ИНДУСТРИСКИ САЈБЕР НАПАДИ – ГЛОБАЛНА БЕЗБЕДНОСНА ЗАКАНА

Митко Богданоски, Александар Ристески, Марјан Богданоски

[1]*Воена академија "Генерал Михаило Апостолски " – Скопје*

[2]*Факултет за електротехника и информациски технологии – Скопје*

INDUSTRIAL CYBER ATTACKS – GLOBAL SECURITY THREAT

Mitko Bogdanoski, Aleksandar Risteski, Marjan Bogdanoski

Military Academy "General Mihailo Apostolski" – Skopje

Faculty of Electrical Engineering and Information Technology - Skopje

АПСТРАКТ

Сајбер нападите за многу брзо време прерастнаа во една од водечките закани врз комплетниот безбедносен систем како на национално, така и на глобално ниво. Полето на искористување на овие напади од ден на ден е сè поголемо, што е причинето пред сè од сè поголемата компјутеризираност на секоја гранка во индустријата.

Сè поголема е свеста и кај најмалите познавачи на оваа проблематика дека сајбер закана може да предизвика огромни штети кои не би се разликувале од штетите нанесени со било каква воена операција, а сајбер оружјето, на многу посуптилен начин, може да одземе повеќе животи од било каков конвенционален напад.

Владите низ целиот свет, како и сите големи светски организации, се подготвуваат да се справат со овој масивен технолошки повик за закани од глобални размери. Свеста за заканата и ризиците е висока, што условува, и покрај кризната економска ситуација во светски рамки, издвојување на голема сума на пари со цел подготовка за одговор на нови вонредни состојби кои би биле причинети од глобалните сајбер напади.

Работата во овој труд се фокусира на сајбер нападите како глобална безбедносна закана со огромни импликации не само врз поединци или системите на една компанија, туку и врз комплетниот безбедносен систем на една држава, со можност за предизвикување на кризи од многу поширок размери. Посебен акцент се става врз најновите индустриски напади, кои според најголем број истражувања од релевантни организации во оваа област, се ставени како најголеми моментални сајбер закани и меѓу најголемите глобални закани воопшто.

Клучни Зборови: Глобална безбедност, Сајбер, Индустриска безбедност, Stuxnet, Duqu

ABSTRACT

In a very short period of time, cyber attacks have become one of the leading threats to the complete security system on national as well as global level. The field of utilization of these attacks is increasing day by day, which is primarily caused by the increased computerization of every branch of the industry.

Even the people and companies that are not experts in this issue are aware that cyber threat can cause enormous damage which would not differ from damages caused by any military operation, and cyber weapons, on very subtle way, may take more lives than any other conventional attack.

Governments around the world and all major world organizations are preparing to cope with this massive technological call for threats with global scale. Awareness of the threat and risk is high, which requires, despite global financial crisis, allocating a large sum of money in order to prepare against the new emergencies that would be caused by global cyber attacks.

The work in this paper focuses on cyber attacks as a global security threat with enormous implications not only on individuals or company systems, but the entire security system of a country with the possibility of causing a crisis on a global scale. Special emphasis is put on the latest industry attacks, which, according to most researches of relevant organizations in this area, are placed as the most dangerous cyber threats in recent time and one of the biggest global security threats of our time.

Key Words: Global Security, Cyber, Industrial Security, Stuxnet, Duqu

1. ВОВЕД

Во денешно време компјутерите секојдневно се искористуваат од злонамерните корисници за реализирање на нивните активности, било да се тие поврзани со стекнување личен профит или со нанесување на штети кои можат да имаат и последици по животите на луѓето.

Покрај големината и обемот на заканата, еден од најголемите предизвици во борбата против компјутерскиот криминал е во фундаменталната природа на компјутерскиот свет. Сајбер просторот е динамичен и се менува многу често со рапидно темпо. Зголемувањето на можностите на компјутерите, во однос на нивните капацитети и брзината на комуникацијата, ја зголемува можноста за криминални дејства на мотивираните сторители, како и достапноста на соодветни цели. Од друга страна, светската компјутерска мрежа (Интернет) го трансформира компјутерскиот криминал од локален проблем, во интернационално безбедносно прашање.

Сајбер заканите моментално се толку значајни што станаа приоритет во националната безбедност во повеќето водечки светски земји. Со цел подобро да се разберат предизвиците со кои се соочува сајбер инфраструктурата во водечките светски земји, потребно е да се испита како владините агенции се однесуваат кон заканите од злонамерниците кои извршуваат компјутерски базиран напади. Од една страна знаеме дека компјутерските напади често се „хај-тек“ верзија на повеќето традиционални кривични дела како што се кражбите, шпионажата, саботажата и измамата. Од друга страна, последиците од сајбер криминалот се толку обемни и технолошки комплексни да истите бараат специфични знаења за подобро разбирање на природата на заканите, како и тактиките и стратегиите за нивно истражување.

