***Zbornik radova s***
***III. međunarodne znanstveno-stručne konferencije***
***„Nove sigurnosne ugroze i kritična nacionalna infrastruktura“***

***Nakladnik***
*Ministarstvo unutarnjih poslova Republike Htvatske*
*Policijska akademija*

***Za nakladnika***
*Želimir Radmilović*

***Urednik***
*doc. dr. sc. Krunoslav Antoliš*

***Recenzenti***
*doc. dr. sc. Krunoslav Antoliš, dr. sc. Damir Brnetić, prof. dr. sc. Ksenija Butorac, prof. dr. sc. Milan Daničić, prof. dr. sc. Josip Kasum, prof. dr. sc. Mirko Kulić, prof. dr. sc. Dario Matika, dr. sc. Ante Orlović, dr. sc. Goran Ribičić, prof. dr. sc. Branislav Simonović, prof. dr. sc. Zdravko Skakavac*

***Lektorice***
*Antonija Rakuljić, Slava Rosandić*

***Korektorica***
*Slava Rosandić*

***Priprema i tisak***
*Policijska akademija*
*Služba za razvoj policijskog obrazovanja i nakladničko-knjižničnu djelatnost*

***Naklada***
*500 primjeraka*

***ISBN*** *978-953-161-276-0*

***CIP*** *zapis dostupan u računalnome katalogu*
*Nacionalne i sveučilišne knjižnice u Zagrebu*
*pod brojem* ***853091***

**ZBORNIK RADOVA S**
**III. MEĐUNARODNE ZNANSTVENO-STRUČNE KONFERENCIJE**

# „Nove sigurnosne ugroze i kritična nacionalna infrastruktura“

Zagreb, 2013.

**„Nove sigurnosne ugroze i kritična nacionalna infrastruktura“**
**„New Threats and Critical National Infrastructure“**

***Pokrovitelj***

*Ranko Ostojić*

*potpresjednik Vlade Republike Hrvatske i ministar unutarnjih poslova Republike Hrvatske*

***Organizatori***

*Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija, Visoka policijska škola*

***Programski odbor*** *(prema abecednom redoslijedu)*

*doc. dr. sc. Krunoslav Antoliš – predsjednik (Hrvatska), prof. dr. sc. Milan Bajić (Hrvatska), prof. dr. sc. Katica Biljaković (Hrvatska), prof. dr. sc. Ksenija Butorac (Hrvatska), prof., dr. sc. Nika Chitadze, (Georgia), doc. dr. sc. Denis Čaleta (Slovenija), prof. dr. sc. Milan Daničić (BiH), dr. sc. Stjepan Gluščić (Hrvatska), dr. sc. Milivoj Jelenski (Hrvatska), prof. dr. sc. Josip Kasum (Hrvatska), prof. dr. sc. Zoran Keković (Srbija), prof. dr. sc. Hana Korać (BiH), doc. dr. sc. Atanas Kozarev (Makedonija), prof. dr. sc. Mirko Kulić (Srbija), prof. dr. sc. Dario Matika (Hrvatska), prof. dr. sc. Mile Matijević (BiH), doc. dr. sc. Marinko Ogorec (Hrvatska), dr. sc. Ante Orlović (Hrvatska), doc. dr. sc. Anita Perišin (Hrvatska), dr. sc. Jadran Perinić (Hrvatska), dr. sc. Goran Ribičić (Hrvatska), Professor, John R. Schindler, PhD (USA), prof. dr. sc. Zdravko Skakavac (Srbija), prof. dr. sc. Branislav Simonović (Srbija), doc. dr. sc. Mile Šikman (BiH), dr. sc. Joško Vukosav (Hrvatska), prof. dr. sc. Milan Žarković (Srbija)*

***Organizacijski odbor*** *(prema abecednom redoslijedu)*

*dr. sc. Damir Brnetić, Danijela Petković, mag. iur. - predsjednica, Nikša Jelovčić, prof., Dušanka Pribičević-Gelb, dipl. polit., Nikola Protrka, univ. spec. inf., mr. sc. Davor Solomun*

***Moderatori***

*doc. dr. sc. Krunoslav Antoliš, dr. sc. Milivoj Jelenski, dr. sc. Stjepan Gluščić, doc. dr. sc. Anita Perešin, dr. sc. Ante Orlović, Danijela Petković, mag. iur., dr. sc. Goran Ribičić*

**SADRŽAJ**

STRUČNI ČLANAK
UDK 351.759:681.3

NIKOLA PROTRKA, TONIMIR KIŠASONDI

# Pregled metoda kibernetičkih napada na kritičnu nacionalnu infrastrukturu Studije slučaja iz prakse

## *Overview of methods and cyber attacks on critical national infrastructure, case studies*

***Sažetak***

*Napretkom tehnologije pojavljuje se trend povećanja korištenja sve sofisticiranijih napada na kritičnu nacionalnu infrastrukturu uz pomoć metoda koje uključuju napade visoke složenosti usmjerene protiv računalno-mrežne infrastrukture, koja je oslonac rada te kritične infrastrukture. U radu je opisano nekoliko slučaja iz prakse, a koji se odnose na napade usmjerene ka kritičnoj nacionalnoj infrastrukturi, načine izvršenja tih napada (modus operandi) i opis skupina koje su bile umiješane u navedene napade. Sve navedeno prikazuje nove mogućnosti ratovanja i uništavanja kritične nacionalne infrastrukture, a da ti ratnici niti ne izađu iz svog ureda koji je tisućama kilometara udaljen od mete napada. Umjesto zaključka bit će opisano par preporuka za poboljšanje stanja kritične nacionalne infrastrukture i strategijski pregled kako spriječiti takve napade.*

