

## **GENEZA, ŠIRENJE I ANATOMIJA KOMPJUTERSKOG CRVA *STUXNET***

## **GENESIS, EXPANSION AND ANATOMY OF COMPUTER WORM STUXNET**

**Gojko Grubor**

Univerzitet Singidunum, Danijelova 32, Beograd

Telefon: 062/577367

E-mail: [ggrubor@singidunum.ac.rs](mailto:ggrubor@singidunum.ac.rs)

**Bojan Marković**

Telefon: 061/6476550

E-mail: [bojanmarkovic88@gmail.com](mailto:bojanmarkovic88@gmail.com)

**Sažetak:** Predmet ovog rada je da približi i opiše suštinu, jednog od najmodernijih i najsavremenijih oružja takozvanog kibernetičkog rata, kompjuterskog crva *Stuxnet*. Opisane su osnovne karakteristike *Stuxnet*-a, a zatim analiziran proces *Stuxnet* napada, koji se realizuje infekcijom *Windows* sistema, *Step 7* softvera i PLC sistema. Navedene su mogućnosti i glavni ciljevi *Stuxnet*-a. Na kraju su predloženi njegovi potencijalni autori, njihovi razlozi, kao i eventualne posledice koje donosi ovo remek delo malicioznog programa.

**Ključne reči:** kibernetički rat, *Stuxnet*, PLC sistem, SCADA sistem

**Abstract:** The aim of this work is to clarify and describe the essence of one of the latest most modern weapon of the so called cyber war, the computer worm *Stuxnet*. Basic characteristics of *Stuxnet* are described, then, the process of *Stuxnet* attack, which is realized through the infection of *Windows* system, *Step 7* software and the PLC system, is analyzed. The possibilities and main goals of *Stuxnet* are stated. Finally, its potential authors are presented, as well as their reasons, and the consequences which this master piece of malicious program might bring.

### **1. UVOD**

Poznato je da najsavremeniji računari u kombinaciji sa neograničenim mogućnostima, ali i potencijalnim pretnjama Interneta, istovremeno predstavljaju najmoćniji alat, ali i oružje za zloupotrebe, kriminal pa i informaciono ratovanje. Stoga, ne bi trebalo da nas zbunjuje sve češća upotreba termina *CyberWar* (kibernetički rat) u medijima. Naime, *CyberWar* je u neverovatnoj ekspanziji, odvija se negde u pozadini Interneta i predviđa se da će u bliskoj budućnosti poprimiti globalne razmere i predstavljati primarni način ratovanja<sup>9</sup>. U okviru *CyberWar*-a, koriste se tehnološka sredstva kako bi se lansirali različiti tipovi napada, koji neretko mogu imati veoma konvencionalnu formu. *CyberWar* podrazumeva i napade na specifičnu opremu i infrastrukturu, što predstavlja veliki problem za industrijalizovane zemlje, koje se, u izvršavanju

---

<sup>9</sup> Izvor: EC Workshop, 3.11.2010; Beograd: „Krajem 2010 oko 120 zemalja u svetu je organizovalo jedinice za *CyberWar*; Kina ima 15000 ljudi angažovanih u ovom sktoru“.

mnogih zadataka, oslanjaju na računarsku podršku. Zbog lakoće napada malicioznim programom (malverom), potpuno je jasno zašto se klasični oblici ratovanja sve uspješnije prenose u računar. Trenutno, jedno od najmoćnijih oružja za industrijsku sabotažu i *CyberWar* predstavlja, visoko sofisticirani kompjuterski crv - *Stuxnet*.

## **2. GENEZA, ŠIRENJE I ANATOMIJA KOMPJUTERSKOG CRVA *STUXNET***

*Stuxnet* je prvi put identifikovan od strane kompanije koja se bavi zaštitom računarskih sistema, *VirusBlockAda*, sredinom juna 2010. godine. Međutim, prema izveštaju stručnjaka kompanije *Kaspersky Lab*, *Stuxnet* je počeo da se širi marta 2010. godine, a prva verzija ovog crva pojavila se juna 2009. godine, što je gotovo godinu ranije, u odnosu na početak pisanja medija o njemu. Potvrđen je i najnoviji napad *Stuxnet* crvom, gde su hakeri napadom na SCADA sistem za kontrolu vodovodne mreže u Springfield-u, Illinois (SAD) uništili pumpu za snabdevanje vodom<sup>10</sup> [6].