Нашиот труд е поделен во следните поглавја. После воведот во втората глава се дава објаснување за третманот на сајбер нападите од страна на светските велесили, како и од големите светски организации, кога истите се разгледуваат како глобална безбедносна закана. Потоа во Глава 3 се наведуваат најновите концепти на сајбер војувањето и се набројуваат најмодерните и најдеструктивни сајбер напади со можности за нарушување на глобалната безбедност. Во Глава 4 посебен акцент се става на индустриските сајбер напади каде пред сè се разгледуваат Stuxnet и Duqu нападите, при што се дава подетално објаснување за начините на инсталирање и функционирање и на двата напади. На крај, во последната глава се даваат некои конкретни заклучоци за овие напади и предлог мерки за намалување на ризиците од истите.

2. МЕСТОТО НА САЈБЕР НАПАДИТЕ ВО ГЛОБАЛНИТЕ БЕЗБЕДНОСНИ ЗАКАНИ

Доколку се погледне во литературата која го дефинира поимот за глобални безбедносни закани и пред сè во класификацијата на овие напади, ќе се види дека има разлика во дефиницијата и поделбите на овие закани и дека истото зависи од многу фактори. Прво, зависи од периодот од кога датира таа литература, второ, зависи од кој аспект се разгледуваат глобалните безбедносни закани (економски, здравствени, воени и сл.) и трето, зависи од која меѓународна организација или држава се третира овој проблем, т.е., кои се приоритетите на таа организација/држава. Но, речиси во сите стратегии, доктрини, концепти и останати документи кои ја третираат оваа проблематика, а кои датираат од поново време, сајбер заканите се рангираат како една од најголемите глобални закани.

За да се разбере улогата и местото на сајбер нападите во глобалните безбедносни закани, како и нивниот тренд на пораст, доволно е само да се впише во било кој интернет пребарувач зборот “Cyber attacks”. Листата на линкови кон кои може да се пристапи е многу поголема и од онаа која се однесува на самите глобални безбедносни закани. Оваа глобална безбедносна закана е една од најполемизираните закани, со најразлилни пристапи на истражување и дискусија во врска истата.

Доколку се погледне воодредени валидни информации кои се неодамна објавени [1,2,3,4], веднаш ќе се забележи местото на овие несиметрични закани во глобалните безбеднисни закани. Истото ќе се случи доколку се погледне и во најновите безбедносни стратегии на сите светски велесилии организации [4,5,6], каде овие напади ги завземаат највисоките места во набројувањето на главните безбедносни закани.

Во Интернационалната Стратегијата за Сајбер Безбедност и најновата Стратегија за Безбедност на САД, сајбер заканите се третираат на исто ниво како и воените закани [7,8]. Ако се анализира изјавата на Леон Панета, која ја даде додека беше на функцијата Директор наCIA (Central Intelligence Agency), каде истиот наведува дека “сајбер нападите се најголемата национална безбедносна закана на САД”, може лесно да се увиди третманот на овие закани од страна на една од најмоќните разузнавачки организации во светот [9].

Од друга страна, FBI (Federal Bureau of Investigation) уште во 2009 година ги рангира сајбер нападите како трети по ред најопасни закани, кои следат веднаш по нуклеарната војна и оружјето за масовно уништување [10].

Според најновиот Извештај за глобални ризици за 2012 година [11], кој е годишен извештај на Светскиот Економски Форум, Сајбер заканите се рангирани на четврто место, секако гледано од економски аспект.

Во Табела 1 е даден приказ на најпознатите сајбер напади позади кои како напаѓачи се јавуваат држави или непознати групи, а чија цел се важни државни јавни и приватни институции. Најчести последици од овие напади се одбивање на услуга, шпионажа, саботажа и крадење информации [12].

ТАБЕЛА 1: ШИРОКО ПОЗНАТИ НАПАДИ ВРЗ НАЦИОНАЛНАТА/ГЛОБАЛНАТА БЕЗБЕДНОСТ И КРИТИЧНАТА ИНФРАСТРУКТУРА

Година	**Напаѓач**	**Цел**	**Последици**
1982	САД - ЦИА	Логичка бомба насочена кон гасоводот на СССР во Сибир	Деструкција
1999 и 2000	Русија	Пентагон, NASA, Национална Лабараторија	Крадење информации и шпионажа
2004	Кина	Sandia Национална Лабараторија, Lockheed Martin и NASA	Шпионажа
2007	Кина	Компјутерска мрежа на САД (750,000 компјутери)	Одбивање на услуга
2007	Русија	Web сајтови на владата и други важни институции /банкина Естонија	Одбивање на услуга
2008	Непознато	Воена мрежа на САД	Злонамерен код и зомби машини
2008	Кинаи/или Русија	Претседателски избори на САД	Упадво email системите
2008	Русија	Web сајтови на владата и други важни институции /банкина Грузија	Одбивање на услуга
2010	Непознато (неофицијално Израел)	Иранси објект за збогатување на ураниум	Саботажа
2010	Anonymous “Operation Avenge Assange”	Повеќе цели во западните земји (јавни и приватни)	Одбивање на услуга