***Ključne riječi:*** *kibernetički kriminal, kritična nacionalna infrastruktura, zaštita nacionalnih resursa, kibernetički terorizam, računalna špijunaža.*

***Summary***

*With the advancement of technology there is the growing trend of using increasingly sophisticated attacks on critical national infrastructure using methods that include attacks directed against the high complexity of computing and network infrastructure, which is the backbone of the critical infrastructure. The paper describes several case studies, which are related to attacks aimed at critical national infrastructure, the execution of these attacks (modus operandi) and the description of the groups that were involved in these attacks. All of the above shows the new features of warfare and destruction of critical national infrastructure, and the warriors do not even leave their offices, which are thousands of kilometers away from the targets. Instead of a conclusion, a couple of recommendations for the improvement of critical national infrastructure and strategic overview of how to prevent such attacks will be described.*

***Key words:*** *cybercrime, critical national infrastructure, protection of national resources, cyberterrorism, computer espionage.*

## 1. Uvod

Kibernetički napadi postali su svakodnevnica, te se gotovo na dnevnoj bazi može čuti u raznim informativnim emisijama i pročitati na internet portalima o napadima na web stranice, napadima na korisničke profile na društvenim mrežama, krađu osobnih podataka, krađu intelektualnog vlasništva itd. Svi ovi slučajevi nerijetko se vežu kako uz tvrtke tako i uz pojedince. Ali što je s napadima na kritičnu nacionalnu infrastrukturu (u daljnjem tekstu KNI), odnosno sve ono što ta infrastruktura obuhvaća. O toj temi nema baš puno domaće ili strane literature. U interesu državnih službi, ali i velikih kompanija je da takve napade sakriju od javnosti kako bi građani zadržali povjerenje, bilo da se radi o poslovnom odnosu ili građanskoj lojalnosti.

Ako govorimo o kibernetičkim napadima na KNI moramo odmah razjasniti da takav napad dolazi s javnog interneta i bez ekspertnog tehničkog znanja stručnjaka ne možemo niti sa sigurnošću utvrditi tko stoji iza napada. Napadaču je svejedno koliko je udaljen od svoje mete, dok god ima dobro oružje, a u ovom slučaju internetsku mrežu i alate. Ne smijemo zanemariti insiderske prijetnje, gdje je akter osoba unutar sustava, kojima ne treba internetska mreža, nego LAN kao lokalna računalna mreža i softverski alati, ali kako govorimo o KNI uzet ćemo u obzir širi perimetar napada, odnosno infrastrukturu koju pruža internet.

U pravilu iza napada rijetko stoji jedna osoba nego skupina ili organizacija koja broji više članova, te svi oni međusobno komuniciraju također internetom. Navedena skupina može upravljati *botnet* infrastrukturom u kojoj se može nalaziti više stotina tisuća zaraženih računala kojima upravlja napadač koji je zarazio ta računala. Računala se mogu zaraziti malicioznim kodom, ili čak kupiti na *underground* sceni (deep web) za imaginarnu internetsku valutu BitCoin (Paganini, 5.2013) koja se prodaje i kupuje za prave valute, a jedna od najvećih burzi je Mt. Gox koja drži preko 80% svih BitCoin transakcija.

Za razliku od glasovne komunikacije telefonom ili elektronskom poštom u prošlosti, današnja komunikacija se odvija putem servisa za koje se ne može osigurati presretanje u realnom vremenu, osim ako nismo prisutni na serveru pružatelja usluge (jedan od primjera je i Skype u vlasništvu Microsofta ili Google Talk u vlasništvu Googlea). Kao što se može pročitati na nekoliko internetskih izvora, FBI ja kao najveći prioritet za ovu godinu sebi postavio zadatak da dobije mogućnost presretanja i čitanja internetskih datotečnih (cloud based) i e-mail servisa u realnom vremenu, ali i drugih oblika internetske komunikacije. Kako proizlazi iz dostupne literature, to još uvijek nisu u stanju, barem ne legalno. (Gallagher, 2013.)[1]

Informacije koje dolaze iz FBI-a govore da će se već ove godine promijeniti zakonska regulativa i da će biti moguće u realnom vremenu nadzirati sve internetske servise i to od Dropboxa do internetskih igara u kojima je moguće komunicirati među korisnicima. Svaki od ovih tipova komunikacije može se potencijalno koristiti za kriminalne aktivnosti. Jedna od takvih aktivnosti su i napadi na kritičnu nacionalnu infrastrukturu.

