CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Stuxnet – malver za cyber rat

NCERT-PUBDOC-2011-03-324

Nacionalni CERT

Sadržaj

1 Uvod

Zasigurno ste u životu pogledali barem jedan znanstveno-fantastični film u kojem se pojavljuje nekakav oblik računalnog virusa koji je toliko moćan da npr. dovodi do uništenja špijunskog postrojenja ili koji na neki drugi način uspije oštetiti nešto opipljivo. Upravo je Stuxnet, crv koji je zadnjih nekoliko mjeseci podigao puno prašine, uspio napraviti taj skok iz virtualnog u realni svijet.

Računalni crv Stuxnet, otkriven je u lipnju 2010. Riječ je o jednom od najsloženijih oblika malvera koji se ikad pojavio, a namjena mu je reprogramiranje rada specifičnih industrijskih postrojenja. Glavne mete su mu sustavi za kontrolu rada koji koriste upravljačke sklopove utemeljene na PLC-u (engl. *Programmable Logic Controller*). Takvi sustavi koriste se u plinovodima i elektranama. Stuxnet, koji se sastoji od niza vrlo složenih komponenti, koristi prvi PLC rootkit u povijesti, odnosno prikriva svoje aktivnosti (izmjene koda) unutar samog PLC-a. Nadalje, Stuxnet ima dvostruku prirodu, odnosno za širenje koristi sveprisutne operacijske sustave Windows (ekspanzivna priroda), dok mu je meta zapravo vrlo specifična. Ta činjenica jedan je od glavnih razloga zašto je crv znatno vrijeme (nekoliko mjeseci) ostao neotkriven.

Većina otkrivenih zaraženih računala nalazi se u Iranu, a analize su pokazale da su izgledne mete Stuxneta bila tamošnja nuklearna postrojenja, što je automatski povuklo niz špekulacija. Iranski predsjednik Ahmadinejad je potvrdio da je nuklearni program zemlje zaista pretrpio štetu [5]. Nadalje, stručnjaci procjenjuju da potrebne resurse za izradu ovako kompleksnog softvera, može imati samo neka nacija, odnosno vlada. Također je procijenjeno [4] da je potrebno 10 čovjek-godina samo za izradu programskog koda (ne uključujući golem posao testiranja na industrijskim postrojenjima itd.). Za izradu bi također bilo potrebno imati projektnu dokumentaciju postrojenja, odnosno mete pošto svaki industrijski sustav ima svoje specifične karakteristike.

Ovaj dokument razmatra samo tehničke aspekte malvera.

2 Kronologija, ranjivosti i mete

2.1 Kronologija događaja

Bjeloruski proizvođač anti-virusnih rješenja, VirusBlokAda [1], 17. je lipnja 2010., otkrio malver koji će kasnije bit nazvan Stuxnet. Ista tvrtka je tad upozorila na .LNK ranjivost operacijskih sustava Windows, ali Microsoft tada, kao i većina sigurnosnih tvrtki, nije reagirao. Daljnji tijek događaja naveden je u tablici:

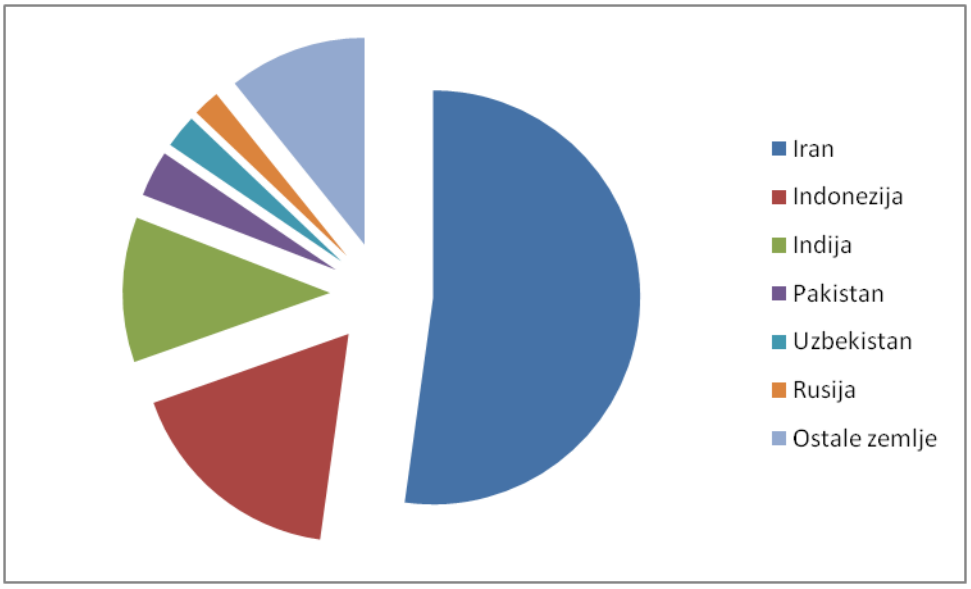
Tabela 1: kronologija događaja vezanih uz Stuxnet

24.6.2010.	Tvrtka Realtek Semiconductor obaviještena kako joj je ukraden digitalni certifikat
14.7.2010.	Siemens izdao obavijest o malveru kojem su meta industrijski sustavi koji koriste njegov softver WinCC
15.7.2010.	- Krebs upozorava da malver pogađa kontrolna postrojenja - US-CERT i ICS-CERT izdaju preporuke
16.7.2010.	Microsoft izdaje sigurnosnu preporuku 2286198 (kasnije MS10-046) za .LNK (Shortcut) ranjivost
17.7.2010.	VeriSign poništava ukradeni certifikat tvrtke Realtek Semiconductor
19.7.2010.	- SANS izdaje preporuku o .LNK ranjivosti - Siemens daje dodatne informacije o WinCC problemu - otkriveno kako Stuxnet koristi još jedan ukradeni certifikat (JMicron)
22.7.2010.	VeriSign poništava ukradeni certifikat tvrtke JMicron
2.8.2010.	Microsoft napokon izdaje zakrpu koja otklanja .LNK ranjivost (MS10-046)
6.8.2010.	Symantec izvijestio kako Stuxnet može ubaciti i sakriti kod u PLC-ima i tako utjecati na rad industrijskih postrojenja
14.9.2010.	Microsoft izdaje zakrpu koja otklanja ranjivost servisa Print Spooler (MS10-061) koju također koristi Stuxnet
12.10.2010.	Microsoft otklanja win32k.sys ranjivost (MS10-073)
14.12.2010.	Microsoft otklanja ranjivost u servisu Task Scheduler (MS10-092)

Još krajem 2008., otkrivena je varijanta trojanskog konja Zlob koja je koristila navedenu .LNK ranjivost [2]. U travnju 2009., Hakin9, časopis za računalnu sigurnost, objavio je članak o ranjivosti servisa Printer Spooler i korištenju iste za izvršavanje proizvoljnog programskog koda. Prve inačice Stuxneta nisu koristile .LNK ranjivost niti ukradene digitalne certifikate za potpisivanje lažnih upravljačkih programa., a uočene su u lipnju 2009. [2].

2.2 Rasprostranjenost

Statistička raspodjela otkrivenih zaraženih računala prema zemljama (podaci iz kraja rujna 2010.) [3], prikazana je na grafikonu slike 2.1. Više od polovice (52.2%) zaraženih računala nalazilo se u Iranu, slijede druge dvije azijske zemlje, Indonezija (17.4%) te Indija (11.3%). Većina zaraženih računala nalazi se u istoj regiji, što može upućivati da se tamo nalazi meta, ali se ti podaci moraju uzeti s oprezom zbog Stuxnetove prirode masivnog širenja i činjenice da u navedenim zemljama sigurnosna zaštita nije na razini kao na zapadu. Također, točne informacije o zaraženosti računala koji koriste softver tvrtke Siemens za upravljanje SCADA sustavima, nisu dostupne.



Slika 2.1: rasprostranjenost crva Stuxnet prema zemljama

2.3 Iskorištene ranjivosti u Windowsima

Stuxnet je za svoje uspješno djelovanje, odnosno širenje i dobivanje potrebnih privilegija na operacijskim sustavima Windows, iskoristio ukupno pet ranjivosti različitih inačica Microsoftovog operacijskog sustava. Tri od njih je crv iskoristio za svoje širenje, a dvije za povećanje privilegija koje su mu bile potrebne za izvršavanje zlćudnog koda. Ranjivost servisa Server (MS08-067) nešto je starija i Microsoft ju je ispravio još 2008. godine, a Stuxnet je koristi za širenje u lokalnoj mreži putem dijeljenih direktorija. Zanimljivo je da istu ranjivost koristi i poznati računalni crv Conficker. Tablica daje pregled svih ranjivosti Windowsa koje koristi Stuxnet.