3. НАЈНОВИ КОНЦЕПТИ НА САЈБЕР НАПАДИТЕ

Иако сајбер безбедноста го придружува ИКТ секторот уште од ставањето во употреба на првиот компјутерски систем, дури во 2007 година, кога е реализиран сајбер напад со големи размери напаѓајќи цела нација, овие напади станаа центар на меѓународното внимание. Ова беше само предупредување до сите светски големи сили за новиот тип на закана кој за кратко време ќе стане и една од најголемите закани врз глобалната безбедност [13].

За подобро разбирање на оваа глобална безбедносна закана прво ќе ги опишеме најчестите напади кои спаѓаат во оваа група на закани. Во листата која следува, нападите се распоредени според нивното влијание и тоа од наједноставни, до најдеструктивни [14].

- **Сајбер шпионажа**
  Сајбер шпионажата е акт или практика на здобивање на тајни (осетливи, сопствени или класифицирани информации) од индивидуалци, конкуренти, ривали, влади и непријатели за стекнување на воена, политичка или економска предност користејќи нелегални методи за искористување на Интернетот, мрежите, софтверот и/или компјутерите.
- **WEB вандализам**
  Ова се напади кои ги обезличуваат web страните, или напади со одбивање на услуга.
- **Пропаганда**
  При овој вид на напад можно е да се испраќаат политички пораки кон секој кој има пристап кон интернет.
- **Собирање информации**
  Овој напад се користи со цел информациите кои не се чуваат безбедно да се пресретнуваат, па дури и модифицираат, овозможувајќи вршење на шпионажа од било кој дел од светот.
- **Напади со дистрибуирано одбивање на услуга**
  Овој напад се карактеризира со можност за искористување на голем број компјутери во една или повеќе држави за лансирање на напад врз системите на држава од каде воопшто и не се лансира нападот.

- **Нарушување на функционирањето на опремата**
  Жртви на овој напад се воените активности во кои за координација се искористени компјутери и сателити. Користејќи го овој напад, злонамерниците можат да ги пресретнат или да ги изменат наредбите и комуникациите, со што војниците би се ставиле во ризична ситуација.
- **Напаѓање на критичната инфраструктура**
  Со помош на овој напад, злонамерниците можат да навлезат во системите за контрола на електричната енергија, водата, горивото, комуникациите, транспортот и слични клучни инфраструктурни елементи и да се обезбеди контрола врз истата со основна цел уценување, кражби, изнудувања, измама и слично.
- **Компромитиран фалсификуван харвер**
  Овој напад се однесува на заедничкиот хардвер искористен во компјутерите и мрежите кои имаат злонамерен софтвер скриен во софтверот, firmware-от или дури и во микропроцесорите.

За време на скорешното интервју на секретарот за одбрана на САД, Леон Панета, дадено за CBC News [15], сајбер компонентата на војување привлече големо внимание. Имено, тој ја покажа загриженоста од овие напади и можните последици од истите, кои можат да бидат од „парализирање на финансискиот систем“ и „исклучување на електричната мрежа“, па сè до „парализирање на државата“. Ако се земе во предвид дека оваа изјава е дадена од едно од најкомпетентните лица кои може да ја коментираат оваа проблематика и воедно од висок претставник на една од најмоќните светски велесили, повеќе од јасно е дека треба и тоа како да се разгледа сериозноста на овие напади. Како што објаснува Панета, за да се одговори соодветно и навремено на овие напади мора навремено да се вршат подготовки за истите. Секако дека ова е пред сè насочено кон оние кои се најинволвирани во сајбер безбедноста.

Подолу се набројани петте најголеми предвидувања за развојот на сајбер напади за 2012 година:

- Сајбер нападот во 2012 година се предвидува да биде фокусиран на мобилните уреди [16].
- Глобалните трошоци за сајбер војувањето за 2012 година се проценети на $15.9 милијарди [17].
- Се очекува сајбер нападите да бидат насочени кон специфични оранизации во специфични индустрии [18].
- Сајбер нападите во 2011 имаа пораст за 2.6 пати, а во 2012 година се предвидува овој пораст да биде уште поголем [19].
- Во 2012 сајбер шпионажата, која за цел ги има компаниите и владините агенции ширум светот, ќе доминира во генералната слика за информациската безбедност на корпоративно и национално ниво [20].