U ovoj problematici otišlo se toliko daleko da je NATO izdao priručnik za kibernetičko ratovanje. Na priručniku je zadnje tri godine radilo dvadeset eksperata u Talinu, glavnom gradu Estonije pod zapovjedništvom Co-operative Cyber Defence Centre of Excellence (CCDCOE). Centar je osnovan 2008. godine nakon serije kibernetičkih napada na baltičke zemlje iz Rusije. Jedna od preporuka iz priručnika je da se moraju izbjeći kibernetički napadi na osjetljive civilne ciljeve kao što su bolnice, brane ili nuklearne elektrane, dok se navodi da takozvani *haktivisti* mogu biti legitimni ciljevi, iako su civili, ako sudjeluju u kibernetičkom napadu.

[1] Po američkom saveznom zakonu iz 1994. godine: «Communications Assistance for Law Enforcement Act» (CALEA), koji daje ovlasti državnim agencijama da instaliraju svoju opremu za prisluškivanje i praćenje kod telekomunikacijskih i drugih mrežnih operatera. Isti zakon ne pokriva davatelje internetskih usluga poput e-maila, Skypea i ostalih mrežnih servisa koje kontroliraju treće strane.

## 2. Modus operandi (MO) napadača iz primjera incidenata

Analizom javnih izvještaja koje su objavile strane koje su bile zahvaćene napadima, moguće je deducirati par najčešćih MO napadača. Najčešći oblici napada mogu biti kategorizirani u sljedeće grupe:

1. Ciljani napadi na infrastrukturu primjenom malicioznog koda
2. Napadi uskraćivanjem usluge
3. Napadi koji su usmjereni prema zaposlenicima u meti
4. Napadi na infrastrukturu primjenom ciljanih napada.

Ove grupe ne prikazuju sve moguće varijante napada, već samo 4 glavne kategorije koje su najčešće bile korištene zbog vrlo dobrog omjera uloženog truda i efekta protiv cilja napada. Prikaz određenih slučajeva iz prakse bolje će ocrtati trendove napada na KNI. Također, bitno je napomenuti sinergiju primijenjenih napada, te korištenje više metoda napada. Kao studije slučaja, možemo spomenuti sljedeće događaje koje smo obuhvatili u analizi:

1. Napadi protiv sustava SAD-a pod nazivom Titan Rain od 2003
2. Napadi na Estoniju 27. 4. 2007.
3. Korištenje malicioznog koda Flame (prvi znakovi infekcije 2007.)
4. Napadi pod oznakom Operacija Aurora – 2009.
5. Napad na Iranska nuklearna postrojenja uz pomoć malicioznog koda Stuxnet – 2010.
6. Napadi uz pomoć malicioznog koda Duqu – 2011.
7. Otimanje Twitter računa novinskog portala Associated Press – 2013.
8. Napad na SpamHaus – 2013.
9. Ostale napade niskog intenziteta (GhostNet, Napadi za vrijeme Sirijskog građanskog rata, operacije koje provodi Anonymous...).

### *Napadi protiv sustava SAD pod nazivom Titan Rain od 2003*

Meta napada koji su dobili oznaku Titan Rain bile su istraživačke agencije i instituti koji su koncentrirani na razvoj i istraživanje u području obrambenih tehnologija (NASA, Redstone arsenal, Lockheed Martin, laboratoriji Sandia i drugi). Metoda napada na metu je uključivala ciljani oblik zaobilaženja zaštitnih mjera i proboj u sustave s ciljem prikupljanja povjerljivih podataka koji bi bili korisni napadačima i primjenu trojanskog koda protiv računala u mreži (Thornburg, 2005.). Kao izvršitelj napada sumnja se na Kinu zbog toga što su krajnje točke na kojoj su se skupljali podaci bila računala u kineskoj provinciji Guangdong.

### *Napadi na Estoniju 27. 4. 2007.*

Povod napada na Estoniju bilo je micanje kipa ruskog brončanog vojnika i vojnih grobova u Tallinnu koji su Estonci smatrali simbolom Sovjetske okupacije na vojno groblje. Micanje kipa je negativno utjecalo na rusku manjinu unutar Estonije i Rusije. Kao rezultat nezadovoljstva pokrenuti su napadi protiv entiteta u Estoniji. Metoda napada na mete je uključivala DDoS (Distribuirano uskraćivanje usluge) protiv banaka, novinskih portala,

vladinih portala, web stranica političkih stranaka, telekomunikacijskih pružatelja usluge i sličnih. Također, uz DDoS napade, defaceani su i određeni portali na kojima su ostavljene političke poruke. Kao kraj napada, osuđena je jedna osoba stara dvadeset godina (BBC, 2008.), koja je sudjelovala u jednom napadu, ali većina izvora napada bila je vezana uz entitete koji su bili locirani u Rusiji.

***Projekt Olympic Games (Maliciozni kodovi Flame, Duqu, Stuxnet)***

Projekt Olympic Games nikad nije bio javno potvrđen od strane agencija iz SAD-a ili Izraela, za koje se sumnja da su u suradnji razvijali razne oblike *cyber* oružja koji su bili iznimno uspješni u izvršenju svojih zadataka protiv meta u Bliskom istoku. Projekt je započeo oko 2006. godine pod administracijom tadašnjeg predsjednika G. W. Busha, koji je prihvatio mogućnost korištenja malicioznog koda da bi se onesposobio Iranski nuklearni program u postrojenju Natanz. Točni detalji projekta nisu poznati, ali poznat je detalj da je u projekt bila umiješana Izraelska jedinica 8200. Kao rezultat projekta sumnja se da su bili razvijeni maliciozni kodovi: Stuxnet, Duqu i Flame.