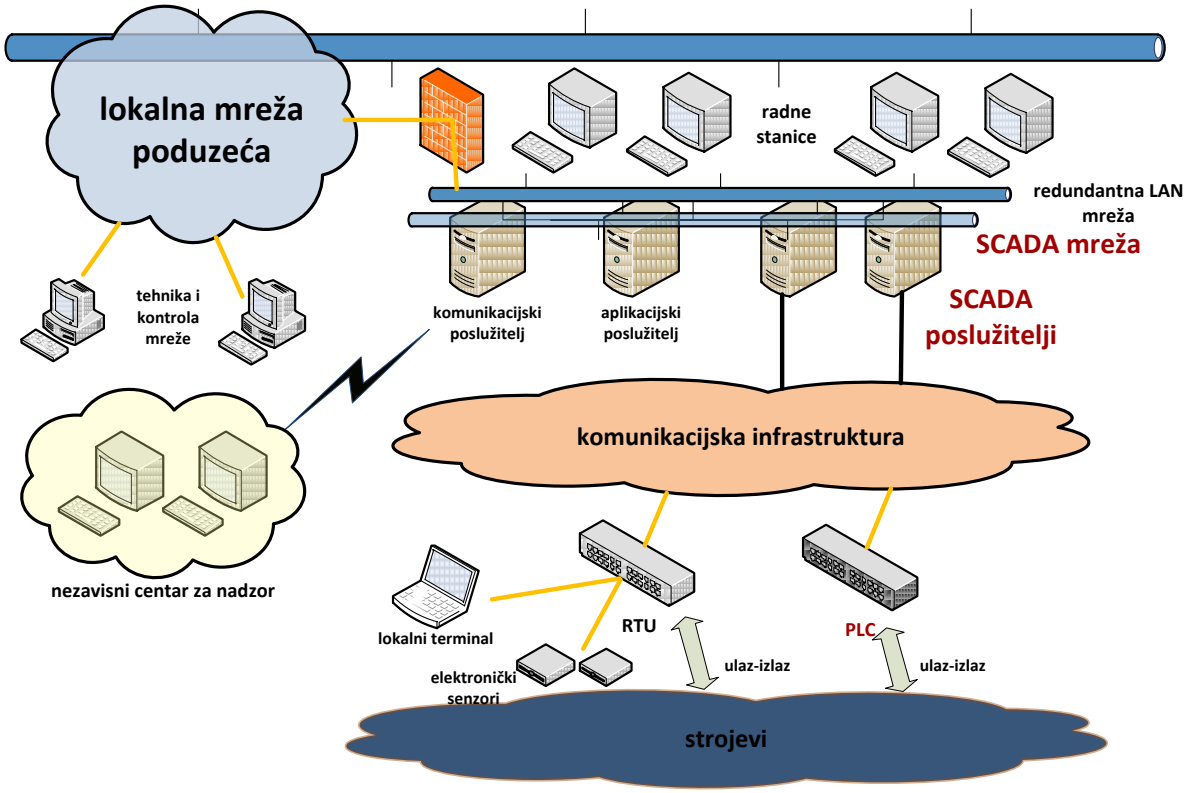
oznaka ranjivosti (Microsoft / MITRE)	MS08-067 CVE-2008-4250	MS10-046 CVE-2010-2568	MS10-061 CVE-2010-2729	MS10-073 CVE-2010-2549 CVE-2010-2743 CVE-2010-2744	MS10-092 CVE-2010-3338
pogođene inačice operacijskog sustava Windows	**SVE prije Win 7**	**SVE**	**SVE**	**2000 i XP**	**Vista i 7**
datum službenog otklanjanja	**23.10.2008.**	**2.8.2010.**	**14.9.2010.**	**12.10.2010.**	**14.12.2010.**
gdje se nalazi ranjivost	**servis Server**	**.LNK (Shortcut) ikone**	**servis Print Spooler**	**win32k.sys**	**servis Task Scheduler**
za što je Stuxnet koristi	**širenje u lokalnoj mreži**	**širenje putem prijenosnih USB uređaja (memorija)**	**širenje u lokalnoj mreži**	**povećanje privilegija**	**povećanje privilegija**
kod za ljusku napisan u više razina	**DA**	**NE**	**NE**	**DA**	**NE**
omogućuje udaljene napade	**DA**	**DA**	**samo za XP**	**NE**	**NE**

2.4 SCADA sustavi i PLC

SCADA je skraćenica od „Supervisory Control and Data Acquisition“, odnosno riječ je o računalnim sustavima za nadzor i upravljanje industrijskim, infrastrukturnim procesima i postrojenjima. To uključuje elektrane, tvorničke strojeve, pumpe za naftu, vojne instalacije itd. SCADA sustav obično se sastoji od sljedećih komponenti:

- HMI (*Human-Machine Interface*) – sučelje preko kojeg čovjek upravlja procesima na strojevima
- nadzornog računalnog sustava koji prikuplja podatke i šalje naredbe za upravljanje procesima
- RTU (*Remote Terminal Unit*) – sklopovi povezani na senzore i koji informacije iz njih pretvaraju u digitalni oblik i šalju nadzornim sustavima
- PLC (*Programmable Logic Controller*) – koriste se „na terenu“ umjesto RTU sklopova zbog svoje fleksibilnosti, raznovrsnosti, veće mogućnosti konfiguriranja i cijene
- komunikacijske infrastrukture koja povezuje RTU sklopove i nadzorne sustave

Važno je naglasiti kako, po svojoj definiciji, SCADA sustavi ne upravljaju procesima u stvarnom vremenu nego samo koordiniraju njima. Također, SCADA sustavi nisu procesno-orijentirani, nego orijentirani prema prikupljanju podataka, odnosno događajima (promjenama stanja koja se očitavaju iz prikupljenih podataka). U novije vrijeme, razvojem tehnologije koja omogućuje veće brzine (kapacitet) u komunikacijskim sustavima, SCADA sustavi se prema funkciji približavaju raspodijeljenim sustavima za upravljanje (DCS) koji imaju različite osobine od navedenih. Slika 2.2 prikazuje primjer SCADA arhitekture.



Slika 2.2: primjer SCADA arhitekture

PLC-ovi (slika 2.3) su digitalna računala koja se koriste pri automatizaciji sklopova u raznim industrijama. Za razliku od osobnih računala, dizajnirana su tako da u različitih uvjetima (neovisno o temperaturi, šumu, vibracijama itd.) mogu proizvesti isti niz izlaznih vrijednosti (rezultata) na temelju ulaznog niza. Važna osobina PLC-a je da je riječ o stvarno-vremenskom uređaju, što znači da su njegovi rezultati ovisni i o vremenu dolaska ulaznih podataka. Svoje rezultate PLC-ovi pohranjuju na neizbrisivu memoriju (npr. EPROM).