Анализата на овие пет предвидувања поврзани со сајбер заканите даваат една мрачна слика за сајбер нападите за 2012 година. Заканите изгледаат крајно предизвикувачки, ако не и малку преголеми. На видик е модернизација на вооружените конфликти и во овој момент има повеќе прашања отколку одговори.

Според Винсет Вифер, потпретседателот на McAfee, која компанија воедно е придружница на Intel Corp., „многу од заканите кои ќе станат познати во 2012 година веќе се наѕираа под радарот на 2011 година“.

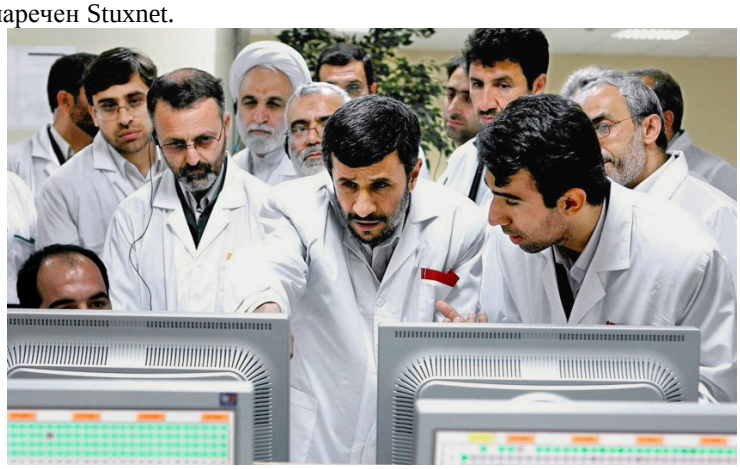
Според оваакомпанија, која е една од водечките компании во производство на анти-вирус програми, најголемите пет сајбер закани за 2012 година се [21]:

- **Индустриски напади:** Многу од средините каде се искористени SCADA (Supervisory Control And Data Acquisition) системите, како што е искористеноста кај системите кои ја контролираат водата, електричната струја, нафтата, гасот и нуклеарните централи, немаат доволно строги безбедносни практики што ги прави подложни на уцени, изнудувања и кражби.
- **Вграден хардвер:** Вградените системи, кои се дизајнирани за специфични контролни функции во големите системи, многу често се користат во возилата, GPS системите, медицинските уреди, рутерите, дигиталните камери и принтери. Хакерите со пристап кон злонамерен софтвер кој го напаѓа хардвер нивото, како што е системот, ќе се здобијат со контрола и долгорочен пристап до системот и неговите податоци.
- **Хактивизам:** McAffee предвидува дека вистинските Анонимни групи ќе се откријат или ќе изумрат, а основна цел на водечките дигитални напади здружени со физичките извршители ќе бидат јавните личности, како што се политичарите и индустриски лидери, судии и сл.
- **„Легитимен“ спам:** Додека глобалниот спам во поново време се намалува, легитимните реклами сега ги користат истите техники, како што е купување на email листи на корисници кои се согласиле да примаат реклами, или купување на низата на податоци за потрошувачите од компаниите кои ги поседуваат овие бази на податоци. Се очекува „легалниот“ спам да расте со побрзо темпо од илегалниот фишинг и другите измамина интерент.

- **Напади на мобилните уреди:** Техниките кои во минатото се користеа за online банкарство, како што е крадење од жртвите додека истите се логирани, според предвидувањата, сега како цел ќе ги имаат корисниците на мобилното банкарство.

4. ИНДУСТРИСКИ САЈБЕР НАПАДИ

Како што може да се забележи од претходните објаснувања, меѓу најголемите закани со глобални размери, а кои спаѓаат во сајбер нападите, се нападите над SCADA системите или индустриските напади. Доколку се разгледаат последните примери за искористување на овие напади, овој наш заклучок ќе стане повеќе од јасен. Еден од тие примери и нападот на нуклеарната програма на Иран, во 2010 година, од високо софистициран вирус наречен Stuxnet.



Слика 1. Претседателот на Иран, Махмуд Ахмединеџад, во посета на Натанц погонот во 1998 година

Поточно, нападнат беше погонот Натанц за збогатување на ураниум, нонападот за среќа беше навреме откриен и немаше посериозни последици.

Иако белоруската компанија за анти-вирус програми VirusBlokAda овој вирус го идентификува во компјутер на иранскиј државјанин нешто порано, во средината на Јуни 2010 година, сепак, во тоа време овој вирус сеуште се третирал како непознат. Според неофицијални информации кои можат да се најдат по интернет страниците, овој напад е извршен од страна на израелеската разузнавачка агенција Mossad. Истражувањата покажале дека овој вирус покрај во Иран, во најголем процент се распространил во Индонезија и Индија (Табела 2).

