DOI: 10.19279/TVZ.PD.2016-4-1-04

NAPADI ZLONAMJERNIM PROGRAMIMA NA RAČUNALNO UPRAVLJANJA INDUSTRIJSKA POSTROJENJA

MALICIOUS SOFTWARE ATTACKS AGAINST COMPUTER – CONTROLLED INDUSTRIAL PLANTS

Marinko Žagar

Tehničko veleučilište u Zagrebu

Sažetak

Računalno upravljana industrijska postrojenja upotrebljavamo svakodnevno iako toga nismo ponekad svjesni. Kad ulazimo u lift, dok boravimo u klimatiziranom prostoru, dok prelazimo cestu ili se vozimo tunelom, pa do kompleksnih proizvodnih postrojenja poput tvornice stakla, proizvodnje piva ili nuklearne centrale. U svim navedenim slučajevima procese upravljaju i nadziru računala ili PLC-ovi u SCADA sustavima. U ovom radu opisani su i analizirani napadi na navedene računalno vođene industrijske sustave. Unatrag nekoliko godina opće prihvatljivo mišljenje je bilo kako PLC sustavi nisu podložni zlonamjernim programima jer nisu spojeni na Internet pa su stoga zaštićeni od zlonamjernAih programa. Otkrićem zlonamjernog programa Stuxnet svijet se suočio sa posve novim načinom upotrebe zlonamjernih programa. Prvi puta takav program upotrjebljen je kao ofenzivno oružje i kibernetičkom ratu (cyberwar) su širom otvorena vrata. U radu su prikazani načini i razlozi zaraze računala te područja na kojima su zaraze bile najrasprostranjenije.

Ključne riječi: *SCADA, Stuxnet, industrijska postrojenja, zlonamjerni programi, cyberwar*

Abstract

We use computer-controlled industrial plants every day, even when we are not aware of that. We are using computer-controlled systems when entering the elevator, when staying in the air-conditioned space and crossing the road or riding through a tunnel. Computer-controlled systems operate with complex production facilities such as a glass factory, a brewery plant or a nuclear power plant. In all these cases, the process is controlled and monitored by computers or SCADA systems. This paper describes and analyzes the attack against the computer-driven industrial system. Several years ago general opinion that PLC systems were not vulnerable to malware was acceptable because PLC was not connected to the Internet and therefore, they were protected against malware. By the discovery of the Stuxnet malware the world was faced with a completely new way of using malware. For the first time malware was used as offensive weapons and the door for cyberwar was open wide. The paper presents the ways of infecting the computer and the area where the infection was most widespread.

Keywords: *SCADA, Stuxnet, industrial plants, malitious software, cyberwar*

1. Uvod

1. *Introduction*

Kad se dogodio prvi crash na postrojenjima za obogaćivanje urana Natanz u Iranu 2008. godine, nitko u postrojenju nije bio svjestan da se nalaze pod napadom ofenzivnog zlonamjernog programa ili računalnog crva Stuxnet. Upravo je to bio cilj tvoraca Stuxneta [11]. Stuxnet je izrađen s namjerom da bude kibernetičko ofenzivno oružje kojim će se napasti i onesposobiti centrifuge za obogaćivanje urana te onesposobiti Iranski nuklearni program na duže vrijeme. Tvorci Stuxneta nisu razmišljali o posljedicama i mogućem širenju izvan Natanze. Danas znamo da je napad u potpunosti uspio ali jednako tako znamo da se Stuxnet proširio internetom i na žalost može ugroziti mnoga industrijska postrojenja širom zemaljske kugle. Supervisory control and data acquisition system