Slika 2.3: industrijski PLC

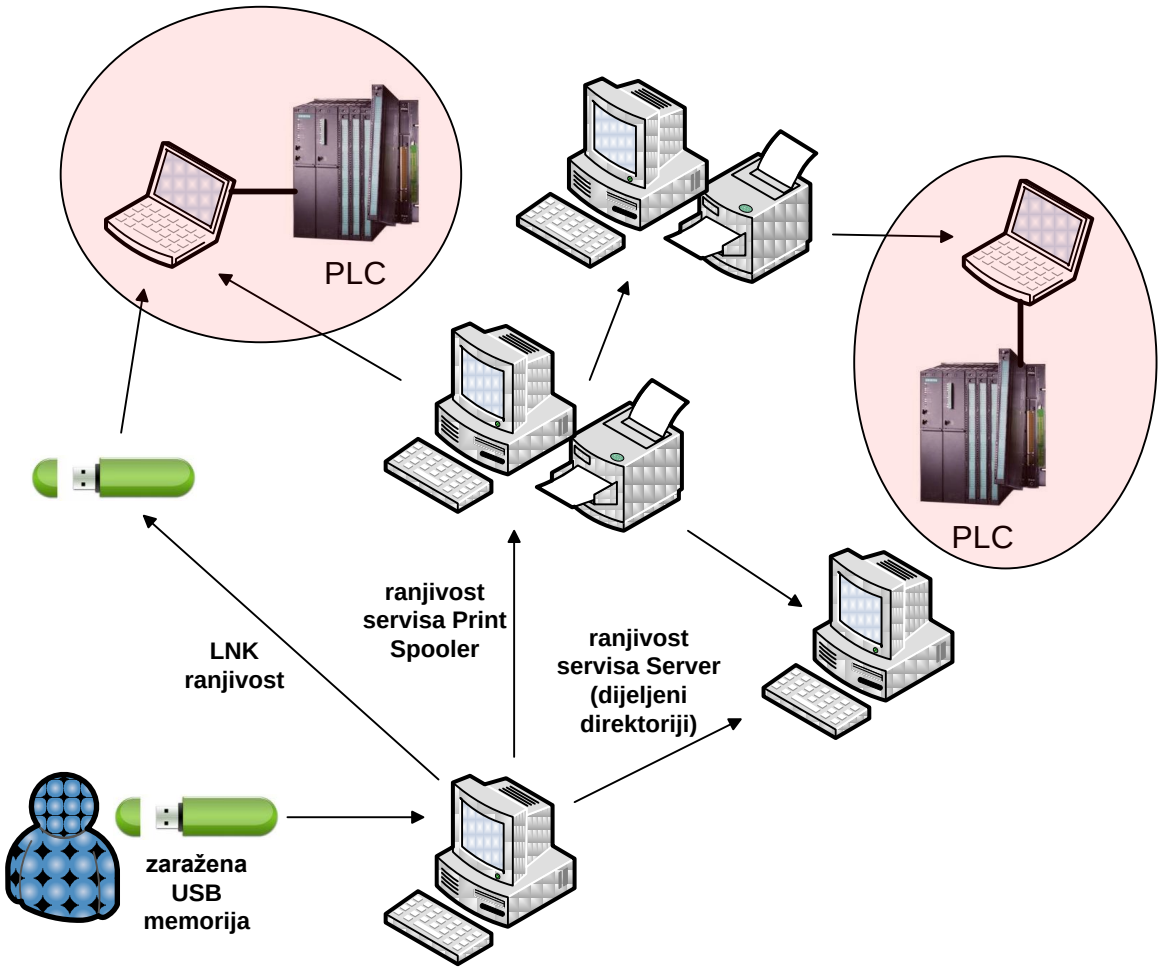
2.5 Ranjivosti SCADA i PLC sustava

PLC-ovi se obično programiraju putem računala (prikazanog na slici 2.4) sa Windows operacijskim sustavom koji nisu priključeni na Internet ili često bilo kakvu (pa i internu) mrežu. Iako je to sa sigurnosnog stajališta prednost, ipak postoji jedan ozbiljni nedostatak, a to je neredovita nadogradnja takvih sustava novim inačicama operacijskih sustava i softvera zakrpama koje ispravljaju sigurnosne propuste. Upravo je taj nedostatak, odnosno ranjivost MS08-067, Stuxnet iskoristio za širenje u lokalnoj mreži. Navedena ranjivost je mnogo vremena prije pojave crva otklonjena, ali ne i na spomenutim računalima koji upravljaju PLC-ovima.
Siemens, jedan od glavnih proizvođača softvera i upravljača za SCADA sustave, našao se pod udarom Stuxneta. Naime, Siemens je u svoj softver za upravljanje PLC-ovima, SIMATIC PCS (inačice 7) i WinCC, upisao („hardkodirao“) korisnička imena i lozinke za pristup pozadinskim Microsoft SQL bazama podataka (ranjivost CVE-2010-2772). Navedene podatke koristi softver za internu komunikaciju sa bazom podataka. Ovu ranjivost je iskoristio Stuxnet za dobivanje potrebnih ovlasti. Primarni cilj crva je preko računala na kojima se nalazi navedeni softver i koja upravljaju Siemensovim PLC-ovima, poput modela Simatic PLC 101, reprogramirati rad izmjeničnih pretvarača visokih frekvencija koji upravljaju radom električnih motora i to onih od proizvođača Vacon (Finska) i Fararo Paya(Iran) [4]. Takvi motori se, između ostalog, koriste u centrifugama za obogaćivanje urana.

2.4: mete Stuxneta - PLC i računalo koje upravlja njime [2]

3 Arhitektura i način rada Stuxneta

Kao što je i spomenuto, Stuxnet ima vrlo složenu arhitekturu. Njegovu jezgru predstavlja velika DLL (*Dynamic Link Library*) datoteka koja sadrži više različitih funkcija (*exports*) i programskih dodataka (*resources*) koje funkcije koriste kako bi upravljale crvom. Svaka funkcija ima svoj zadatak, a ukupno ih je 32, dok je dodataka 15. Svaki puta kad se poziva neka od funkcija, Stuxnet ubacuje cijelu DLL datoteku unutar nekog drugog procesa i tada poziva tu funkciju. Također, Stuxnet može ubaciti kod u postojeći ili novopokrenuti proizvoljni proces ili u neki unaprijed odabrani proces. Ako koristi unaprijed odabrani proces, Stuxnet može koristiti programski kod unutar njega ili narediti procesu ubacivanje koda u neki drugi proces.
Ugrubo, arhitekturu Stuxneta, prema namjeni možemo podijeliti na tri glavna dijela: dio zadužen za instalaciju, dio zadužen za širenje i dio zadužen za komunikaciju s PLC-om.
Što se tiče metoda širenja (na računala sa Windowsima), Stuxnet koristi čak njih četiri [3], od kojih je najznačajnija ona putem USB prijenosnih medija. Ostale tri su: putem dijeljenih direktorija (*Network Shares*), putem RPC poslužitelja, odnosno ranjivosti te koristeći ranjivost servisa *PrintSpooler* namijenjenog mrežnom dijeljenju pisača. Slika 3.1 prikazuje model Stuxnetovog širenja i iskorištenih ranjivosti.



3.1: Stuxnetove metode širenja do krajnje mete

3.1 Širenje putem USB medija i instalacija

3.1.1 Ubacivanje crva putem USB memorije

Glavna metoda širenja (propagacije) Stuxneta je putem USB prijenosnih memorija (odnosno diskova). Kako bi to ostvario, crv je iskoristio već spomenutu .LNK ranjivost operacijskih sustava Windows. LNK je ekstenzija tzv. „shortcut" datoteka, odnosno prečaca prema izvršnim datotekama (aplikacija) u Windowsima. Računala koja upravljaju PLC-ovima, odnosno mete crva obično nisu mrežno povezana i jedini način izmjene podataka sa drugim računalima kojeg koriste su USB memorije.

Na USB mediju zaraženom Stuxnetom nalazi se sljedećih šest datoteka:

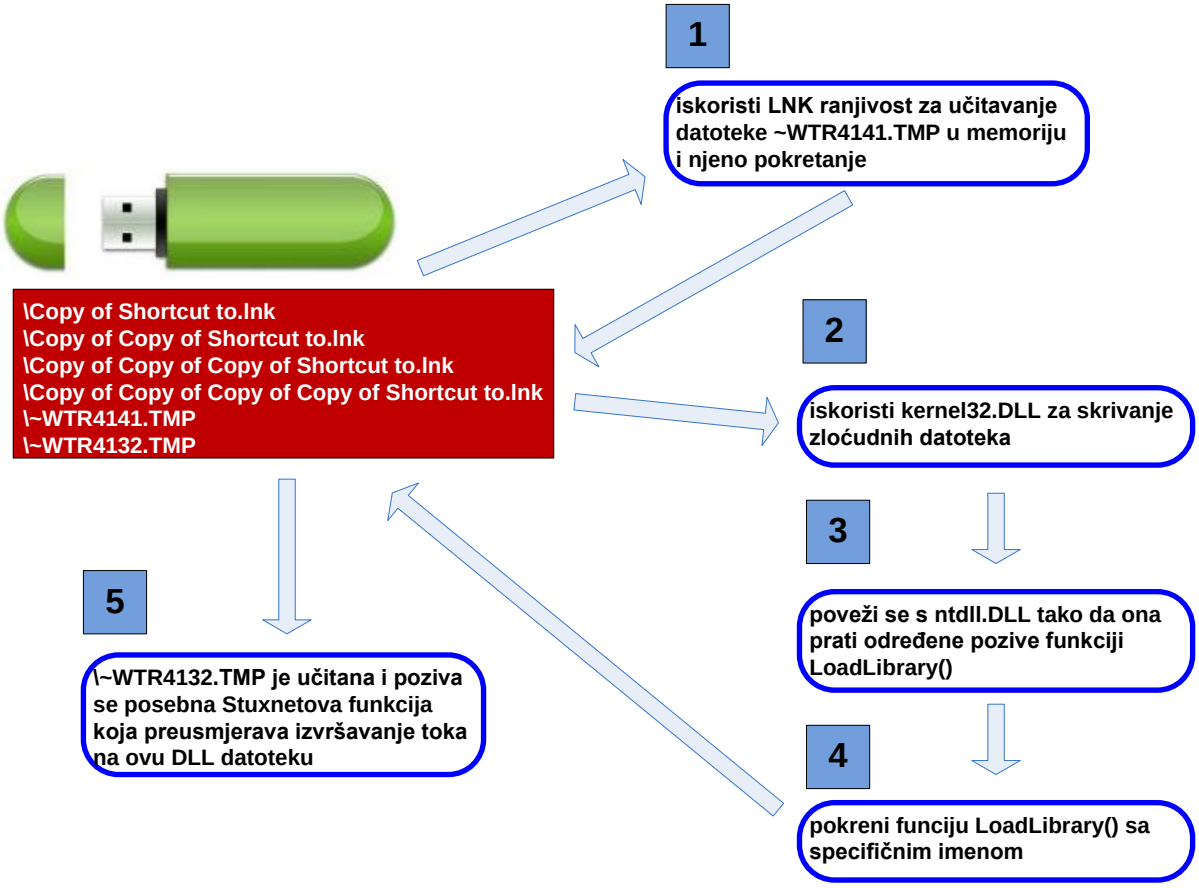
- **Copy of Shortcut to.lnk**
- **Copy of Copy of Shortcut to.lnk**
- **Copy of Copy of Copy of Shortcut to.lnk**
- **Copy of Copy of Copy of Copy of Shortcut to.lnk**
- **~WTR4141.TMP**
- **~WTR4132.TMP**