Една година подоцна, или поточно на 1 Септември, 2011 година, во Лабораторијата за Криптографија и Безбедност на Системи (CrySyS) на Универзитетот за технологии и економија во Будимпешта, Унгарија, откриен е нов компјутерски црв или malware, наречен Duqu. Подоцна овој вирус е анализиран од страна на Symantec, кои веруваат дека овој вирус е креиран од истите автори на Stuxnet, или автори кои имаат пристап кон изворниот код на Stuxnet. Овој црв, како и Stuxnet, има фалсификуван дигитален сертификат и собира информации кои би биле искористени за понатамошни напади. Во делот кој следи е даден подетален опис на овие два напади, кои во последните две години претставуваат најголеми закани врз безбедноста на системите на национално и глобално ниво.

ТАБЕЛА 2: РАСПРОСТРАНЕТОСТ НА STUXNET НАПАДОТ

Земја	Инфицирани компјутери
Иран	58.85%
Индонезија	18.22%
Индија	8.31%
Азербејџан	2.57%
САД	1.56%
Пакистан	1.28%
Други	9.2%

4.1. Stuxnet

Stuxnet е компјутерски црв дизајниран да ги инфицира Siemens SIMATIC WinCC и S7 PLC (Programmable Logic Controllers) производите, кои се или инсталирани како дел од PCS 7 системот, или оперираат самостојно. Овој црв, за да се шири, користи познати и претходно непознати повредливости и беше доволно моќен за да ги избегне најновите безбедносни технологии и процедури [22].

Имено, Stuxnet ги користи слабостите на Window оперативниот систем и производите на Siemens. Откако ќе ја детектира соодветната жртва, ја модифицира контролната логика во специфични модели на PLC. Целта би била вршење на саботажа на специфични индустриски процеси. Stuxnete способен даги инфицира сите моментални верзии на Windows, вклучувајќи ги и Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 и Windows 7. Исто така, ги инфицира и Siemens STEP 7 проект фајловите на таков начин што тој се извршува автоматски кога STEP 7 проектот е иницран од неинфициран Siemens систем. Примарна функција на Stuxnet е пенетрирање и оневозможување на SCADA системите.

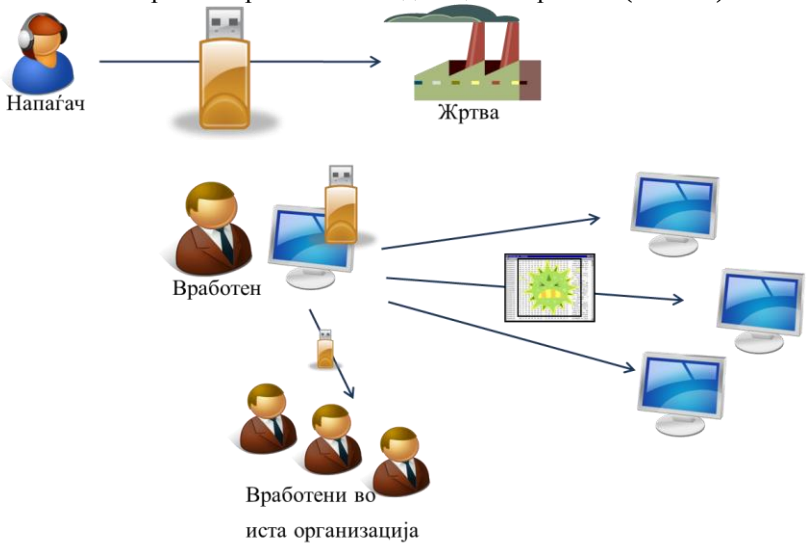
ТАБЕЛА 3: ПОДЕЛБА НА STUXNET НАПАДОТ СПОРЕД МОТИВАЦИЈАТА

Мотивација	Цел	Процена
Политичка	Саботажа	Најверојатно
Комерцијална	Шпиона	Можно
Криминал	Придобивки, на пр. уцени	Малку веројатно
Приватна	Демонстрација	Најневеројатно

Веднаш по откривањето на овој црв, од страна на најголемите компании се преминало на строга анализа, што е и разбирливо, ако се земе во предвид дека навлегувањето во функционирањето на било кој вирус може да им помогне на компаниите за антивирус програми да произведат подобар софтвер за детектирање на тој вирус.

Stuxnet е првиот црв кој ги напаѓа индустриските системи за контрола. Нападот започнува кога инфицирана USB (или друга пренослива) флеш меморија на инсајдер или некој контрактор ќе биде стартуван во околината која е цел на овој вирус. Вирусот, исто така, може да биде внесен и преку 3 мрежни техники, S7 Проект фајлови и конекции кон WinCC базата на податоци.