Maliciozni kod Flame (CrySyS, 2012) je bio detektiran 2012-te godine od strane CrySiS laboratorija, Iranskog CERT-a i Kaspersky laboratorija. Prve infekcije od ovog malicioznog koda mogu se pratiti već od 2007. što znači da maliciozni kod nije bio detektiran 5 godina, gdje je većina infekcija bila vezana uz računalne sustave u Iranu, Izraelu, Saudijskoj Arabiji, Siriji, Egiptu i Libanonu. Primarna namjena Flamea je bila za špijunažu i prikupljanje informacija, gdje su napadači htjeli prikupiti veliki broj PDF dokumenata i Word dokumenata te nacrta koji su bili izrađeni u alatu AutoCad. Interesantna je velika fleksibilnost Flamea koji ima desetak modula koji služe za razne funkcije te njegova ogromna veličina od 20-ak megabajta. Neke od funkcionalnosti koje je imao je širenje putem mreže, USB stickova, modul za krađu podataka s uređaja koji imaju bluetooth povezanost s inficiranim računalom, prisluškivanje Skype razgovora, spremanje sadržaja koji korisnik unosi putem tipkovnice, spremanje slika koje korisnik vidi na ekranu i velika količina drugih modula. Cijela kompleksnost ovog malicioznog koda je zavidna, gdje se sumnja na povezanost s malicioznim kodom Stuxnet gdje je modul za širenjem malicioznog koda putem USB memorije skoro pa identičan na ta dva maliciozna koda.

Drugi maliciozni kod za koji se sumnja da je iz iste porodice je Duqu (CrySyS, 2011). Duqu je bio identificiran krajem 2011. godine, gdje je CrySyS laboratorij utvrdio da se radi o malicioznom kodu iz iste porodice kao Stuxnet. Duqu je bio namijenjen za skupljanje informacija i podataka s računala koje je zarazio i služio je za pripremanje terena za daljnje napade. Jedna od funkcionalnosti mu je bila krađa kriptografskih ključeva i certifikata što je omogućavalo veću razinu pristupa za napade koji su slijedili.

Najzanimljiviji maliciozni kod iz skoro svih studija slučaja je Stuxnet (Eset, 2011), (Symantec 2011), (Paganini, 2013). Stuxnet je bio poznat po svojem učinku protiv Iranskog nuklearnog programa. Stuxnet je inficirao računalnu mreže uz pomoć više mehanizama širenja, kao što je širenje putem USB memorija, putem ranjivih mrežnih servisa. Interesantno je bilo korištenje više *0day* ranjivosti za koje nije postojala protumjera za zaštitu. Zadnje verzije Stuxneta su imale čak 6 takvih ranjivosti, koje je koristio za inficiranje kontrolera za upravljanje industrijskim postrojenjima gdje mu je primarna namjena bila uništavanje centrifuga za obogaćivanje urana. Prema nekim slobodnim procjenama Stuxnet je uništio oko 1 000 centrifuga u Natanzu povećavanjem brzine rada centrifuge i pokazivanjem operateru centrifuge da je odabrana brzina ona koju je operater unio u kontroler. Prema nekim slobodnim procjenama, Natanz je u to vrijeme imao oko 3 000 centrifuga što bi značilo da je Stuxnet

imao značajni utjecaj na Iransku nuklearnu infrastrukturu. Postoje neke informacije prema kojima Stuxnet nije imao značajan utjecaj protiv Iranske infrastrukture jer su nakon 2010. očito povećane zaštitne mjere i povećan broj centrifuga za obogaćivanje urana. (Leyden, 2013). Kao reakciju na taj napad, Iran je povećao svoje ofenzivne sposobnosti za kibernetičko ratovanje i započeo napade na razne mete diljem SAD-a. (Perlroth; Sanger, 2013)

***Napadi pod oznakom Operacija Aurora***

Napadi koji su dobili naziv Operacija Aurora su za metu imali razne tvrtke i entitete iz SAD-a kao što su Google, Yahoo, Symantec, Adobe, Rackspace i mnogi drugi. Pretpostavlja se da su napadači htjeli prikupiti intelektualno vlasništvo, podatke, nacrte radi produbljivanja svojeg znanja u interesnim sferama te da su htjeli ukrasti i modificirati izvorni programski kod aplikacija koje su razvijale napadnute strane. Google je kao jedna od napadnutih strana tvrdio da su napadači htjeli i uspjeli doći do određenih GMail računa koji koriste kineski disidenti i politički aktivisti. Mehanizam napada je bio dosta kompleksan, napadači su napadali stranice koje bi posjećivali korisnici gdje bi te stranice nosile maliciozni kod koji bi zarazio korisnikovo računalo kada bi korisnik posjetio te web strance, gdje bi napadači mogli dalje i dublje upadati u mrežu gdje se nalazi korisnikovo računalo. Kao glavne napadače sumnja se na Elderwood (O'Gorman; McDonald, 2012) skupinu ili PLA jedinicu 61398 koja je pobliže opisana u (Mandiant, 2003) dokumentu.