Kao što vidimo, prve četiri datoteke su sa ekstenzijom LNK i one iskorištavaju spomenutu ranjivost. Stuxnet koristi četiri posebne LNK datoteke, a svaka od njih na svoj način definira put (direktorije) do iste datoteke, naravno one koja se inicijalno pokreće, ~WTR4141.TMP. Razlog za to je što postoje razlike između inačica Windowsa i u tome koje će slovo operacijski sustav dodijeliti USB mediju. Time se crv osigurava da će bit izvršen na svim inačicama Windowsa.

Kada korisnik otvori zaraženi USB medij koristeći aplikaciju zaduženu za prikaz ikona za prečace, datoteka ~WTR4141.TMP se učitava te se poziva njezina početna funkcija. Ta datoteka je zapravo DLL datoteka kojoj je glavna svrha učitati drugu datoteku sa USB medija, ~WTR4132.TMP. Čim se dogodi učitavanje crva sa USB medija, on koristi ugrađene funkcija Windowsa (unutar DLL datoteka kernel32.dll i ntdll.dll) kako bi prikrio ranije navedene datoteke crva. Funkcije tako filtriraju prikazivanje svih datoteka unutar operacijskog sustava koje imaju sljedeća svojstva:

- datoteke imaju LNK ekstenziju i veličine su 1471 bajt
- datoteke imaju TMP ekstenziju, ime im se sastoji od 12 znakova (zajedno sa točkom i ekstenzijom) i to u formatu „~WTRabcd.TMP" gdje su a, b, c i d znamenke od 0 do 9 čiji je zbroj djeljiv sa 10 (odnosno zbroj po modulu 10 jednak je nuli)

~WTR4132.TMP je glavna instalacijska datoteka Stuxneta koja u obliku .stub datoteke pokreće funkciju 15, zaduženu za instalaciju malvera na računalo. Grafikon na slici 3.2 prikazuje slijed izvođenja nakon pokretanja zaraženog USB medija.



3.2: procedura ubacivanja crva putem USB memorije

3.1.2 LNK ranjivost

Takozvana LNK ranjivost (CVE-2010-2568) javnosti je bila poznata duže od mjesec dana, prije nego ju je Microsoft otklonio u kolovozu 2010. (**MS10-046**). Ranjivost tako elementarne funkcionalnosti u operacijskom sustavu bila je velika vijest u području računalne sigurnosti i veliki problem za Microsoftove programere, ali i za ugled tvrtke.
Sama ranjivost se nalazi u činjenici da ikone LNK datoteka za svoje učitavanje koriste CPL datoteke (*Control Panel File*) koje su ništa drugo nego dinamičke programske biblioteke (DLL). U formatu LNK datoteke nalazi se polje „*File Location Info*“ koje definira lokaciju sa koje se učitava CPL datoteka. Upravo se to polje moglo zlonamjerno izmijeniti tako da pokreće malver, odnosno u ovom slučaju instalaciju crva. Kada korisnik putem Windows Explorera otvori direktorij koji sadrži zloćudnu datoteku, pokreće se niz sistemskih funkcija od kojih posljednja *LoadLibraryW()* poziva DLL datoteku crva. Navedenoj se funkciji kao parametar prosljeđuje put do nekog modula i ranjivost je posljedica izostanka bilo kakve provjere puta do tog modula.

3.1.3 Instalacija crva

Nakon što Stuxnet provjeri koji i koja inačica operacijskog sustava je instalirana na zaraženom računalu, vrši provjeru je li postoje administratorska prava. Ako ne postoje, iskoristit će jednu od ranjivosti koje služe za povećanje privilegija, ovisno o inačici

operacijskog sustava Windows. U slučaju da je crv prethodno otkrio da je riječ o 64-bitnoj inačici operacijskog sustava, prekida svoje izvršavanje.
Slijedi pronalaženje procesa u koji će se crv ubaciti. Postoji skup unaprijed definiranih procesa koje Stuxnet koristi za izvršavanje svojeg programskog koda. To su:

- **lssass.exe**
- **winlogon.exe**
- **svchost.exe**
- **proces (otkrivenog) anti-virusnog softvera**

Prva tri procesa pripadaju operacijskom sustavu Windows, dok što se tiče procesa anti-virusnog softvera, crv otkriva koji je softver instaliran (i inačica) na zaraženome računalu i prema tome koristi neki od procesa navedenih u tablici:

instalirano anti-virusno rješenje	**proces (meta crva)**
Kaspersky AV v1 – v7	lsass.exe
Kaspersky AV v8 – v9	avp.exe
McAfee	winlogon.exe
AntiVir	lsass.exe
BitDefender	lsass.exe
ETrust v5 – v6	crv se ne uspijeva ubaciti u proces
ETrust ostali	lsass.exe
F-Secure	lsass.exe
Symantec	lsass.exe
ESET NOD32	lsass.exe
Trend PC Cillin	tmproxy.exe

Nakon toga slijedi pokretanja funkcije (export) 16 koja je glavni instalacijski dio Stuxneta. Funkcija pokreće provjere je li računalo već zaraženo i je li trenutni datum stariji od 24.6.2012. (crv se izvršava samo do toga datuma). Nadalje, funkcija instalira rootkit datoteke i ključeve za registar operacijskog sustava, ubacuje se u proces **services.exe** kako bi bio spreman dalje zaraziti prijenosne USB memorije, ubacuje se u procese Siemensovog Step 7 softvera, konfigurira parametre potrebne za komunikaciju između komponenti i spaja se na RPC poslužitelj. Zanimljivo je da postoji ključ u registru koji ako je postavljen u određenu vrijednost, sprečava Stuxnet da zarazi računalo. Riječ je o ključu „NTVDM TRACE“ na lokaciji KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \MS-DOS Emulation ako je postavljen u vrijednost „19790509“.

Slijedi stvaranje tri kriptirane datoteke, a to su:

- **Oem7a.pnf** – glavna DLL datoteka crva
- %SystemDrive%\inf**mdmeric3.PNF** – 90 bajtova velika datoteka
- %SystemDrive%\inf**mdmcpq3.PNF** – konfiguracijski podaci

Log datoteka nalazi se u: %SystemDrive%\inf**oem6C.PNF**. Ako se u (zaraženo) računalo putem USB-a umetne memorija koja sadrži Stuxnet, inačice navedenih kriptiranih datoteka uspoređuju se sa onima koji se nalaze na memoriji. Ako su one iste, nastavlja se izvršavanje, a inače se crv nadograđuje novijim inačicama. Nakon toga, Stuxnet otpakirava i dekodira dvije datoteka koje potom pohranjuje na disk. To su „**Mrxnet.sys**“ i „**Mxcls.sys**“.