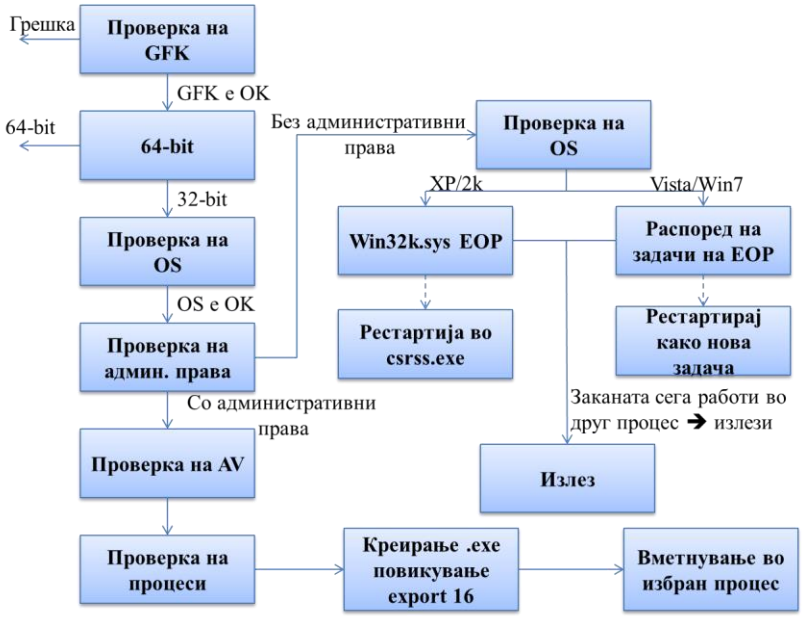
Кога ќе се внесе во оваа околина Stuxnet го инфицира компјутерот на вработениот каде е поставена инфицираната надворешна меморија. Овој вработен, без негово знаење, го шири црвот во другите вработени со размена на USB, или размена на податоци од компјутерот со неговите соработници. Дополнително на ова, Stuxnet се шири и во локалната мрежа со размена на податоци во мрежата (Слика2).



Слика 2. Инфицирање на компјутерот со Stuxnet

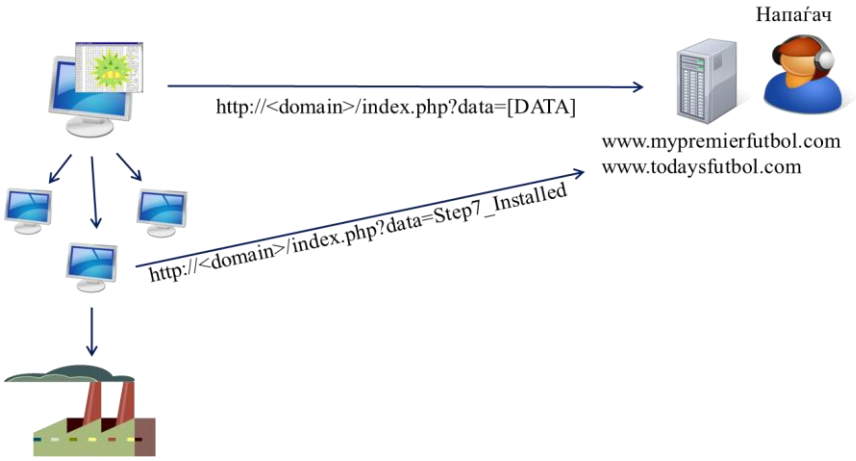
Export 15 е привиот export кој се повикува кога .dll фајлот ќе се внесе за прв пат. Одговорен е за да провери дали заканата работи на компатибилна верзија на Windows, дали компјутерот е можеби веќе инфициран или

не, да ги процени привилегиите на моменталниот процес во системот, да провери кои антивирус производи се инсталирани и кој би бил најдобриот процес во кој би можел да биде вметнат. Потоа тој го вметнува во .dll фајлот во избраниот процес користејќи уникатна техника за вметнување и го повикува export 16 (Слика 3).