Zvanično istraživanje kompanije *Symantec*, o širenju *Stuxnet*-a, pokazalo je da su najugroženije zemlje u ranim danima infekcije: Iran (58,85%), Indonezija (18,22%), Indija (8,31%), Azerbejdžan (2,57%), SAD (1,56%), Pakistan (1,28%), ostale zemlje (9,2%) [5].

### **2.1 . Anatomija *Stuxnet* napada**

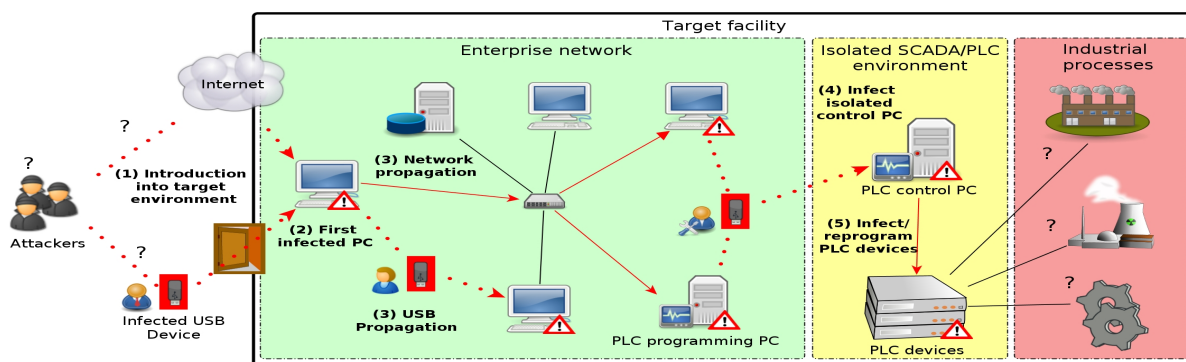
*Stuxnet* koristi višestepeni vektor napada za dostizanje krajnjeg cilja, odnosno upravljanja programabilnim logičkim kontrolerima – PLC-s (*Programmable Logic Controllers*), koji se koristi za kontrolu industrijskih procesa u okviru računarski kontrolisanih industrijskih sistema – ICS-s (*Industrial Control Systems*) [7].

Svakako, treba naglasiti da je *Stuxnet* veoma precizan. Naime, *Rootkit* ovog crva, dizajniran je originalno da napada isključivo sistem SCADA (*Supervisory Control and Data Acquisition*), proizveden od strane kompanije *Siemens*, tačnije deo kôda ovog sistema, koji se naziva *Operacioni blok 35*. Ova komponenta zadužena je za kontrolu procesa i očekuje brzinu odgovora za 100 milisekundi. Naravno, bilo koja, i najmanja izmena, može da dovede do katastrofalne eksplozije kontrolisanog sistema [1].

Na slici 1. prikazan je proces širenja *Stuxnet*-a i infekcije ciljnih sistema [7]. Naime, pretpostavlja se da proces sadrži pet faza: (1) crv je na izvestan način implementiran u ciljno okruženje (najverovatnije preko USB memorije, što još uvek nije zvanično potvrđeno); (2) nakon toga, inficira se prvi računar; (3) crv se dalje širi preko određenog tipa mreže (*Enterprise Network*), USB memorije i zaraženih fajlova iz projekta PLC programiranja; (4) crv se širi sve dok se ne inficira računar koji upravlja PLC sistemom; (5) otkrivanjem specifične kombinacije procesa operativnog sistema, kontrolnog softvera i PLC sistema, *Stuxnet* modifikuje softver za PLC programiranje i napokon inficira sam PLC sistem, čije se funkcionalnosti sada mogu lako modifikovati. Ovo se, potencijalno, može iskoristiti za manipulisanje fizičkim industrijskim procesima koje PLC uređaji kontrolišu.