Stuxnet mijenja vrijeme njihovog nastanka kako bi se izbjegla sumnja, a također unosi potrebne ključeve u registar kako bi se obje datoteke pokretali kao servisi. Prva datoteka služi za početno učitavanje crva, a druga za skrivanje datoteka koje pripadaju Stuxnetu, ali i za obnavljanje istih ako budu uklonjene.
Pri procesu instalacije, moguće je da crv ugasi procese **explorer.exe** i **S7tgtopx.exe**, naravno ako su oni pokrenuti. Specijalna funkcija služi za inficiranje svih Step7 projektnih datoteka. Zadnja stvar koju crv još čini je da se proba spojiti na RPC poslužitelj kojeg je prethodno uspostavila jedna od njegovih funkcija, a podatke o tome pohranjuje u svoju log datoteku.
Nakon cijelog procesa, Stuxnet je aktiviran u potpunosti.

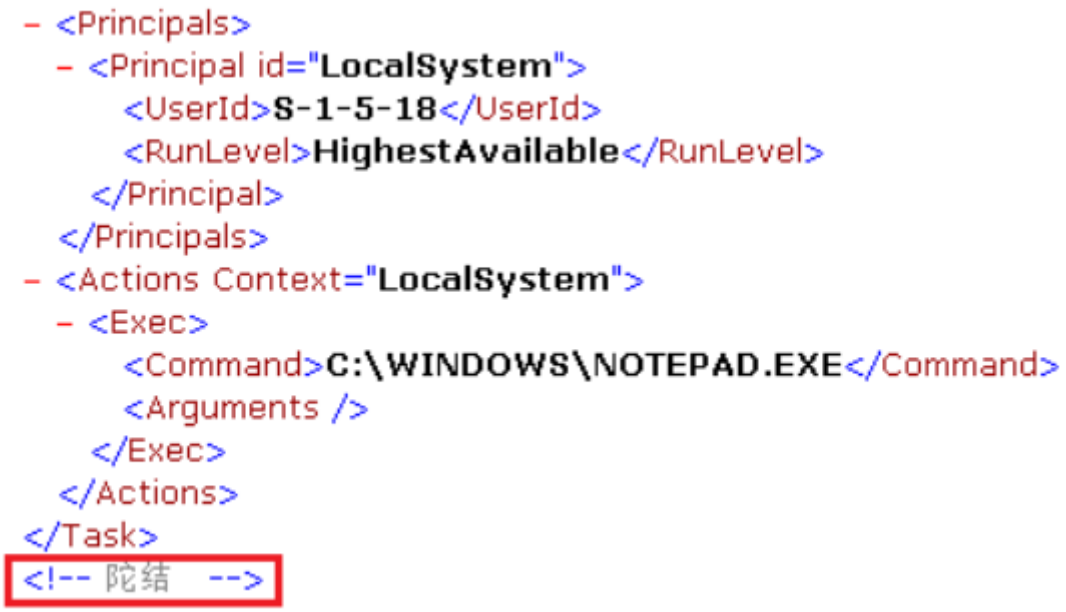
3.1.4 Povećanje privilegija

Kada crv nema dovoljne ovlasti, odnosno (administratorske) privilegije da se instalira, koristi jednu od dviju ranjivost za povećanje svojih privilegija, ovisno o inačici operacijskog sustava Windows.
Ako je riječ o Windows 2000 ili Windows XP (bez SP2 nadogradnje) sustavu, crv iskorištava tzv. Win32k.sys ranjivost (**MS10-073**). Time podiže razinu svojih ovlasti na „SYSTEM“ što mu omogućuje obavljanje bilo kojeg zadatka na lokalnom računalu. Kako bi iskoristio navedenu ranjivost, Stuxnet učitava posebno izrađenu datoteku predloška rasporeda tipki na tipkovnici (takva datoteka je zapravo DLL datoteka sa posebnom strukturom jednog dijela). Povećanje privilegija događa se prilikom odašiljanja primljenih znakova sa tipkovnice unutar modula **Win32.sys**. Prilikom obrade znakova sa tipkovnice putem funkcije *NtUserSendInput* izvršava se programski kod kojem je svrha odrediti na koji način operacijskom sustavu odaslati kodove pritisnutih znakova. Koristeći spomenutu datoteku predloška, crv pokreće funkciju *NtUserloadKeyboardLayoutEx* kojoj kao argument prosljeđuje memorijsku lokaciju koda kojeg treba izvesti sa SYSTEM ovlastima. Također, manipulira sadržajem registra *ecx* tako da u njemu definira pozivanje određene procedure (indeksa 5) za određene kodove znakova. Kako bi mogao izvršiti svoj zloćudni kod, crv alocira memorijski međuspremnik u koji ga pohranjuje.
Drugu ranjivost koju Stuxnet koristi za istu namjenu, koristi za inačice operacijskih sustava Windows Vista i Windows 7. Kao i kod prethodno spomenute ranjivosti, pomoću nje Stuxnet diže svoje ovlasti na razinu SYSTEM.
Ova vrlo ozbiljna ranjivost nalazi se u servisu **Task Scheduler** (**MS10-092**), odnosno njegovom načinu kontrole integriteta metapodataka koji opisuju vremenski raspored definiranih zadataka. Naime, u pogođenim operacijskim sustavima Task Scheduler izrađuje XML datoteku sa konfiguracijskim podacima za svaki registrirani zadatak. Datoteke te vrste obično se nalaze u direktoriju **%SystemRoot%\system32\Tasks** i sadrže podatke kao što su vrsta zadatka, put do izvršne datoteke, argumenti za naredbenu liniju, korisnički računi unutar kojih će se zadatak izvršavati, potrebne privilegije itd. Iako direktorij Task Schedulera mogu čitati samo lokalni administratori, XML datoteke koje opisuju zadatke mogu čitati svi osim onih sa „Guest“ ovlastima. Za zaštitu integriteta navedenih datoteka i sprečavanja korisnika da ih modificiraju, Task Scheduler računa zaštitnu sumu svaki puta kad se otvori novi zadatak. Kad je vrijeme za početak nekog zadatka, zaštitna suma se ponovno računa i uspoređuje sa originalom, a ako su one jednake, zadatak se izvršava. Nedostatak leži u tome što se pri računanju zaštitne sume koristi algoritam CRC32. Navedeni algoritam je dobar u otkrivanju nenamjernih pogrešaka (nastalih pogreškama prije prijenosu komunikacijskim kanalima), ali ne i onih namjernih kao u ovom slučaju. Naime, algoritam CRC32 ima linearna svojstva i vrlo je lako izraditi datoteku sa istom zaštitnom sumom kao i original. To je upravo ono što i Stuxnet čini.

Koraci koje Stuxnet čini su sljedeći:

- otvara novi zadatak koji će se izvršavati pod trenutnim korisničkim računom sa najvišim mogućim privilegijama
- čita konfiguracijsku XML datoteku zaduženu za otvoreni zadatak i računa njezinu CRC32 zaštitnu sumu
- modificira konfiguracijsku datoteku (iz 2. koraka) tako da ima istu zaštitnu sumu kao i originalna te postavlja sljedeća svojstva:
    a) Principal Id=LocalSystem (nadležni korisnik)
    b) UserId=S-1-5-18 (SID korisnika)
    c) RunLevel=HighestAvailable (privilegije)
    d) Actions Context=LocalSystem (sigurnosni kontekst)
- pokreće zadatak

Kako bi osigurao da nova konfiguracijska datoteka ima istu zaštitnu sumu kao i original, crv dodaje na kraj datoteke komentar (u obliku <!--XY-->) i računa XY tako da ima istu vrijednost zaštitne sume. Primjer takve manipulacije prikazan je na slici ispod.



3.3: način krivotvorenja konfiguracijske datoteke Task Managera (izvor: [3])

3.2 Udaljeno širenje i komunikacija

Nakon instalacije, Stuxnet putem protokola HTTP pokušava uspostaviti vezu sa kontrolnim (C&C) poslužiteljem kojem šalje prikupljene informacije o zaraženom računalu i njegovoj mreži.
Što se širenja tiče, osim širenja putem USB prijenosnih memorija, Stuxnet koristi još i nekoliko drugih metoda. Za sve metode udaljenog širenja zadužena je jedna programska funkcija, koja za svaku metodu sadrži podfunkciju, kojih je ukupno pet.