ili kratko SCADA sustav upotrebljava se u industrijskim postrojenjima za upravljanje raznim automatiziranim procesima. [5] Svakodnevno se nalazimo i koristimo uređaje koje upravljaju SCADA sustavi poput liftova, klimatizacijskih sustava, upravljačko kontrolnih sustava na cestama i tunelima. Jednako tako SCADA sustavi upravljaju različitim proizvodnim postrojenjima a prema istraživanjima provedenim u SAD-u, SCADA sustavi upravljaju sa oko 80% elektrocentrala u SAD-u.[5] Kod dizajniranja ovakvih sustava glavni problem su bile performanse a o sigurnosnom aspektu nije se donedavno uopće razmišljalo.
U ožujku 2000. godine, Vodoopskrbni sustav Maroochy u Australiji izgubio je komunikaciju između pumpnih stanica što je prouzročilo nestabilan rad cijelog sustava vodoopskrbe. U prvi mah operateri su posumnjali u tehnički kvar ali su detaljnijim pregledom utvrdili da se radilo o hakiranju sustava te da je maliciozni softver uzrokovao probleme u radu. Sličan problem dogodio se u kolovozu 2003. godine u nuklearnoj centrali David-Besse u Ohaju, SAD. [1] Zlonamjerni program je zaobišao kontrolnu sobu i vatrozid te zarazio SCADA sustav. Ovakvi problemi kulminirali su u srpnju 2010. Kad je otkriven Stuxnet, SCADA specifičan zlonamjerni program.

2. Olimpijske igre

2. *The Olympic Games*

Napadi zlonamjernim programima na računalno upravljana industrijska postrojenja postali su novi oblik ofenzivnog ratovanja. Specijalizirani zlonamjerni programi dizajnirani su u svrhu sabotaže i napada na programibilne logičke kontrolere (programmable logic controllers - PCL) kako bi ih onesposobili ili natjerali da rade izvan predviđenih parametara. Prema navodima New York Times [8] zlonamjerni program proizveli su zajedničkim snagama SAD i Izrael s ciljem napada na Iransko nuklearno postrojenje Natanz. Jedna od najtajnijih operacija pod nazivom Olimpijske igre (Olypic Games) [11] bila je poznata samo malom uskom krugu vojno-obavještajnih dužnosnika SAD-a. Osim onesposobljavanja Iranskog nuklearnog programa na duže vrijeme, bilo je potrebno privoljeti Izrael da ne bombardira Natanz postrojenje planiranim avionskim napadom već da zajedno provedu kibernetički napad. Ovo je prvi ofenzivni kibernetički napad izveden na jednu državu od strane američka agencije NSA i izraelskog pandana Unit 8200. Operacija je trajala nekoliko godina i odvijala se u nekoliko faza dok u konačnici zlonamjerni program kojeg danas poznajemo pod nazivom Stuxnet nije ubačen u postrojenje. Napad je izveden kombinacijom nekoliko različitih vrsta napada, socijalni inženjeringom, izradom ciljanog zlonamjernog koda, uključenjem špijunskih agencija, otimanjem i mučenjem odgovornih pojedinaca s ciljem otkrivanja vrijednih informacija i sl. [4]
Rotori kao najvažniji dijelovi centrifuge, okreću se na velikoj brzini i svaka centrifuga u nizu proizvodi čišću verziju Urana 235 od prethodne. Brzina na kojoj se okreće centrifuga je vitalna i ukoliko bi se brzina značajno povećala prijetila je raspadom sustava. Ukoliko bi se sustav naglo zaustavio, također postaje nestabilan i ponaša se kao metalni tornado uništavajući sve u blizini uključujući i ljude koji rade u postrojenju. Upravo su ovo efekti koje je operacija "Olimpijske igre" trebala proizvesti.
Prvi korak operacije bilo je snimanje postrojenja i izrada tzv. Blueprinta. U tu svrhu proizveden je zlonamjerni kod Beacon koji je ubačen sa ciljem mapiranja cijelog Natanza postrojenje, otkrvanja kako kontroliraju centrifuge, kako se odvija dnevna rutina i sl. Najbitnija informacija je kako su centrifuge povezane sa PLC-ovima (programmable logic controllers)? PLC-ovi su računala koja upravljaju svim aspektima rada centrifuga i u to vrijeme su bili potpuno nezaštićeni. Podizanje takozvane "air gap[1]" zaštite podrazumijevalo se sigurnim od bilo kakvih zlonamjernih programa ili napada. Zaobilaženje „air gap" zaštite bio je prvi operativni problem tj. ubacivanje Beacona u sustav. U tu svrhu iskorišteni su djelatnici Siemensa koji su redovito servisirali PLC-ove, a koji nisu ni znali za operaciju tj. da su njihova računala nosioci Beacona. Nakon nekoliko mjeseci rezultati tj. blueprints svih direktorija, elektroničkih