***Otimanje Twitter računa novinskog portala Associated Press***

Dana 23. 4. 2013. skupina Syrian Electronic Army koja ideološki podržava Sirijsku vladu, neovlašteno je pristupila računu Associated Pressa na društvenoj mreži Twitter (Moore; Roberts, 2013.), (Associated Press, 2013.). Rezultat neovlaštenog pristupa je bio da s računa AP-a odaslan lažni tweet koji je glasio "Dvije eksplozije u Bijeloj kući, Barack Obama je ozlijeđen" na oko 2 012 212 korisnika koji prate tvrtku Associated Press. Učinak lažnog Tweeta je bilo moguće osjetiti na burzi, gdje je Dow Jones Industrial Average indeks pao 130 bodova, tj. procijenjen je pad od 136 milijardi USD po Standard & Poor 500 indeksu, koji je nakon objave da je vijest lažna te da je AP bio žrtva hakerskog napada uspio vratiti na stare vrijednosti. Cijeli napad je bio izveden uz pomoć *phishing* tehnike gdje su e-mailovi koje su korisnici primili sadržavali link na maliciozni kod koji je omogućio krađu autentikacijskih podataka.

**Napad na Spamhaus**

U svibnju 2013. organizacija SpamHaus koja se bavi borbom protiv neželjenih e-mail poruka je bila metom najvećeg DDoS napada nakon što je označila pružatelja hosting usluge CyberBunker kao da je izvor spam poruka (Henley, 2013). Tvrtka CloudFlare koja migrira DDoS napade je javila da je DDoS napad u svojem naponu bio jak oko 300 Gbps a da je bio stabilan oko 90 Gbps po čemu je to bio najveći DDoS napad u povijesti. Kao usporedba, napad koji je onesposobio veći dio estonijske infrastrukture se procjenjuje na oko 1 od 10 Gbps. Tvrtka CloudFlare je govorila da je to napad zbog kojeg su korisnici interneta osjećali posljedice i da je to bio napad koji je skoro "slomio internet" (Prince, 2013), ali utjecaj na globalnu mrežu nije potvrđen, niti je bio osjetan što je zapravo mnoge eksperte dovelo do toga da su govorili da je više bilo riječi o marketingu tvrtke CloudFlare nego o napadu koji bi

"slomio internet". Napad je bio uspješan protiv ciljanog entiteta i stao je kada je jedan od glavnih ljudi u napadu bio uhićen.

***Akteri navedenih napada***

Akteri navedenih napada su relativno bitni ako gledamo atribuciju napada ili otkrivanje aktera za neki upad. S pogleda zaštite su relativno nebitni, napadačima je dovoljno da otkriju jedan sigurnosni propust da ispune svoj cilj, a obrana mora pokriti sve moguće ranjivosti ili vektore napada. Kao neki od aktera, možemo spomenuti sljedeće strane jedinice i skupine za koje se sumnja da imaju mogućnost izvođenja kibernetičkih napada:

1. Kineski PLA Unit 61398 koji je opisan u dokumentu o (Mandiant, 2003) prijetnji
2. Izraelski Unit 8200 (IDF, 2008)
3. SAD: NSA, CIA, jedinice iz Wright-Patterson Air Force baze (Wright-Patterson, 2011)
4. Syrian Electronic army
5. Iranian Cyber Army
6. Honker Union / Red Hacker Alliance (Kina)
7. RedHack (Turska)
8. Anonymous (koji tehnički nije skupina)
9. Razne manje grupacije.

Analiza mogućih metoda napada i MO navedenih jedinica i skupina je izvan opsega ovog rada, ali navedeni popis je dobra referenca za daljnje istraživanje u tom području za zainteresirane čitatelje.

## 3. Analiza napada i uzoraka iz napada

U prijašnjem poglavlju, definirali smo da se napadi mogu klasificirati u četiri kategorije. Svakoj od navedenih kategorija možemo pridružiti par značajki koje smo izdvojili analizom tih slučajeva.

***Napadi uskraćivanjem usluge (DDoS)***

1. Većina napada uskraćenjem usluge koristi zaražena računala koja su inficirana napadačevim malicioznim kodom (botom) za izvršavanje napada uskraćivanja usluga. Sinergijski efekt je u tome da se isti bot može koristiti i za prikupljanje podataka, špijunažu, korištenje računalne snage za probijanje lozinki i kriptoanalizu i ostale primjene.
2. Većina napada nije koristila primitivno generiranje prometa, već je koristila Slowloris tehniku ili su koristili otvorene DNS poslužitelje da generiraju veliku količinu prometa uz pomoć DNS amplification napada (US-CERT 2013).
3. Ukoliko napad nije mogao onesposobiti glavnu metu, pokušao je onesposobiti infrastrukturu pružatelja usluge u cilju da uruši pristup glavnoj meti na način da napadne

infrastrukturu koju ne održava meta, čime se dodatno komplicira obrana od napada zbog potrebe koordinacije s više pružatelja usluge i napadnutom stranom.

