionalnim metodama razmjene novca. Ako žrtva ne plati unutar tri dana, napadači udvostručuju otkupninu na $600 te konačno, ako žrtva i nakon sedam dana ne plati, podaci su navodno zauvijek izgubljeni.

3.6 Ostale tehnike

Kako bi podaci (nakon plaćanja otkupnine) bili dešifrirani, napadači moraju nekako žrtvi predati ključ za dešifriranje. Neki oblik komunikacije s napadačevim poslužiteljima je zato nužan. U slučaju WannaCrya, a i brojnog drugog zlonamjernog softvera, ta komunikacija odvija se preko Tor mreže anonimnosti. Konkretnije, komunikacija se odvija **preko Tor skrivenih servisa** (eng. *hidden service* ili *onion service*).

WannaCry koristi još brojne uobičajene tehnike zlonamjernog softvera:

- Mehanizmi trajnosti (eng. *persistence mechanisms*)
    - WannaCry stvara Windows servise i *registry* ključeve kako bi se automatski pokrenuo prilikom pokretanja računala.
    - Na taj način WannaCry „preživljava” ponovno pokretanje (eng. *reboot* ili *restart*) računala.
- Mehanizam međusobnog isključivanja (eng. *mutex*)
    - WannaCry stvara *mutex* kako se ne bi pokrenulo više WannaCry procesa na istom računalu. Više istih procesa bi si potencijalno smetalo te bi bilo lakše za otkriti, bez ikakvog pozitivnog učinka iz perspektive autora zlonamjernog softvera.
- Datotekama, servisima i *mutex*-ima daje nazive koji nisu sumnjivi
    - Primjerice „mssecsvc.exe” i „tasksche.exe” za datoteke te „MsWinZonesCacheCounterMutexA” za *mutex*.

4 Identitet i motiv napadača

Točan identitet napadača, tj. autora WannaCrya, je nepoznat, no sigurnosna tvrtka Symantec tvrdi kako postoje snažne poveznice između WannaCry napada i tzv. **Lazarus grupe** (11). Kao potporu toj izjavi, Symantec navodi tragove koji između ostaloga uključuju (11):

1. Zlonamjerni softver prethodno povezan s Lazarus grupom pronađen na računalima koja su inficirana ranim inačicama WannaCrya u veljači 2017.

2. Zlonamjerni softver Alphanc koji je širio WannaCry u ožujku i travnju 2017. modificirana je inačica zlonamjernog softvera Duuzer koji je prethodno povezan s Lazarus grupom.

3. Zajednički kod WannaCrya i zlonamjernog softvera Contopee koji je prethodno povezan s Lazarus grupom.

Lazarus je napredna „hakerska" grupa koja je između ostaloga povezana s velikim napadom na *Sony Pictures Entertainment* s kraja 2014. godine te s krađom 80 milijuna dolara iz Centralne Banke Bangladeša s početka 2016. **Lazarus grupa često se povezuje sa Sjevernom Korejom, no konkretni tragovi su i dalje rijetki** (12) (13)**.**

Motiv napada nije moguće precizno utvrditi, no moguće je postaviti hipoteze na temelju poznatih činjenica. Lazarus grupa povezuje se s brojnim **financijskim napadima** (13). Na temelju svojih analiza, sigurnosni stručnjaci iz tvrtke Kaspersky vjeruju da postoji cijela podgrupa Lazarusa koja je odgovorna za financijske zločine (14). Podgrupu su prozvali **BlueNoroff,** a njen cilj mogao bi biti osiguravanje financijskih sredstva za rad Lazarus grupe (14). Kako je općenito cilj *ransmoware* (ilegalno) zaraditi novac za njegove autore, prethodno navedene činjenice podržavaju hipotezu da je WannaCry napad bio financijski motiviran.

5 Zaključak

WannaCry napad iz svibnja 2017. godine jedan je od najvećih *ransomware* napada do sad, ako ne i najveći. Europol navodi da je sveukupno bilo preko 200.000 žrtava u barem 150 zemalja (1).