1 Air-gap zaštita kod koje je sustav fizički odvojen od Interneta ili drugih sustava

komunikacija i što je najvažnije konfiguracija centrifuga stigle su u stožer operacije Olympic Games. NSA i Unit 8200 imali su materijal za početak rada na računalnom crvu kojeg su nazvali „bug“. Nakon razvoja Bug je trebalo testirati na istim centrifugama koje je imao Iran, oznake P-1. Iste centrifuge preko nekoliko ruku SAD je kupio od Muammera Qaddafia nakon što je 2003. odustao od nuklearnog programa. Nakon niza testova na nekoliko centrifuga Bug se pokazao vrlo uspješnim i akcija je mogla započeti. Kad je izveden prvi napad 2008. godine, inženjeri u Natanz postrojenju nisu bili ni svjesni napada već su mislili da se radi o grešci sustava. Od ukupno 5.000 centrifuga onesposobljeno je njih 984 i cijeli program je zaustavljen. [11]

3. Stuxnet

3. *Stuxnet*

Najstarija poznata verzija Stuxneta bila je 1.001 iz 2009. godine i ta se verzija povezivala sa napadom na Natanz postrojenje, ali je istraživanje provedeno od strane Symantec-a [7] pokazalo da postoji još starija verzija 0.5. Prema provedenim analizama na Symantec dostupnom Stuxnet kodu, pokazala je da je ova verzija bila operativna još 2005. godine. Osnovne karakteristike verzije 0.5:

- Najstarija pronađena verzija Stuxneta
- Izgrađena na Flame[2] platformi
- Širi se putem USB uređaja
- Prestala se širiti 04.07.2009.
- Ne sadrži Microsoft exploite
- Ima punu funkcionalnost za napad na Siemens 417 PLC-ove

Osim navedenih, Stuxnet ima i sljedeće osobine [12]:

- Samostalno kopiranje putem prijenosnih diskova i iskorištavanje ranjivost Windows prečica za samostalno pokretanje (ranjivost Microsoft Windows prečica kod LNK i PIF datoteka omogućuje napadaču izvršavanje koda).
- Širenje po LAN-u kroz ranjivost Windows usmjerivača ispisa (eng. *Print Spooler*).
- Širenje kroz SMB protokol (eng. *Server Message Block*) iskorištavanjem propusta prilikom poziva udaljene procedure kod Microsoft Windows Server servisa.
- Kopiranje i izvršavanje na udaljenim računalima putem dijeljenih direktorija u mreži.
- Kopiranje i izvršavanje na udaljenim računalima s pokrenutim WinCC poslužiteljem baze podataka.
- Kopiranje u Step 7 projekt (.S7P datoteke) na način da se automatski izvršava kada se Step 7 projekt učita u PLC.
- Ažuriranje unutar LAN-a putem peer-to-peer mehanizma.
- Iskorištavanje ukupno četiri Microsoft ranjivosti, od kojih su dvije već spomenute ranjivosti za samostalno umnožavanje, a druge dvije su ranjivosti za eskalaciju privilegija koje tek trebaju biti objavljene.
- Uspostavlja kontakt s upravljačkim i nadzornim poslužiteljem koji omogućuje hakeru preuzimanje i izvršavanje koda.
- Sadrži rootkit Windows sustava kojim sakriva svoje datoteke.
- Izbjegava sigurnosne mehanizme sustava na kojem se nalazi.
- Imitira specifične ICS-e i mijenja kod na Siemens PLC-u za potencijalno sabotiranje sustava.
- Skriva promjene koda na PLC-u (u suštini rootkit za PLC).

Stuxnet je građen da se može infiltrirati u platforme odnosno operacijske sustave na kojima se može instalirati Step7 ili PCS7. Spominju se takvi sklopovi unutar elektrana i sličnih velikih industrijskih postrojenja, ali Stuxnet je specijalno bio namijenjen za uništavanje centrifuga P-1 koje su se koristile za obogaćivanje urana u Iranu. Direktno su ciljani PLC uređaji tvrtke Siemens, modeli „Simatic“ S7 i PSC7, koji su koristili podatkovne blokove DB 890 i DB8062 i to s takvim postavkama koje se koriste isključivo u ciljanom okruženju kojeg se napada. Jedna od glavnih komponenti koje je zlonamjerni kod koristio bio je prvi PLC rootkit u povijesti. Industrijskim sustavima kontrole (ICS) se upravlja pomoću specijaliziranog koda sličnog asemblerskom jeziku koji se nalazi na programibilnim logičkim kontrolerima (PLC). Simatic manager je program za programiranje rada PLC-ova koji su u vrijeme pronalaženja Stuxnet crva mogli raditi na Windows 32 bitnim operacionim sustavima koja obično nisu spojena na Internet ili internu mrežu. Zadnja verzija Step7