---

<sup>10</sup> Kim Zetter, *H(ackers)2O: Attack on City Water Station Destroys Pump*, The Net Security News, 18.11.2011.



Slika 1. Faze Stuxnet napada [7]

Proces širenja *Stuxnet*-a može se, grubo, podeliti u dve faze, od kojih je svaka realizovana na osnovu različite funkcionalnosti crva. Prva faza predstavlja širenje crva u okviru jedne ili više različitih mreža, a druga faza predstavlja sam proces infekcije izolovanog industrijskog sistema. U drugoj fazi se pravi razlika između infekcije *Windows* računara korišćenih za programiranje i samih PLC uređaja, jer se upravo na taj način dobija interfejs između računarskih sistema i kontrolisanih industrijskih procesa, što i jeste krajnji cilj *Stuxnet*-a [7].

### 2.1.1 Infekcija *Windows* sistema

Takozvani, “trojanski deo” *Stuxnet*-a, sastoji se iz dva maliciozna drajvera, *mrxnet.sys* i *mrxcsl.sys*, koji se automatski kopiraju u direktorijum *System32/drivers* i na taj način se *Stuxnet* infiltrira na bilo koju *Windows* platformu. Odlično kreirana *Rootkit* komponenta, omogućava da *Stuxnet* „trojanac“ ostane potpuno neopažen, jer ga *Windows* operativni sistemi vide kao sistemski fajl [6].

Sledeća fazu napada predstavlja takozvani *zero-day-attack* (napad nultog dana). *Zero-day* predstavljaju ranjivosti *Windows* sistema, koje su poznate samo proizvođaču softvera, odnosno, nisu objavljene niti otkrivene od strane hakera. *Stuxnet* koristi nekoliko *zero-day* ranjivosti, gde se u početku prenosi preko zaraženih prenosnih drajvova, kao što su USB memorije, a nakon toga koristi druge ranjivosti i tehnike širenja, kao što je *peer-to-peer RPC*<sup>11</sup> (*remote procedure call*), kako bi se inficirali i ažurirali ostali računari iz lokalne mreže, koji nisu direktno konektovani na Internet.

Broj *zero-day Windows* ranjivosti, kombinovanih u *Stuxnet*-u, veoma je neobičan, jer krekeri gotovo nikada ne iskoriste četiri potencijalne ranjivosti sistema za napad jendog crva. Takođe, *Stuxnet* je neobično velik za maliciozne programe - zauzima više od pola megabajta, a interesantno je to da je pisan u nekoliko programskih jezika, uključujući C i C++, što je, opet, veoma neobično za kompjuterske crve koji se tipično pišu u jednom programskom jeziku [2].

### 2.1.2 Infekcija *Step 7* softvera

<sup>11</sup> RPC predstavlja inter-procesnu komunikaciju koja omogućava kompjuterskom programu da pokrene određenu proceduru koja bi se izvršila u drugom adresnom prostoru (na drugom računaru unutar deljene mreže), bez da programer prethodnim eksplicitnim kodovanjem dozvoli ovu udaljenu interakciju.

Prema rezultatima istraživanja nemačkog eksperta, *Ralfa Langnera*, jednom instaliran *Stuxnet* na bilo koju *Windows* platformu, inficira fajlove koji su deo *Siemens*-ovog WinCC/PCS 7 SCADA kontrolnog softvera (*Step 7*) i podriva ključnu komunikacionu biblioteku WinCC-a, koja se naziva *s7otbxdx.dll*. To omogućava da se presretne komunikacija između WinCC softvera, koji radi pod *Windows*-om i ciljnog *Siemens* PLC uređaja, koji može da se konfigurira pomoću softvera i programa, kada su ova dva sistema povezana kablom. Na taj način, crv može sam da se instalira na PLC uređaj potpuno neprimećen, a zatim maskira svoje prisustvo, ukoliko kontrolni softver WinCC sistema pokuša da iščita sve zaražene blokove memorije PLC sistema. Nakon toga, crv iskorišćava *zero-day* ranjivosti u WinCC/SCADA softveru baze podataka, koriseći formu jako kôdovane šifre za bazu podataka [6].