Kao zaključak nakon napada, bitno je razumjeti sljedeće:

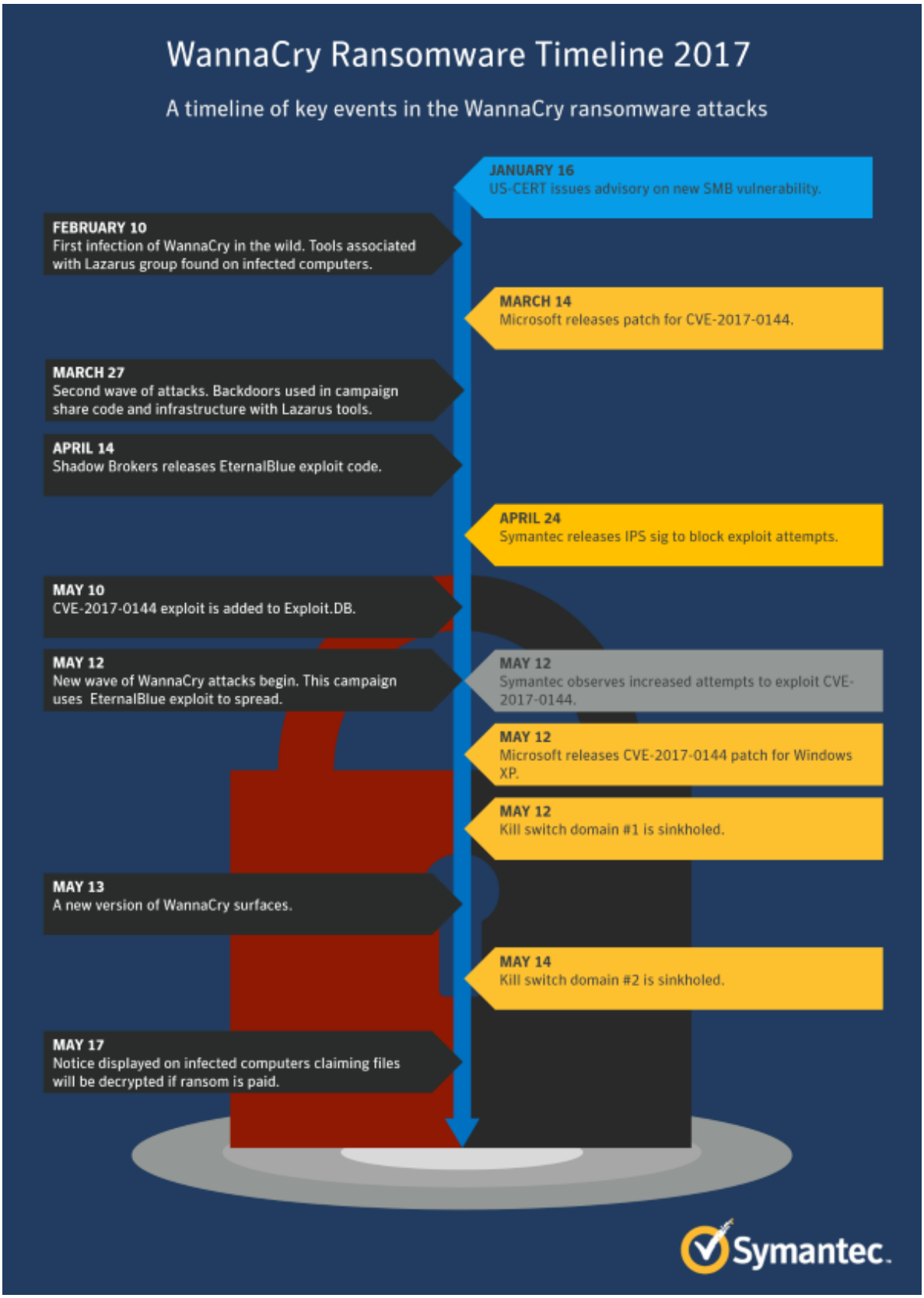
1. **Za sprječavanje zaraze bilo je dovoljno samo redovito ažurirati računalo**. No mnoga računala nisu bila ažurirana – štoviše, brojna računala još su bila na starim, nepodržanim te nesigurnim operacijskim sustavima kao što je Windows XP.

2. Čak i da su računala uspješno zaražena te njihovi podaci šifrirani, šteta ne će biti visoka ako su dostupne **sigurnosne kopije podataka**. Također, ključno je čuvati te sigurnosne kopije **odvojeno od računala čija se kopija radi**. U suprotnom, *ransomware* može šifrirati i sigurnosne kopije jednako lako kao što je šifrirao i izvorno računalo.

U konačnici, zbog toga je šteta bila ogromna.

Pozadina WannaCry napada bila je izrazito složena – od Shadow Brokers objave, preko „prekidača" za gašenje do pretpostavke sigurnosne tvrtke Symantec da je napad povezan s Lazarus grupom. Symantec je izradio vremensku crtu za pregled ključnih događaja pomoću koje je lakše shvatiti cijeli kontekst napada. Vremenska crta prikazana je na slici 7. Vremenska crta spominje i novije inačice WannaCrya i novije domene vezane za prekidač za gašenje, no općenito smatra se kako su te inačice samo manje varijacije koje su treće strane izmijenile te slučajno ili namjerno pustile u javnost.