2 Flame platforma

V5.5 Siemens Simatic manegera može raditi na windows 64 bitnom sustavu, ali ona je izdana nakon pronalaska Stuxneta. Osim toga, industrijski sustavi kontrole i sami većinom nisu spojeni na Internet, ali mogu biti umreženi u neki industrijski lokalni LAN. Prvi korak napada je izviđanje. Kako je svaki PLC konfiguriran na sebi jedinstven način, napadač bi prvo trebao imati saznanja o strukturi ICS-a. Takva se dokumentacija mogla ukrasti osobno ili kao u navedenom slučaju izradu blueprinta postrojenja izvodi posebno dizajnirani zlonamjerni kod Beacon. Nakon pribavljanja potrebne dokumentacije te upoznavanja s konfiguracijom mreže, računalnim okruženjem i sl., razvija se prilagođena verzija zlonamjernog programa prilagođena specifičnom ICS-u. Napadači mogu koristiti ogledno okruženje koje će uključivati potrebnu ICS opremu kao što su PLC, moduli i periferije kako bi testirali svoj kod što je u navedenom slučaju i napravljeno zahvaljujući ranije nabavljenoj opremi iz Libije. Napadači su, da izbjegnu svaku sumnju, datoteke sa zlonamjernim kodom i digitalno potpisali. Da bi to postigli napadači su se domogli dva digitalna certifikata najvjerojatnije fizičkom krađom jer su dvije tvrtke od kojih su certifikati ukradeni u neposrednoj blizini. Kako bi zarazio ciljani sustav, Stuxnet je trebao biti uveden u ciljnu okolinu. Pretpostavka je da je do zaraze došlo neznanjem treće strane Siemensa, koji je imao pristup do objekta i sustava radi održavanja istih, dok je izvorna zaraza uvedena pomoću prijenosnog diska (USB stika). Nakon zaraze računala unutar sustava Stuxnet se počeo širiti u potrazi za Siemens računalima Field PG, (Windows računala koja su namijenjena specijalno za programiranje PLC-ova). Većina tih računala nisu umrežena, zlonamjerni kod širi se na druga umrežena računala putem prijenosnih diskova iskorištavajući još neotkrivenu (nezaštićenu rupu u sustavu) starijih Step 7 projekata. Umnožavanje preko mreže kroz LAN i prijenosne diskove vjerojatno služi kao korak kako bi se zarazila Field PG[3] računala. Ključno zaraženo računalo vjerojatno nije imalo pristup Internetu tako da su sve potrebne funkcionalnosti za sabotažu sustava ugrađene izravno u Stuxnet izvršnu datoteku. Ažuriranje ove datoteke vrši se peer-to-peer metodom koju uspostavlja sam Stuxnet. Kada bi Stuxnet konačno pronašao pogodno računalo s instaliranim Step 7 programom on bi izmijenio kod na PLC-u. Stuxnet bi svoje modifikacije sakrio tako da je svaki pokušaj da se otkrije zaraženi PLC bio uzaludan.

Slika 1 *Siemens PLC i HMI[4]*

Figure 1 *Siemens PLC i HMI*

Iskorišten je sigurnosni propust kako bi se pristupilo podacima PLC-a, tj. iskorišten je sigurnosni propust u Siemensovom SCADA softveru za upravljanje PLC-om ("WinCC"), instaliranom na računalima koja su izravno povezani sa PLC-om. Najveća pogreška tih sustava bilo je to što su korisnička imena i zaporke za pristup bazi podataka bila ručno upisana u programskom kodu. Tako poslužena, nezaštićena korisnička imena i zaporke zlonamjerni program je jednostavno pročitao. Za daljnje širenje putem operacijskog sustava Windows korišteni su zero-day exploitovi[5] [3] kao što je bio LNK ikona koja se koristila za širenje putem USB-a ili print spooler. Za preuzimanje kontrole nad računalima korišteni su ukradeni certifikati računalnih tvrtki sa Tajvana.