3.2.1 Komunikacija sa kontrolnim poslužiteljima

Putem porta 80 namijenjenom protokolu HTTP, Stuxnet uspostavlja vezu sa kontrolnim poslužiteljem kojem šalje određene prikupljene podatke. Zabilježene su dvije domene kontrolnih poslužitelja koje su se nalazile u Maleziji i Danskoj, no ubrzo su blokirane kako bi se spriječilo da crv dobija naredbe od napadača. Osim komunikacije, crv ima i sposobnost nadogradnje na ovaj način, no stručnjaci nisu pronašli ni jednu na ovaj način nadograđenu inačicu malvera. Neki od podataka koje Stuxnet prikuplja i šalje svojem kontrolnom poslužitelju su:

- inačica i podinačica operacijskog sustava
- inačica „Service Pack“ nadogradnje
- ime računala
- ime domene
- IP adrese svih sučelja

Prije slanja posebno oblikovanog podatkovnog sadržaja, crv provjerava je li postoji veza prema Internetu i to tako da šalje zahtjeve na web stranice www.windowsupdate.com i www.msn.com te ako je veza aktivna, izrađuje se paket. Podaci se kodiraju posebno pripremljenim algoritmom koji koristi ključ veličine 31 bajta i potom, koristeći GET metodu, šalju na jednu od domena kontrolnog poslužitelja.
Ova metoda vjerojatno je, prije otkrivanja Stuxneta, služila za preuzimanje nadogradnji i dodatnih alata.

3.2.2 P2P komunikacija

Komponenta crva zadužena za P2P komunikaciju radi tako da prvo na zaraženo računalo instalira RPC poslužitelja i klijenta. Kada crv zarazi računalo, instalira RPC poslužitelja i čeka uspostavu veza. Svako drugo zaraženo računalo unutar mreže, može se spojiti i provjeriti koja je inačica crva instalirana na dotičnom računalu. Ako je riječ o novijoj inačici, računalo šalje zahtjev za dohvaćanje novije inačice te se nakon toga izvršava nadogradnja. Ako je u pitanju obrnut slučaj, računalo šalje kopiju svojeg crva kako bi se na prvom računalu izvršila nadogradnja. Sam crv je DLL datoteka, tako da je potrebno da se prije slanja pretvori u izvršnu datoteku. To čini tako što jednu izvršnu datoteku, koja mu služi kao predložak, puni sa svim potrebnim podacima, uključujući najnovije konfiguracijske parametre i informacije o zaraženom računalu.
Na ovaj se način udaljena nadogradnja izvršava vrlo efikasno na svim zaraženim računalima u lokalnoj mreži.
Zbog činjenice, da je P2P mehanizam pogodan za lokalne mreže, Stuxnet ga ne koristi za komunikaciju sa kontrolnim poslužiteljima, nego samo kao alternativnu metodu širenja na računala koja nisu povezana na Internet, ali koja se nalaze u lokalnoj mreži i preko nje mogu komunicirati sa računalima koja su povezana na Internet, odnosno koja komuniciraju sa kontrolnim poslužiteljima.

3.2.3 Širenje u lokalnoj mreži

Jedan od načina na koji se crv širi lokalnom mrežom je koristeći ranjivost servisa **Print Spooler** (**MS10-061**). Računala koja imaju uključeno dijeljenje datoteka i pisača, ranjiva su

na ovaj napad. Ranjivost, koja pogađa i najnoviju inačicu Windowsa, omogućuje udaljenom korisniku, koji koristi „Guest“ pristup, pisanje unutar direktorija %SYSTEM%, za što naravno ne bi smio imati privilegije.

Napad se provodi u dvije faze:

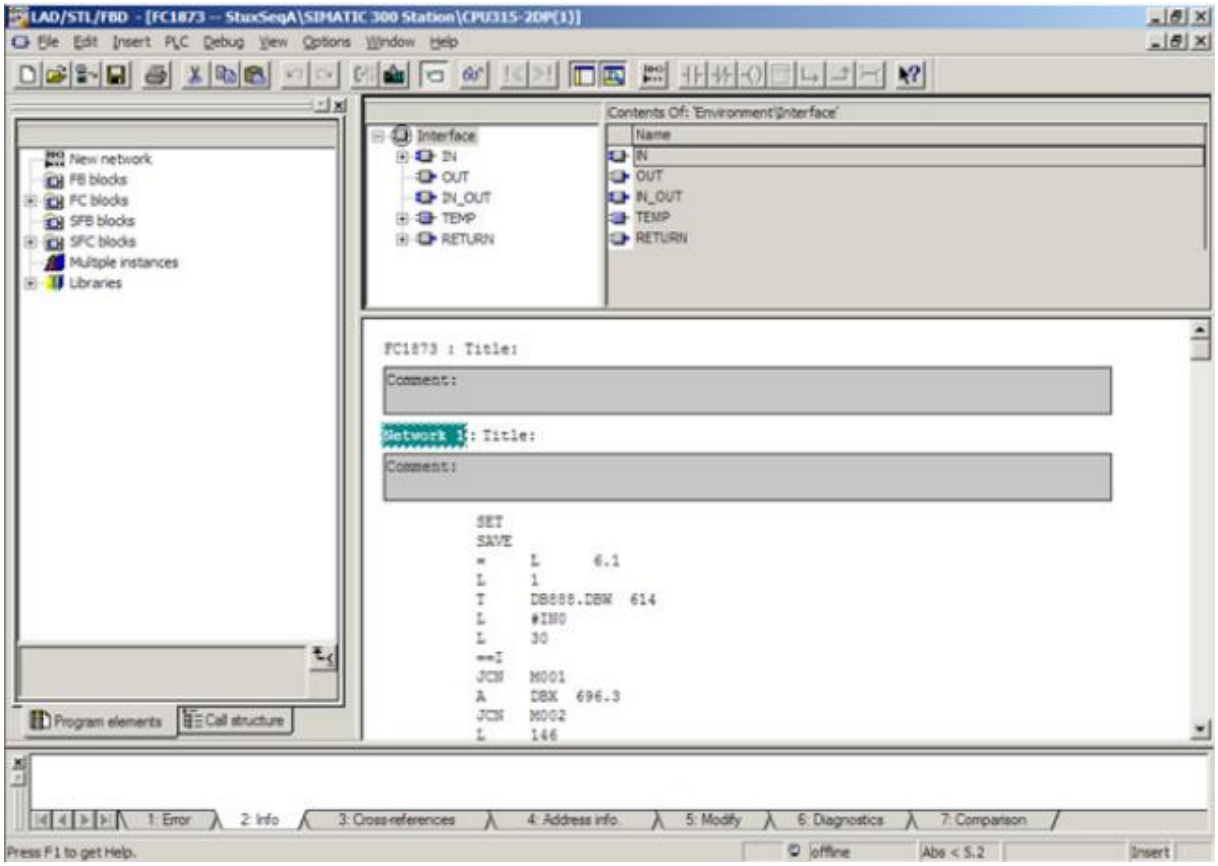
- tijekom prve faze, crv kopira sljedeće dvije datoteke u sistemski direktorij: Windows\System32**winsta.exe** i Windows\System32\wbem\mof**sysnullevnt.mof**
- tijekom druge faze izvodi se prva datoteka. Prilikom iskorištavanja ranjivosti, servis pogrešno „šalje“ dva dokumenta na ispis, a zapravo te dvije datoteke zapisuje u direktorij %SYSTEM%. Tijekom operacije, proces **spoolsv.exe** koristi API Windows funkciju StartDocPrinter().

Kod starijih inačica operacijskog sustava Windows, Stuxnet se može proširiti putem dijeljenih direktorija (*network shares*) koristeći zakazani zadatak (*scheduled job*) ili WMI (*Windows Management Instrumentation*). Crv provjerava sve korisničke račune na računalu i njegovoj domeni te isprobava postojeće mrežne resurse koristeći korisnikove povjerljive tokene ili WMI operacije unutar procesa explorer.exe kako bi se kopirao i pokrenuo na udaljenom računalu. Način rada je sljedeći: crv utvrđuje je li ADMIN$ dostupan kako bi definirao ime za dijeljenje glavne particije (obično C$), nakon toga se izrađuje izvršna datoteka crva koja uključuje najnoviju konfiguraciju i ona se šalje kao datoteka sa slučajnim imenom u obliku **DEFRAG[slučajni_skup_znakovaLNT].tmp**. Nakon toga se zakazuje mrežni zadatak koji će za točno dvije minute pokrenuti navedenu datoteku. Proces se odvija na isti načina ako se koristi WMI.
Za širenje na spomenuti način, Stuxnet koristi ranjivost označenu od Microsofta kao **MS08-67.** Po oznaci vidimo da je otklonjena još 2008. i prema tome ovaj slučaj najbolje pokazuje sigurnosni nedostatak računala nepovezanih na Internet, odnosno neredovite primjene nadogradnji (putem servisa *Windows Update*). Autori Stuxneta ciljano su iskoristili upravo ovu ranjivost računajući kako računala na terenu koja upravljaju PLC-ovima neće koristiti najnovije nadogradnje. Kao što je ranije spomenuto, istu ranjivost je iskoristio i poznati crv Conficker, no tehnički način na koji je Stuxnet koristi je mnogo sofisticiraniji, ali ovdje nećemo ulaziti u detalje.