### 2.1.3 Infekcija PLC sistema uređaja

*Stuxnet* kôd u celosti još uvek niko nije objavio, što, svakako, ne čudi, ali poznato je da *Stuxnet* iskorišćava ranjivosti isključivo ciljnih SCADA konfiguracija koje ispunjavaju prethodno programirane zadate kriterijume. *Stuxnet* zahteva da specifični potčinjeni uređaji promenljive frekvencije (npr. konvertor frekvencije) bude povezan sa ciljnim *Siemens* S7-300 sistemom i njegovim udruženim modulima (slika 2). Napad se vrši na PLC sisteme sa uređajima promenljive frekvencije koji su prizvedeni od strane dva specifična proizvođača: *Vacon*, Finska i *Fararo Paya*, Iran. Nakon toga, prati se frekvencija povezanih motora i vrši napad isključivo na sisteme koji rade između 807Hz i 1210Hz. Industrijske primene motora sa ovim parametrima su brojne - raznovrsne pumpe, centrifuge gasa itd [1].

Treba naglasiti da se *Stuxnet* instalira u memorijski blok PLC sistema koji se naziva *DB890*, a koji posmatra *Profibus messaging bus*<sup>12</sup> sistema. Kada su ispunjeni određeni kriterijumi, dolazi do periodične modifikacije frekvencije na 1410 Hz, pa na 2Hz, pa na 1064 Hz i na taj način se utiče na rad motora povezanih na PLC sistem odnosno, menja se njihova rotaciona brzina. Takođe, automatski se instalira *Rootkit*, koji maskira i sakriva *Stuxnet* i ujedno modifikuje rotacionu brzinu sistema za nadgledanje [1].



Slika 2. Siemens Simatic S7-300 PLC kontroler

<sup>12</sup> *Profibus (Process Field Bus) messaging bus* predstavlja standard za komunikaciju u automatizacionoj tehnologiji.

## 2.2 Potencijalni autori *Stuxnet*-a

Kao što je već pomenuto, *Stuxnet* se po mnogo čemu razlikuje od ostalih malvera. Osim što predstavlja najsofisticiraniji kompjuterski crv, njegov glavni cilj je potpuno drugačiji u odnosu na „obične“ malvere. Takođe, predstavlja „najteži“ kompjuterski crv i pisan je u nekoliko programskih jezika, pa stručnjaci smatraju da je na njemu morala raditi čitava grupa ljudi, iza koje stoji veoma jaka organizacija.

Takođe, prethodno je pomenuto da se gotovo 60% računara zaraženih *Stuxnet*-om nalazi u Iranu (nešto više od 30.000). S tim u vezi, jasno je da je ovaj neverovatan kompjuterski crv imao svoju specifičnu metu – centrifuge koje rotiraju nuklearne materijale u iranskim postrojenjima za obogaćivanje uranijuma. Naime, vašingtonski Institut za nauku i internacionalnu bezbednost (*Institute for Science and International Security*), pretpostavlja da bi *Stuxnet* mogao biti zaslužan za isključivanje 1.000 centrifuga u iranskom glavnom nuklearnom postrojenju, Natanzu, 2010. godine. Nakon kratkog vremena, iranska Internacionalna agencija za atomsku energiju (*International atomic energy agency*) objavila je da je Iran suspendovao rad na jednom svom nuklearnom postrojenju, iz nepoznatih razloga. Ceni se da je ovim napadom nuklearni program Irana vraćen unazad za dve-tri godine. Sumnja se da je upravo *Stuxnet* razlog tome [4,3].