4. Naučene lekcije

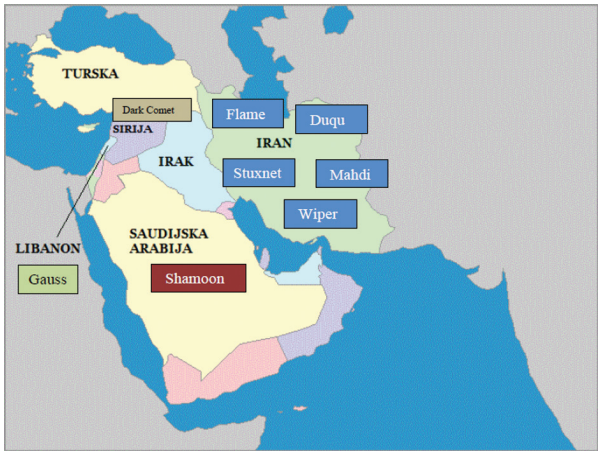
4. *Lessons learned*

Tvrtke koje se bave zaštitom informacijskih sustava, otkrile su vektore napada i vremenom su došle do vrlo zanimljivih informacija pa je osim Stuxneta otkriveno još nekoliko zlonamjernih

3 PG računala—specijalna računala koja služe samo za programiranje PLC-ova

4 HMI - human machine interface

5 Zero-day exploit – do tad nepoznate ranjivost



Slika 2 *Prikaz zaraženosti zlonamjernim programima po državama* [2]

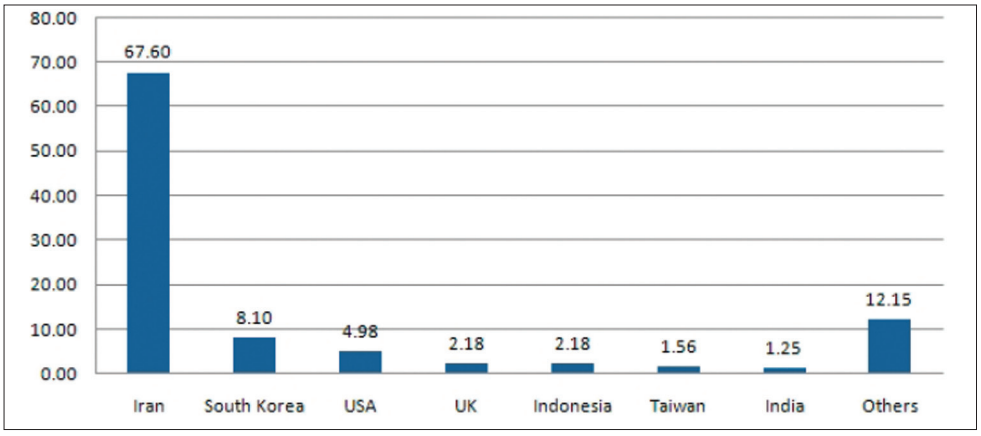
Figure 2 *Malware infection by a country* [2]

programa koji su također proizvedeni u cilju napada na računalno upravljane proizvodne sustave i infrastrukturu određenih zemalja. Stuxnet je otkriven u mnogim zemljama što možemo vidjeti na slikama 3. i 4.

U srpnju 2010. godine, Stuxnet je otkriven osim Irana u Maleziji i Indiji. Naziv je anagram nekih ključnih riječi pronađenih u kodu, a SAD i Izrael nisu nikad koristili ovaj naziv.