3.2.4 Širenje na računala sa softverom WinCC

Posebna komponenta malvera zadužena je i za udaljeno povezivanje sa poslužiteljem na kojem je pokrenut softver za upravljanje bazom podataka, WinCC. Kada crv u lokalnoj mreži pronađe takav poslužitelj, za spajanje na bazu podataka koristi inicijalnu lozinku koja je upisana u programski kod Siemensovog softvera. Nakon spajanja izvodi dvije operacije: ubacuje zlođudni SQL kod koji crvu omogućuje da zarazi WinCC poslužitelj i modificira postojeće sučelje tako da dodaje programski kod koje se onda pokreće svaki puta kada se pristupa navedenom sučelju.
Nakon slanja upita o SQL konfiguraciji, Stuxnet šalje upit koji izrađuje novu tablicu i u nju pohranjuje određenu binarnu vrijednost. Ta vrijednost zapravo je heksadecimalni izvršni oblik glavne (DLL) datoteke crva skupa sa konfiguracijskim podacima. Ako je upit uspješno izveden, Stuxnet se iz baze podataka zapisuje na disk u datoteku **%UserProfile%\sql[slučajna_vrijednost].dbi**. Također se na disk pohranjuje CAB datoteka **GracS\cc_tlg7.sav** koja služi za pokretanje glavne DLL datoteke smještene na

lokaciji **GracS\c_alg.sav**. Kako bi ostao trajno pokrenut, Stuxnet se pomoću SQL koda upisuje kao procedura.



3.4: softver Step7

3.3 Komunikacija i upravljanje PLC-om

Softver WinCC/Step 7 (slika 3.4) koji služi za programiranje PLC-ova glavna je Stuxnetova meta. Nakon što zarazi računalo sa softverom WinCC, Stuxnet na njemu traži datoteke koje pripadaju WinCC/Step7 projektima. Ovisno o vrsti pronađenih datoteka, vrši potrebne preinake i dodatne instalacije kako bi dobio pristup svojoj glavnoj meti, PLC-u.

3.3.1 Inficiranje projektnih datoteka

U Stuxnet je ugrađena i komponenta koja služi za povezivanje određenih programskih sučelja koja se koriste za otvaranje projektnih datoteka softvera WinCC/Step 7 sa procesom **s7tgtopx.exe**. Taj proces je dio WinCC Simatic upravljačkog sklopa zadužen za upravljanje projektima. Crv modificira adresne tablice sljedećih datoteka:

- **s7apromx.dll**
- **mfc42.dll**
- **msvcrt.dll**
- **ccprojectmgr.exe**

Kad softver Step7 otvori (projektnu) datoteku sa ekstenzijom S7P ili MCP, poziva se funkcija koju je definirao Stuxnet, a ona poziva komponentu crva zaduženu za inficiranje direktorija unutar kojeg se projektna datoteka nalazi. Crv koristi datoteku **%Windir%\inf\oem6c.pnf** za pohranu podataka o lokaciji S7P i MCP datoteka.
Crv ima određene kriterije koje projekt mora zadovoljiti kako bi ga zarazio, a to su:

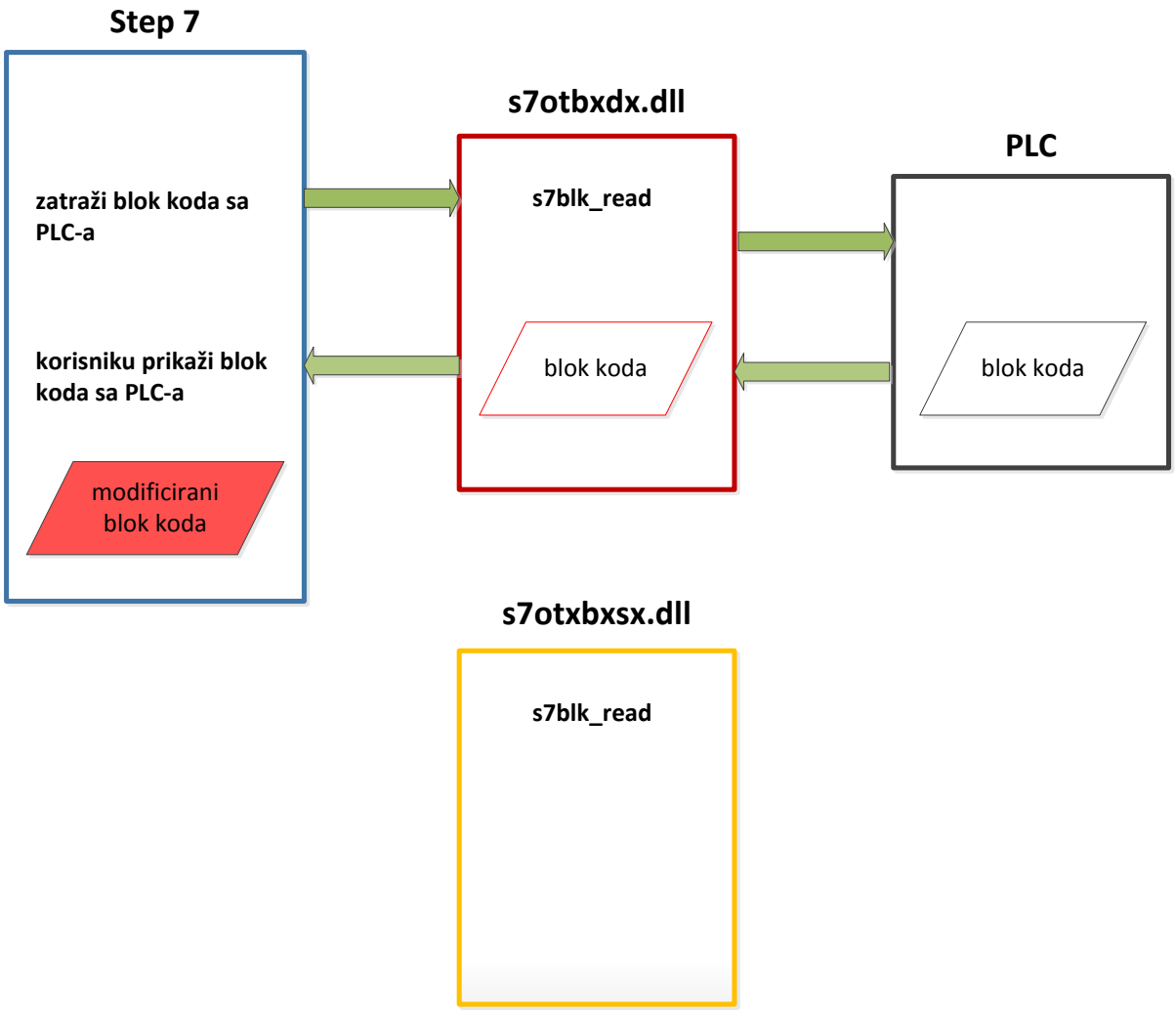
- nije prestar, odnosno mora biti korišten u posljednje 3 i pol godine
- sadrži direktorij „**wincproj**“ sa valjanom MCP datotekom (za slučaj pronađene S7P datoteke)
- sadrži direktorij „**GracS**“ koji uključuje barem jednu PDL datoteku (za slučaj pronađene MCP datoteke)
- nije primjer projekta koji dolazi sa softverom, odnosno crv zanemaruje sadržaj direktorija *\Step7\Examples\

3.3.2 Modificiranje PLC-a

Datoteku softvera WinCC/Step7, **s7otbxdx.dll**, Stuxnet mijenja sa svojom zloćudnom inačicom. Ta datoteka zadužena je za upravljanje zamjene programskih blokova između PLC-a i računala koje služi za programiranje PLC-a putem softvera Simatic. Zamjenom datoteke, Stuxnet može:

- pratiti blokove koda koje se pišu i čitaju sa PLC-a
- zaraziti PLC tako da ubaci svoje blokove koda ili zamijeni postojeće sa svojima
- prikrije činjenicu da je PLC zaražen (to je tzv. PLC rootkit)

Step7 programi (projekti) koriste programske rutine unutar spomenute datoteke s7otbxdx.dll. Tako se na primjer za čitanje blokova koda sa PLC-a koristi rutina **s7blk_read**. Operacija se izvodi tako da Stuxnet preimenuje originalnu datoteku s7otbxdx.dll (na zaraženom računalu) u **s7otbxsx.dll** te umjesto nje postavlja svoju. 93 od originalnih 109 programskih procedura odvija se normalno, dok preostalih 16, Stuxnetova DLL datoteka preusmjerava na sebe i obavlja modifikacije koda koji dolazi sa ili prema PLC-u. Operator ne može ništa posumnjati jer navedene rutine Stuxnet koristi i za prikrivanje svojeg zloćudnog koda.