Mnogi ugledni stručnjaci smatraju da je suština generisanja *Stuxnet*-a upravo za veoma inteligentnu i moćnu operaciju protiv Irana. Na osnovu iznetih podataka, mnogih saznanja i istraživanja, pojavile su se, svakako, špekulacije o tome ko stoji iza *Stuxnet*-a. Ne postoje bilo kakvi dokazi, ali dve zemlje na koje se najviše sumnja su Izrael i SAD. Izrael se dovodi u vezu, pre svega zbog političkih sukoba sa Iranom, a nakon toga i zbog podataka da se u izvornom kôdu *Stuxnet*-a, mogu pronaći određene reference koje su usko povezane sa jevrejskom Biblijom. Takođe, sve češće su i špekulacije da je izraelska obaveštajna služba (*Mossad*) odgovorna za kreiranje *Stuxnet*-a. Sa druge strane, nemački ekspert za bezbednost informacija i informacionih sistema, *Ralf Langner*, kaže: „Moje mišljenje je da je *Mossad* umešan, ali da vodeća sila nije Izrael. Dakle, vodeća sila koja stoji iza svega je kibernetička supersila. Postoji samo jedna, a to je SAD, na sreću. Na sreću, jer u suprotnom, naš problem bi bio čak mnogo veći.“<sup>13</sup> [3,8]

## 3. ZAKLJUČAK

U slučaju visoko sofisticiranog crva *Stuxnet* možda, najvažnije pitanje nije *ko je kreirao Stuxnet*, već *ko će ga redizajnirati* i ponovo ugroziti industrijske sisteme na nepoznat način. *McAfee* Laboratorja je primila od nezavisnog tima istraživača novu verziju *Stuxnet* crva pod nazivom *Duqu*, sa gotovo identičnim programom, ali sa ciljem za industrijsku špijunažu i ciljane napade. Na sajtove kao što su sertifikaciona tela (CA) za infrastrukturu sa javnim ključem (PKI)<sup>14</sup>. Poznato je da evolucija tehnoloških dostignuća napreduje neverovatnom brzinom. Naime, crv koji može da sruši električnu mrežu ili uništi naftovod ili nuklearnu centralu, nakon samo devet meseci od svoje prve detekcije, potpuno je dostupan na Internetu, gde ga može preuzeti i istraživati bilo ko. Zahvaljujući tome, postoji veliki broj analiza i interpretacija

---

<sup>13</sup> Izvor: dostupno na <http://www.sweetsspeeches.com/s/1792-ralph-langner-cracking-stuxnet-a-21st-century-cyber-weapon>

<sup>14</sup> Izvor: The Net Security News, 21.12.2011.

*Stuxnet*-a dostupnih na Internetu. On je, zasigurno, *open source* oružje i ne postoji mogućnost da se zna ko će ga i u koje svrhe koristiti u budućnosti.

## LITERATURA

- [1] Eric D. Knapp, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, First Edition, Syngress, Waltham, 2011.
- [2] Jackson C. Rebane, *The Stuxnet Computer Worm and Industrial Control System Security*, Nova Science Pub Inc, 2011.
- [3] Mark Bowden, *Worm: The First Digital World War*, First Edition, Atlantic Monthly Press, New York, 2011.
- [4] Richard A. Clarke, Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, First Edition, Ecco Publishing, New York, 2011.
- [5] Nicolas Falliere, Liam O Murchu and Eric Chien, *W32.Stuxnet Dossier Version 1.4*, Symantec Security Response, February 2011.
- [6] Aleksandr Matrosov and all, *Stuxnet Under the Microscope*, Revision 1.31, Virus Laboratory, ESET, [www.wswr.com](http://www.wswr.com), 2011.
- [7] Martin Brunner and all, *Infiltrating Critical Infrastructures with Next-Generation Attacks; W32.Stuxnet as a Showcase Threat*, Fraunhofer SIT, 17.12.2011.
- [8] b92 (08.10.2010.): „Izraelski cyber rat“, (pristup 14.01.2012.), [dostupno na [http://www.b92.net/tehnopolis/aktuelno.php?nav\\_id=464039&fs=1](http://www.b92.net/tehnopolis/aktuelno.php?nav_id=464039&fs=1)];