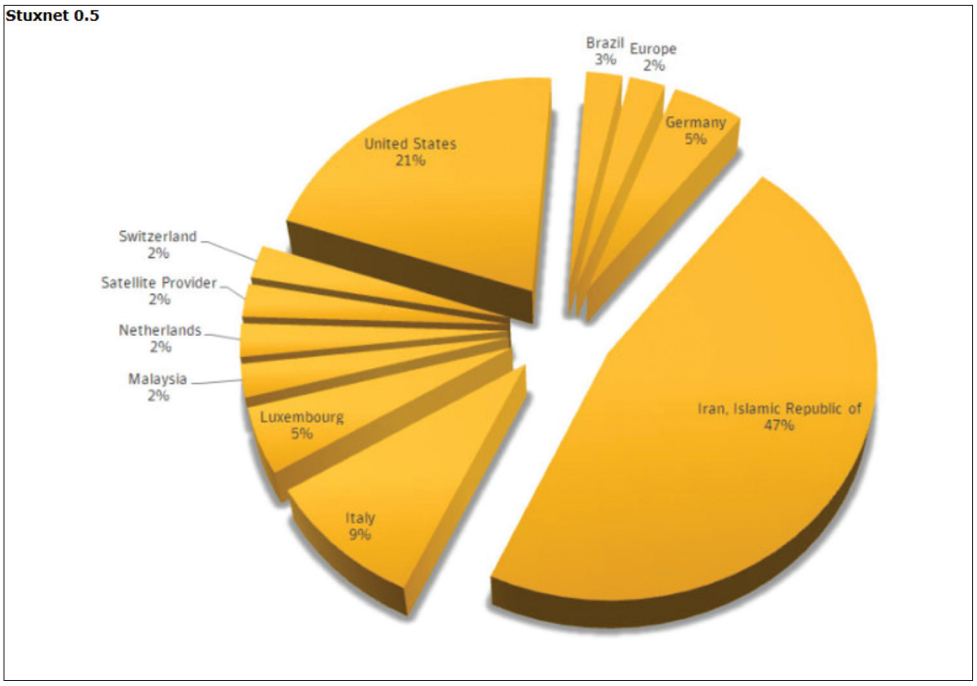
Navedeni primjer pokazuje cijeli niz propusta u sigurnosnom sustavu i politici sigurnosti, za koju možemo zaključiti ili da je nije bilo i je se nisu pridržavali. Kako se radilo o visokorizičnom industrijskom postrojenju u svakom pogledu, začuđuje količina propusta u sigurnosnom sustavu:

- Potpuno nepravilno rukovanje korisničkim imenima i šiframa – Politika sigurnosti



Slika 3 *Prikaz zaraženosti host računala sa instaliranim Siemens softverom po državama* [14]

Figure 3 *Infestations of a host computer with Siemens software installed by a country* [14]



Slika 4 *Pregled otkrivenih uspavanih infekcija Stuxnet 0.5 po zemljama* [9]

Figure 4 *Dormant infections detected in the past years* [9]

- Ne korištenje nikakvog mehanizma zaštite na korisničkom nivou (pametne kartice, kriptografija i sl.)
- Održavanje sustava nije rađeno jer računala nisu imala zakrpe
- Serviseri računala nisu provjeravani nije provjeravana njihova oprema – politika sigurnosti
- Spajanje na mrežu vanjskim računalima i prijenosnim diskovima – politika sigurnosti
- Upravljanje s podatkovnim medijima – politika sigurnosti
- Uvjerenje da je "air-gap" zaštita dovoljna
- Upravljanje podacima i zaštita podataka – politika sigurnosti
- Pristup mrežnim resursima iako su dijelovi mreže segmentirani
- Međusobno povezivanje segmenata mreže nije odrađeno na siguran način
- Zaštita od zlouporabe očito nije postojala i evidencija o zlouporabi nije postojala
- Kompletna politika upravljanja kontinuitetom poslovanja nije postojala
- Neadekvatna politika fizičke sigurnosti ili ne pridržavanje iste
- Neadekvatna politika zaštite osoblja i događanja ili ne pridržavanje iste
- Politika internih istraga – prve naznake nepravilnosti rada nisu dovele do aktiviranja