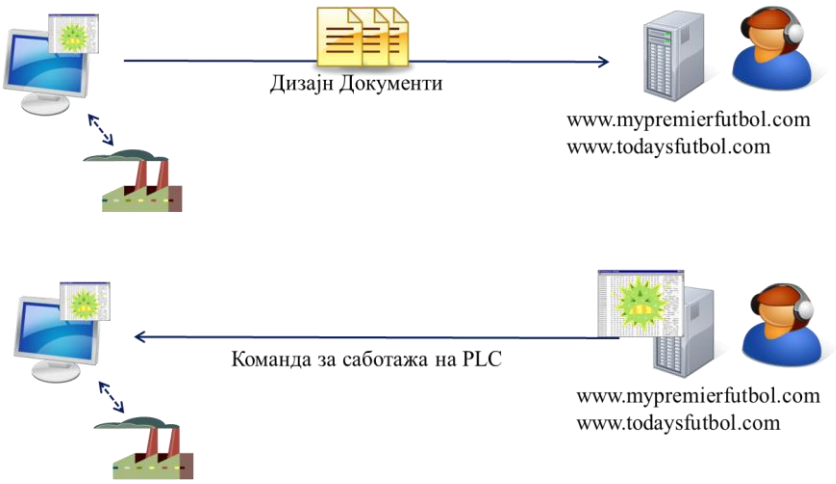
Слика 3. Контролен проток за Export 15

Целта на Stuxnete да го најде комјутерот во организација кој е одговорен за PLC. PLC е мал компјутер кој може да ги контролира индустриските машини, како што се на пример пумпите и центрифугите. Секогаш кога компјутерот е нападнат испраќа информација до напаѓачот преку Интернет со цел да го обезбеди напаѓачот со општи информации за системот. Напаѓачот може да побара од заразениот компјутер да го прошири Stuxnet до другите компјутери и да ги пронајде компјутерите кои можат да го програмираат нападнатиот PLC.



Слика 4. Контрола на PLC и update-ирање на податоците кај напаѓачот

Напаѓачот потоа ги краде дизајн документите (Слика 5) со цел да одреди како да го саботира индустрискиот контролен систем. Откако ќе ги добие дизајн документите способен е да го испрати кодот кон инфицираниот систем, со што се врши негова саботажа. На пример, испратениот код може да резултира во одземање на контролата врз гасовод или врз центрифугалните машини.



Слика 5. Крадење на дизајн документите и испраќање на команди за саботажа ан PLC

Овој вирус ја користи предноста над најмалку четири „0-day“ ранливости и покажува значителна софистицираност во неговата експлоатација и на Windows платформата и на Siemens системите. Некои од најважните карактеристики на овој црв се:

- Споро се пренесува додека не дојде до нова средина (пр. мрежа на одредена компанија), најчесто преку USB флеш меморија или друг „преносliв“ медиум,
- Откако ќе влезе во мрежата која е негова цел, тој брзо се пренесува помеѓу корисниците преку повеќе мрежни патеки,
- Ја пребарува машината/мрежата за присуство на анти-вирус програми на многу производители и го модифицира неговото однесување за да ја избегне детекцијата од овие анти-вирус програми,
- Контактира со серверот за командување и контрола на Интернет за инструкции и update-и,
- Воспоставува peer-to-peer мрежа со основна цел пропагирање на инструкциите и update-ите во мрежата каде се сместил, дури и до опремата кон која нема директна интернет конекција,
- Ја модифицира PLC програмската логика, предизвикувајќи ги физички процеси да не функционираат исправно,
- Ги крие модифицираните PLC програми од контролните инжинери и систем администраторите кои се обидуваат да разберат зошто нивниот систем не функционираат исправно,
- Се потпишува со сертификати кои се украдениод еден или два главни производители на хардвер, така што нема предупредување кога црвот се инсталира, и
- Ако увиди дека одредена машина до која дошол не е потенцијална цел, црвот се отстранува од машината откако ќе се реплицира на други ранливи медиуми и машини.

4.2.Duqu

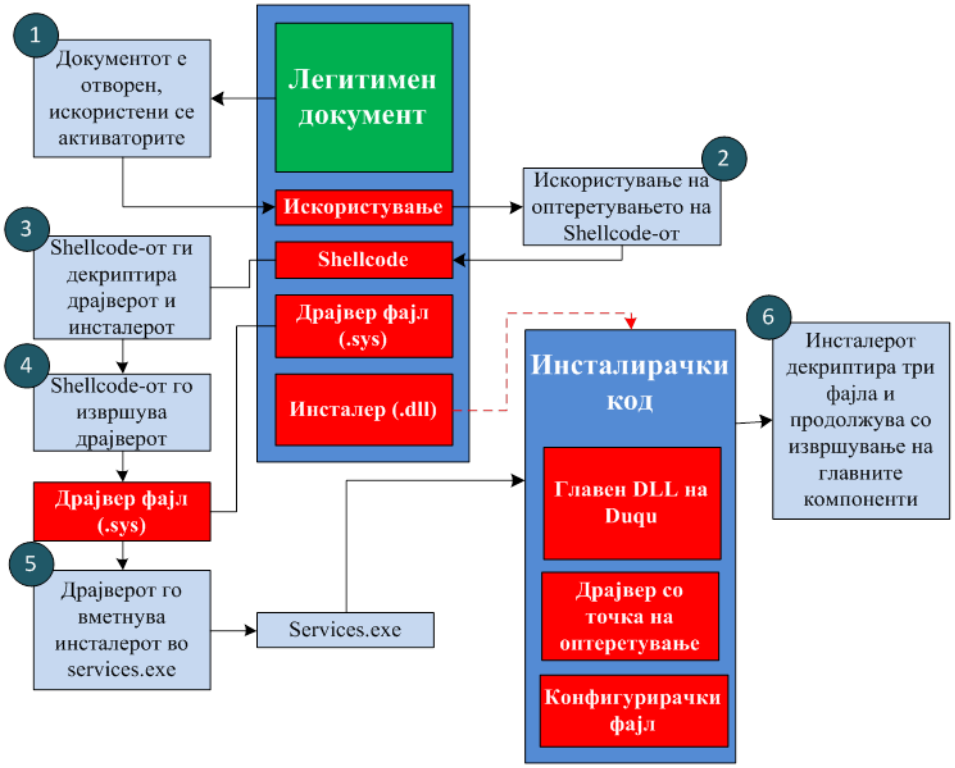
Duqune е Stuxnet, но неговата структура и филозофија на дизајнот се многу слични на оние на Stuxnet. Во овој момент не може со сигурност да се каже дали и овој напад е производ на истите креатори на Stuxnet, но повеќе од сигурно е дека креаторите на Duqu имаат пристап кон изворниот код на Stuxnet [23].