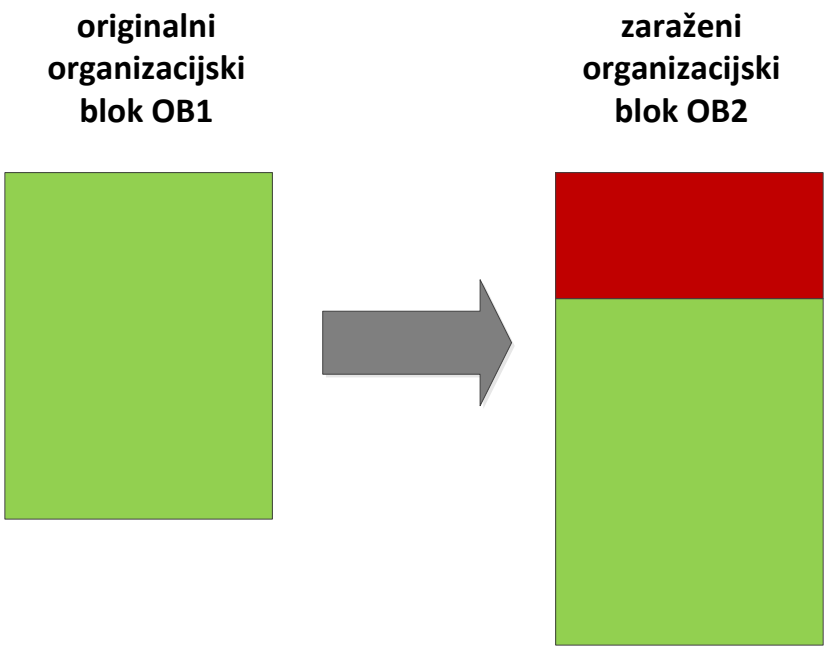
3.5: komunikacija s PLC-om putem zloćudne datoteke s7otbxdx.dll

Postoji nekoliko vrsti programskih blokova kod PLC-ova, od kojih su najvažniji sljedeći:

- podatkovni blokovi (DB) - sadrže podatke ovisne o programu, kao što su brojevi, strukture itd.
- sistemski blokovi (SDB) - sadrže informacije o načinu konfiguracije PLC-a, ovise o broju i vrsti hardverskih modula priključenih na PLC
- organizacijski blokovi (OB) - ulazne točke programa koje centralni procesor izvodi ciklički
- funkcijski blokovi (FC) - standardni blokovi koda koje izvršava PLC; svaki OB referencira barem jedan FC

Stuxnet ubacuje svoj programski kod ovisno o karakteristikama sustava koji napada. Postoje tri glavne sekvence koda (niti) koje koristi, označene kao A, B i C. Sekvence A i B su vrlo slične i napadaju PLC-ove sa istim centralnim procesorom. Djelovanje sekvence C još uvijek je nerazjašnjeno iako vjerojatno služi za upravljanje podacima sa ulazno-izlaznih jedinica koji se zapisuju u za to zaduženu memoriju PLC-a.
U slučaju korištenja sekvenci A i B, pokreću se dvije programske niti, od kojih se prva izvršava svakih 15 minuta i zadužena je za otkrivanje PLC-a i ubacivanje zloćudnog koda. Originalni organizacijski blokovi (**OB1** i **OB35**) se mijenjaju tako da ih se prvo poveća, a

onda se na početak njihovog koda ubacuje zlćudni kod (slika 3.6). Također se modificira funkcijski blok **DP_RECV** koji se koristi za mrežno raspodijeljenu komunikaciju.



3.6: tehnika ubacivanja koda u organizacijski blok

Druga nit služi za praćenje podatkovnih blokova sekvenci A i B. Ako nit pronađe posebnu tzv. magičnu vrijednost u kodu, koju koristi Stuxnet, tada zna da taj dio koda može čitati i pisati po njemu.

Rootkit kod Stuxneta u potpunosti se nalazi u datoteci s7otbxdx.dll, a kako bi izvršio zadatak prikrivanja zlćudnog djelovanja, on mora:

- čitati zahtjeve namijenjene zlćudnom (Stuxnetovom) dijelu koda
- čitati zahtjeve namijenjene zaraženim blokovima (OB1, OB35 i DP_RECV)
- upisivati zahtjeve koje mogu prebrisati Stuxnetov vlastiti kod

Navedene zahtjeve ova nit presrećuje i osigurava da Stuxnetov kod ostane neotkriven ili oštećen.

4 Utjecaj na budućnost i zaključak

Stuxnet je, kako smo vidjeli, vjerojatno najsloženiji malver koji se ikada pojavio koji je pokazao koliku štetu može prouzročiti masivni napad na specifičnu metu. Time je vjerojatno postavio novi trend u razvoju malvera.

Autori crva očito su smatrali potrebnim napraviti određenu nenamjernu štetu, odnosno zaraziti velik broj računala koja nisu meta, kako bi crv uspio stići do svoje glavne mete. Njegova metoda širenja i povećanja svojih privilegija u različitim inačicama operacijskog sustava Windows, upozorila je Microsoft i ostale velike proizvođače softvera kako ubuduće moraju uložiti još veće napore u sigurnost svojih proizvoda. Također, činjenica da ranjivosti (kao što je LNK ranjivost), pogađaju osnovne mogućnosti operacijskog sustava, dodatno je zabrinjavajuća. Otklanjanje takve ranjivosti zahtjeva jako mnogo resursa i vremena, dok isto to vrijeme koriste napadači za izradu malvera, odnosno sam malver za svoje širenje.

Prijetnja od nanošenja fizičke štete industrijskim sustavima natjerat će tvrtke koje koriste bilo kakav oblik informacijske mreže u svojim postrojenjima na primjenu sigurnosnih standarda. Stuxnet je tako na najbolji mogući način pokazao kako sigurnosni model upravljačkih računala bez pristupa Internetu, odnosno prijeko potrebnim sigurnosnim nadogradnjama, ne može opstati. Podaci opet moraju na neki način stići do tih računala i prema tome, njima su također potrebne najnovije softverske nadogradnje. Tvrtka Siemens, čiji je softver pogođen, uvidjet će da se pri razvoju softvera namijenjenog industrijskim pogonima također treba držati sigurnosnih principa koji vrijede za softver namijenjen običnim korisnicima. Crv je za preuzimanje kontrole nad računalima koje je zarazio koristio dva ukradena certifikata poznatih računalnih tvrtki, što također upućuje na nužnost postroživanja mjera prilikom korištenja infrastrukture javnih ključeva.

Uspjeh Stuxneta nažalost je i veliki poticaj kriminalnim grupama na izradu takve vrste malvera. Postoji i realna mogućnost da je crv završio na crnom tržištu. Ne smije se zaboraviti na činjenicu da su potrebni golemi resursi za razvoj, ispitivanje i eventualne nadogradnje malvera, što uvelike otežava mogućnost neke šire primjene istog. Stručnjaci, poput onih iz tvrtke Symantec, nadaju se da ovakav malver više nikad nećemo vidjeti. Nema nikakve dvojbe da će crv Stuxnet uvelike utjecati na budućnost računalne sigurnosti.

5 Literatura

1. http://www.anti-virus.by/en/index.shtml, VirusBlokAda
2. N. Falliere, L. O Murchu, E. Chien: W32.Stuxnet Dossier, tehnički dokument, Symantec, 2010.
3. A. Matrosov, E. Rodionov, D. Harley, J. Malcho: Stuxnet Under the Microscope, tehnički dokument, revision 1.2, ESET, 2010.
4. http://www.f-secure.com/weblog/archives/00002066.html, F-Secure: Stuxnet Redux: Questions and Answers, 23.11.2010.
5. http://af.reuters.com/article/energyOilNews/idAFLDE6AS1L120101129, Iran says cyber foes caused centrifuge problems, Reuters, novinska agencija, 29.11.2010.