Na kraju, čini se da među obavještajnim agencijama postoji praksa gomilanja ranjivosti umjesto njihovog prijavljivanja. I dalje ostaje otvoreno pitanje – štiti li to građane ili ih stavlja u opasnost?



Slika 7 – vremenska crta koju je izradio Symantec za pregled ključnih događaja oko WannaCry *ransomware* napada (izvor)

6 Literatura

1. **Thompson, Mark i Mullen, Jethro.** Ransomware: Attack hits 150 countries, Europol says world is in 'disaster recovery mode'. *CNN tech.* [Mrežno] 14. svibanj 2017. [Citirano: 26. siječanj 2018.] http://money.cnn.com/2017/05/14/technology/ransomware-attack-threat-escalating/.
2. **BBC News.** Cyber-attack 'unprecedented' in scale. [Mrežno] 13. svibanj 2017. [Citirano: 17. siječanj 2018.] http://www.bbc.com/news/world-europe-39907965.
3. **Aid, Matthew M.** Inside the NSA's Ultra-Secret China Hacking Group. *Foreign Policy.* [Mrežno] 10. lipanj 2013. [Citirano: 18. siječanj 2018.] https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/.
4. **Shane, Scott, Perlroth, Nicole i Sanger, David E.** Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. *The New York Times.* [Mrežno] 12. studeni 2017. [Citirano: 26. siječanj 2018.] https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html?_r=0.
5. **Fox-Brewster, Thomas.** Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'. *Forbes.* [Mrežno] 16. veljača 2015. [Citirano: 18. siječanj 2018.] https://www.forbes.com/sites/thomasbrewster/2015/02/16/nsa-equation-cyber-tool-treasure-chest/#7f7861d7417f.
6. **Goodin, Dan.** How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last. *Ars Technica.* [Mrežno] 16. veljača 2015. [Citirano: 26. siječanj 2018.] https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/.
7. **Krebs, Brian.** Who Was the NSA Contractor Arrested for Leaking the 'Shadow Brokers' Hacking Tools? *Krebs on Security.* [Mrežno] 27. studeni 2017. [Citirano: 18. siječanj 2018.] https://web.archive.org/web/20171128050107/https://krebsonsecurity.com/2017/11/who-was-the-nsa-contractor-arrested-for-leaking-the-shadow-brokers-hacking-tools/.
8. **Larson, Selena.** NSA's powerful Windows hacking tools leaked online. *CNN tech.* [Mrežno] 15. travanj 2017. [Citirano: 18. siječanj 2018.] http://money.cnn.com/2017/04/14/technology/windows-exploits-shadow-brokers/index.html.
9. **Biddle, Susan.** WannaCry FAQ - Take-aways and Learnings. *Fortinet Blog.* [Mrežno] 17. svibanj 2017. [Citirano: 16. siječanj 2018.] https://blog.fortinet.com/2017/05/17/wannacry-faq.
10. **Flashpoint.** Linguistic Analysis of WannaCry Ransomware Suggests Chinese-Speaking Authors. [Mrežno] 25. svibanj 2017. [Citirano: 23. siječanj 2018.] https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/.
11. **Symantec.** WannaCry: Ransomware attacks show strong links to Lazarus group. [Mrežno] 22. svibanj 2017. [Citirano: 16. siječanj 2018.] https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group.
12. **Talmadge, Eric.** North Korea, cyberattacks and 'Lazarus': What we really know. *Phys.org.* [Mrežno] 2. lipanj 2017. [Citirano: 22. siječanj 2018.] https://phys.org/news/2017-06-north-korea-cyberattacks-lazarus.html.
13. **Kaspersky.** Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies. [Mrežno] 2017. [Citirano: 22. siječanj 2018.]

https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies.
14. —. Lazarus Under The Hood. *Securelist.* [Mrežno] 3. travanj 2017. [Citirano: 26. siječanj 2018.] https://securelist.com/lazarus-under-the-hood/77908/.
15. **MalwareTech.** How to Accidentally Stop a Global Cyber Attacks. [Mrežno] 13. svibanj 2017. [Citirano: 16. sijčanj 2018.] https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html.
16. **Symantec.** Ransom.Wannacry. [Mrežno] 24. svibanj 2017. [Citirano: 15. siječanj 2018.] https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99.
17. **Windows Security blog.** Exploring the crypt: Analysis of the WannaCrypt ransomware SMB exploit propagation. [Mrežno] 30. lipanj 2017. [Citirano: 16. siječanj 2018.] https://cloudblogs.microsoft.com/microsoftsecure/2017/06/30/exploring-the-crypt-analysis-of-the-wannacrypt-ransomware-smb-exploit-propagation/.