5. Zaključak

5. *Conclusion*

Razvojem digitalnih tehnologija i sveobuhvatnom povezanosti kao i porastom znanja i sposobnosti korisnika, za očekivati je nove načine i vještine za provedbu napadačkih digitalnih strategija. Budući ratovi mogli bi se voditi i pobjeđivati bez ispaljenog metka. Napadač može pritiskom gumba zatvoriti cjelokupnu nacionalnu infrastrukturu napadnute strane te kompletno kontrolirati ili uništiti njegovu infrastrukturu, postrojenja, komunikacijske mreže i sl. Drugim riječima čak i država bez sposobnosti izvršavanja konvencionalnog napada može pokrenuti kibernetički napad.
Ovakve prijetnje zahtijevaju razvoj i implementaciju novih Internet arhitektura otpornijih na kibernetičko ratovanje.
To bi podrazumijevalo kodiranje sa snažnim sigurnosnim elementima, znatno snažniji sustav kontrole upada, razvoj sigurnijih operacijskih sustava te izradu i striktno primjenjivanje politika sigurnosti. U pogledu informatičkog ratovanja Stuxnet predstavlja dosad najsloženije i najopasnije digitalno oružje ikad izrađeno. Prije otkrivanja Stuxneta, zlonamjerni programi koristili su se u svrhe hakiranja računala, ostvarivanja nelegalne zarade, dolaska do povjerljivih informacija ili iz razloga dokazivanja i sl. Ima primjera korištenja zlonamjernih programa tj. kibernetičkih napada od strane država na druge države, poput Rusije na Gruziju ili Čečeniju, Izraela na Palestinu i sl., ali ne u ovako kompleksnim operacijama. Stuxnet je pokazao kako se zlonamjerni računalni program može koristiti kao ofenzivno kibernetičko oružje i time je vjerojatno otvorena Pandorina kutija u pogledu mogućih terorističkih napada na ciljeve koji koriste SCADA ili slične sustave. U prilog tomu ide i izjava bivšeg ministra obrane Velike Britanije kako su nuklearne podmornice Trident ranjive na kibernetičke napade. [13]

6. Reference

6. *References*

[1] The State of the Art in Intrusion Prevention and Detection

[2] Zlonamjerni programi u službi država, NCERT-PUBDOC-2012-10-338

[3] Robert J. Turk, Cyber Incidents Involving Control Systems, U.S. Department of Homeland Security, US-CERT Control Systems Security Center, Idaho 2005.

[4] N. Falliere, L. O Murchu, E. Chien, W32. Stuxnet Dossier; Symantec Corporation, 2011.

[5] SCADA sustavi, FER predavanja 2013.

[6] A. Daneels and W. Salter, "What is SCADA?" in Proceeding of International Conference on Accelerator and Large Experimental Physics Control Systems, pp. 39–343, 1999.

[7] Nacrt prijedloga nacionalne strategije kibernetičke sigurnosti, Zagreb, ožujak 2015.

[8] How Stuxnet (PLC virus) spreads, A Study of Infection Paths in Best Practice Systems by: Eric Byres, P. Eng. ISA Fellow, Andrew Ginter, CISSP, Joel Langill, CEH, CPT, CCNA, 2011.

[9] Stuxnet 0.5: The Missing Link; Symantec Security Response, Veljača 2013. http://www.symantec.com/connect/blogs/stuxnet-05-missing-link (Pristupljeno 10.10.2015.)

[10] Obama Order Sped Up Wave of Cyberattacks Against Iran, The New York Times, By DAVID E. SANGER, June 1, 2012 http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=3 (Pristupljeno 19.10.2015.)

[11] David E. Sanger: Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power, Crown Publishing Group, New York 2012.

[12] Stuxnet Worm Crafted by U.S., Israel to Thwart Iran's Nuclear Program; Chloe Albanesius, 2012. http://www.pcmag.com/article2/0,2817,2405191,00.asp (Pristupljeno 20.10.2015.)

[13] http://www.theguardian.com/uk-news/2015/nov/24/trident-could-be-vulnerable-to-cyber-attack-former-defence-secretary-says (Pristupljeno 26.11.2015.)

[14] Nicolas Falliere, Liam O Murchu, and Eric Chien; W32.Stuxnet Dossier, Symantec Security Response, 02.2011.

AUTORI · *AUTHORS*

Marinko Žagar

Mr.sc. Marinko Žagar rođen je 1965. godine u Ražancu, a gimnaziju završava u Zagrebu. Nakon završene vojne akademije stiče zvanje mag.inž.elektrotehnike. Poslijediplomski znanstveni studij završava na Fakultetu organizacije i informatike 2006. godine u Varaždinu na temu Prijedloga uvođenja XML standarda u sigurnosnom sustavu grafičko izdavačkog poduzeća. Dugogodišnji je suradnik TVZ-a, a od ove godine zaposlenik, viši predavač na Informatičkom odjelu TVZ. Predaje na kolegijima vezanim za informacijsku sigurnost i poslovne informacijske sustave.

Korespondencija:
marinko.zagar@tvz.hr