4. Razne skupine kao što je Anonymous koriste varijante alata pod nazivom LOIC gdje članovi pokreta koriste alat kao mehanizam za DDoS napad protiv neke mete. LOIC je dosta jednostavno blokirati jer ostavlja dovoljno tragova i ima predvidljiv uzorak napada, ali postoji mogućnost razvoja boljih alata i "dijeljenja" tih alata skupinama koje dijele isti cilj ili motiv. Kao primjer, možemo spomenuti alat XerXeS koji koristi aktivist imena th3j35t3r protiv web stranica s ekstremističkim i islamističkim sadržajima. XerXeS je "iscurio" u određenim krugovima i postao dostupan širem krugu mogućih napadača.

***Ciljani napadi na infrastrukturu primjenom malicioznog koda***

1. Maliciozni kodovi koji se koriste kao cyber oružja pokazuju se višestruko "težima" od klasičnih malicioznih kodova. Kao primjer, klasični maliciozni kodovi su veliki od par Kb do 2-3 Mb, dok su varijante Flame malicioznog koda bile velike oko 20 Mb.
2. Kod malicioznih kodova kao što je Stuxnet, koristilo se više *0day*[2] ranjivosti koje su povećavale vjerojatnost da će maliciozni kod upasti u ciljano računalo, takav MO nikada ne bi koristile osobe koje se bave računalnim kriminalom, jer u slučaju detekcije jedne ranjivosti ili jednog elementa u malicioznom kodu, cijeli maliciozni kod bi postao poznat. Ukoliko je broj zaraženih računala cilj napada, onda je rentabilnije iskoristiti više malicioznih kodova gdje svaki iskorištava jednu ranjivost.
3. Antivirusni alati su beskorisni protiv bilo kojeg malicioznog koda koji nije detektiran od strane proizvođača AV alata, zbog toga su ciljani maliciozni kodovi bili detektirani tek nakon što su ih detektirali administratori sustava. Također, namjenski maliciozni kodovi koriste više metoda sakrivanja svoje izvršne verzije programa da bi otežali detekciju uz pomoć antivirusnog alata.

***Napadi koji su usmjereni prema zaposlenicima u meti***

1. Većina napada protiv zaposlenika temeljila se na *phishing* napadima, gdje je zaposleniku poslana e-mail poruka s privitkom koji je korisnik pokrenuo zato što je mislio da dolazi iz legitimnog izvora. Problem kod navedenih *phishing* napada je da su poruke, pošiljatelji i primatelji izgledali iznimno autentično s imenima iz organizacije u kojoj oni rade, što nije navodilo mete u napadu da sumnjaju da je riječ o malicioznom kodu već o legitimnoj poruci koja je namijenjena upravo za njih.
2. Napadači su koristili i "watering hole" napade, gdje su u web stranicu koju posjećuju korisnici koje oni žele napasti umetnuli posebni oblik malicioznog koda koji napada korisnike koji koriste stare verzije web preglednika ili dodataka za web preglednik (Java ili Adobe Flash). Sigurnosni propusti u tim verzijama web preglednika

[2] *0day – zero day* – sigurnosni propusti koje su otkrili pojedinci, ali koje ne zna šira javnost ili proizvođač. Za takve propuste ne postoji zakrpa koja neutralizira ranjivost, već postoji veći rizik od napada na taj servis ukoliko nije ograničen pristup tom servisu. Napadači čuvaju 0day propuste zbog iznimne učinkovitosti protiv ciljanih meta i visoke cijene na crnom ili bijelom tržištu koje se kreću od 500 do 250 000 eura.

ili dodataka su omogućavale i zarazu korisničkih računala i daljnje korištenje tih računala za napad i krađu podataka s tih računala.

3. Računala koja nisu imala vezu s internetom najčešće su bila zaražena od strane zaposlenika koji su namjerno ili nenamjerno koristili USB memoriju da bi proširili zarazu na računala koja nisu bila povezana s internetom. USB memorija je bila zaražena s oblikom malicioznog koda koji nije tražio pokretanje datoteke s memorije već je bilo dovoljno priključiti USB memoriju na računalo.

***Napadi na infrastrukturu primjenom ciljanih napada***

1. Dobar dio napada koji su izveli razni aktivisti ili neke skupine nisu bili usmjereni protiv kritičnih dijelova infrastrukture već je glavni cilj bio defacement, tj. postavljanje poruka na probijene *siteove* ili krađa podataka s tih probijenih računala. U nekim slučajevima, napadnute strane su imale iznimno loše sigurnosne prakse.
2. Većina ciljanih napada je uključivala iznimno dugotrajne aktivnosti protiv ciljeva, uz iznimni trud i uložene resurse. Ukoliko ciljevi nisu imali postavljen cjeloviti sustav sigurnosti na visokoj razini, u većini slučajeva su napadači bili uspješni.

***Budući razvoj cyber oružja***

Teško je predvidjeti budući razvoj *cyber* oružja. Kao osnovicu možemo vidjeti da DARPA (Agencija za istraživanje i razvoj obrambenih tehnologija iz SAD-a) pokušava unaprijediti cyber oružja da budu jednostavnija za korištenje operaterima koji nisu vješti u razvoju takvih oružja (Cox, 2013), (Shachtman, 2013) i da se mogu pokretati, lansirati i ciljati iz mobilnih uređaja ili raznih drugih terminala. Također, pokušava se razne maliciozne kodove, napade i slične pretvoriti i staviti u isti kontekst kao projektile, gdje operateri mogu lagano utvrditi žele li lansirati i otkriti neki oblik malicioznog koda protiv neke proizvoljne mete [CW2]. Također, bitno je naglasiti da neki eksperti (Stevenson, 2013) misle da nije dobro govoriti o cyber ratovanju, već o špijunaži, jer govoriti o cyber ratu samo podiže strah od napada i podiže veću deregulaciju zakona koji omogućavaju veću slobodu raznim vojskama da participiraju u još jednoj novoj utrci naoružanja.

Razvijenim zemljama trenutačno nedostaje domaćih stručnjaka iz područja prirodnih znanosti i tehnologije, a vidljiv je utjecaj stranih stručnjaka iz Dalekog istoka na ovom području, prvenstveno stručnjaka iz Kine i Indije koji su prodrli u sve visokotehnološke institucije gdje se njihovo znanje od iznimne važnosti. Bivši zaposlenik NASA-e Bo Jiang koji je razvijao tehnologiju za prepoznavanje slika dobio je otkaz u NASA-i zbog činjenice da je Kinez i da se sumnjalo da je Kineski špijun, a ne zbog neke njegove krivnje. Kongresnik Frank Wolf, odlučio je upozoriti na opasnost od stručnjaka koji iz Kine dolaze u Ameriku raditi za tehnološki sektor i predstavljaju „sigurnosni rizik“. (Wolf, 2013). Jianga se također teretilo da je već jednom odnio laptop pun povjerljivih sadržaja sa sobom u Kinu, pogotovo sa sadržajima koji su vezani uz visoke tehnologije vojne primjere. FBI je 16.3.2013. presreo Jianga u zračnoj luci te mu je oduzet prijenosnik radi pretrage, na kojem je umjesto raznih povjerljivih sadržaja koje je htio predati kineskim vlastima, pronađena velika količina piratiziranih filmova, serija i pornografskih sadržaja koje je Jiang, preuzeo koristeći NASA-inu infrastrukturu. Kongresnik Wolf je sa svojih stranica povukao prvotno priopćenje, ali se u Googleovom *webcacheu* može pronaći izvorna objava kongresnika Wolfa. (Google Cache od Wolf, 2013). Radi poboljšanja svoje obrane od cyber napada protiv kritične nacionalne

infrastrukture, neke su zemlje počele stvarati svoje strategije i smjernice za zaštitu KNI (CPNI).

## 4. Zaključak

Trenutačni razvoj metoda i napada na informacijske sustave predstavlja ne samo veliki rizik za sve sustave, već otvara nove mogućnosti za informacijsko ratovanje i špijunažu. Iz priloženih studija slučaja, vidimo da takav razvoj nije neka moguća budućnost, već sadašnjost u kojoj moramo pokušati osigurati cjeloviti sustav sigurnosti u cilju sprječavanja novih prijetnji našim sustavima u svim državnim ili poslovnim aspektima. Kao posebni interes, osiguranje sustava sigurnosti za sustave koji su dio kritične nacionalne infrastrukture, trebao bi biti prioritet zbog mogućih utjecaja koje nove metode napada mogu imati protiv te infrastrukture, kao što smo imali priliku vidjeti kroz primjere projekta Olympic Games i napada na Estoniju, te dodatnih razloga jer su neke države već razvile ili razvijaju posebne grupe u agencijama čija je zadaća upravo informacijsko ratovanje ili špijunaža.

U zadnjih par godina, vidimo sve veći trend i značaj *cyber* ratovanja i prve slučajeve napada protiv elemenata KNI-a. Također mehanizmi za *cyber* ratovanje postaju sve dostupniji, i nisu više dostupni samo vladama, već se razvojem može baviti skoro svaka grupacija koja ima minimalne uvjete i volju.

Prema izvještaju Britanskog državnog ureda za reviziju, u Ujedinjenom Kraljevstvu postoji velik manjak sigurnosnih stručnjaka. U izvještaju se ističe kako bi ovaj manjak mogao negativno utjecati na njihovu sposobnost obrane sustava od napada. Procjenjuje se da će se manjak sigurnosnih stručnjaka nadoknaditi tek kroz 20 godina. (ITPro 2013.)

## Literatura

1. Associated Press (2013), http://bigstory.ap.org/article/hackers-compromise-ap-twitter-account
2. BBC, Estonia fines man for 'cyber war' (2008) http://news.bbc.co.uk/2/hi/technology/7208511.stm
3. CALEA: Communications Assistance for Law Enforcement Act (2013), http://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act
4. CCDCOE: NATO Cooperative Cyber Defence Centre of Excellence (2013), https://www.ccdcoe.org/
5. Centre for the Protection of National Infrastructure: CPNI, www.cpni.gov.uk/advice/cyber/ http://www.cpni.gov.uk/advice/cyber/
6. Cox, Matthew: DARPA Outlines Plans To Develop Cyber Weapons (2013), http://www.dodbuzz.com/2013/04/25/darpa-outlines-plans-to-develop-cyber-weapons/
7. Eset: Stuxnet Under the Microscope: January 2011, http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
8. Fox, Zoe: 'Anonymous' hackers hit security group (2011), http://edition.cnn.com/2011/12/26/tech/web/anonymous-hack-stratfor/
9. Gallagher, Ryan: FBI Pursuing Real-Time Gmail Spying Powers as “Top Priority” for 2013 (2013), http://www.slate.com/blogs/future_tense/2013/03/26/andrew_weissmann_fbi_wants_real_time_gmail_dropbox_spying_power.html
10. Google Cache od: Wolf, Frank: Wolf Addresses Arrest at Dulles Airport of Chinese National Potentially Involved in Nasa Langley Security Violations Suspect Currently in

FBI Custody in Norfolk (2013), http://webcache.googleusercontent.com/search?q=cache:F4b7jBPy5WAJ:wolf.house.gov/press-releases/wolf-exnasa-langley-contractor-arrested-trying-to-leave-country/+&cd=1&hl=en&ct=clnk&gl=us
11. Henley, Jon: Was 'the biggest cyberattack in history' all just a PR stunt? (2013), http://www.guardian.co.uk/technology/shortcuts/2013/mar/28/spamhaus-internet-attack-pr-stunt
12. Israel Defense forces: Unit 8200: In the Beginning: (2008), http://dover.idf.il/IDF/English/News/today/2008n/09/0101.htm
13. ITPro: IT skills shortage hampers UK response to cyber threats (2013), http://www.itpro.co.uk/645643/it-skills-shortage-hampers-uk-response-to-cyber-threats
14. LOIC: Low Orbit Ion Cannon, http://sourceforge.net/projects/loic/
15. Laboratory of Cryptography of Systems Security (CrySyS): Duqu: A Stuxnet-like malware found in the wild, (2011), http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf
16. Laboratory of Cryptography of Systems Security (CrySyS): sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks (2012), http://www.crysys.hu/skywiper/skywiper.pdf
17. Leyden, John: 'Lab-smashing' Stuxnet HELPED Iran's nuke effort, says brainiac (2013), http://www.theregister.co.uk/2013/05/21/stuxnet_helped_iran_says_boffin/
18. Mandiant: APT1: Exposing One of China's Cyber Espionage Units" (2013), http://intelreport.mandiant.com/
19. Moore, Heidi; Roberts, Dan: AP Twitter hack causes panic on Wall Street and sends Dow plunging (2013), http://www.guardian.co.uk/business/2013/apr/23/ap-tweet-hack-wall-street-freefall
20. O'Gorman, Gavin; McDonald, Geoff: The Elderwood Project (2012), https://www.cs.cornell.edu/courses/CS6410/2012fa/slides/Symantec_ElderwoodProject_2012.pdf
21. Paganin, Pierluigi: Stuxnet was dated 2005, Symantec discovered earlier version 0,5 (2013), http://securityaffairs.co/wordpress/12616/malware/stuxnet-was-dated-2005-symantec-discovered-earlier-version-05.html
22. Paganini, Pierluigi: How to profit illegally from Bitcoin … cybercrime and much more (5.2013), http://resources.infosecinstitute.com/how-to-profit-illegally-from-bitcoin-cybercrime-and-much-more/
23. Perlroth, Nicole; Sanger, David: New Computer Attacks Traced to Iran, Officials Say (2013), http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html?_r=1&
24. Prince, Matthew: Cloudflare blog (2013), http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet
25. Prolexic, DDOS report (2013), https://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q1.html
26. Shachtman, Noah: This Pentagon Project Makes Cyberwar as Easy as Angry Birds (2013), http://www.wired.com/dangerroom/2013/05/pentagon-cyberwar-angry-birds/
27. Slowloris HTTP DoS, http://ckers.org/slowloris/
28. Stevenson, Alastair: Chinese hacker attacks risk fuelling cyber arms race, warns Bruce Schneier (2013), http://www.v3.co.uk/v3-uk/news/2249975/chinese-hacker-attacks-risk-fuelling-cyber-arms-race-warns-bruce-schneier
29. Symantec, Stuxnet dossier (2011), Preuzeto sa: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

30. Thornburg, Nathan: The Invasion of the Chinese Cyberspies (2005) Preuzeto sa: http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html
31. US-CERT: Alert TA13-088A - DNS Amplification Attacks (2013), Preuzeto sa: https://www.us-cert.gov/ncas/alerts/TA13-088A
32. Wolf, Frank: Wolf Addresses Arrest at Dulles Airport of Chinese National Potentially Involved in Nasa Langley Security Violations Suspect Currently in FBI Custody in Norfolk , (2013). Preuzeto sa: http://wolf.house.gov/press-releases/wolf-chinese-national-potentially-involved-in-nasa-langley-security-violations/
33. Wright-Patterson AFB (2011): Preuzeto sa: http://www.wpafb.af.mil/news/story.asp?id=123262849