Duqu, како и Stuxnet, користи лажни сертификати за да го оневозможи неговото детектирање од страна на антивирус програмите и администраторите на мрежите.

Целта на Duque да се соберат „разузнавачки“ информации од ентитети, како што се индустриската инфраструктура и производителите на системи, како и тие кои не се во индустрискиот сектор, со цел подоцна многу лесно да се реализира напад над некоја трета жртва. Напаѓачите бараат информации, како што се дизајн документи, кои подоцна може да им помогнат да извршат напад врз различни индустрии, вклучувајќи и објекти на индустриските системи за контрола.

Duqu воопшто не содржи код кој е поврзан со индустриските системи за контрола и најчесто се Тројанци со далечински пристап (RAT). Вирусот не е само-реплицирачки. Според истражувањата на Symantec, главна цел на овој malware се ограничен број на организации и тоа само за нивни конкретни средства. Сепак, можно е други слични напади да биле искористени против други организации и истите да останале недетектирани.

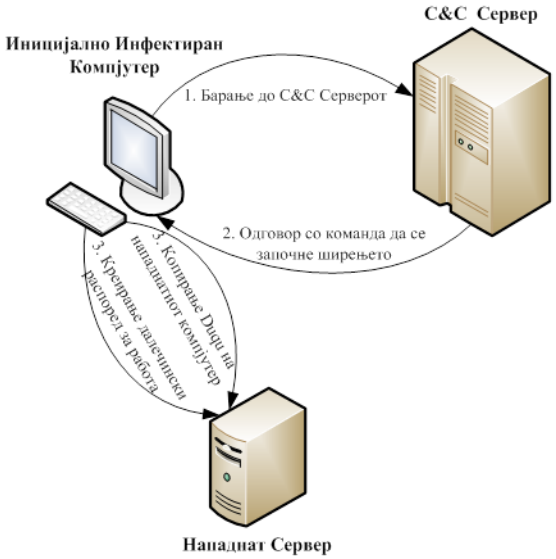
Во еден конретен случај, напаѓачите како цел искористиле еден специфичен email на кој испратиле инфектиран Microsoft Word документ. Word документот содржел моментално неоткриен 0-day кернел кој бил способен да го инсталира Duqu. Сеуште не е познато дали напаѓачите користеле иста методологија и ист 0-day во сите случаи.
Напаѓачите го корситат Duqu за да инсталираат други програми за крадење на информации кои може да снимат пишување на тастатура и да соберат други информации за системот. Всушност, напаѓачите бараат информации кои би можеле да бидат искористени за понатамошни напади.
Duqu се состои од драјвер фајл, DLL (може да содржи многу вградени фајлови), и конфигурациски фајлови. Овие фајлови мора да бидат инсталирани од други извршители – инсталери. Инсталерот драјвер фајловите ги регистрира како сервиси, така што тој започнува со системска иницијализација. Потоа драјверот го вметнува главниот DLL во services.exe. Од тука, главниот DLL започнува со екстрактирање на други компоненти и овие компоненти се вметнуваат во други процеси. Овој процес на вметнување ги крие активностите на Duqu и може да овозможи одредени однесувања да заобиколат одредени безбедносни производи.



Слика 6. Процес на инсталација на W32.Duqu

Еден од регистрираните драјвери е потпишан со валиден дигитален код користејќи сертификат за потпис кој истекува на 2 Август 2012 година. Сертификатот за потпис на дигиталниот код е издаден од компанија со седиште во Тајпеј, Тајван и беше одземен на 14 Октомври, 2011 година. Се верува дека приватните клучеви кои се користат за генерирање на сертификатот се украдени од компанијата. Со помош на валиден сертификат, на Duqu му се овозможило да ги заобиколи стандардните ограничувања на непознатите драјвери и вообичаените безбедносни политики.
Duqu, за да комуницира со серверите за командување и контрола (C&C), користи HTTP и HTTPS. Duqu, исто така, има рутини кои се свесни за proxy-то, но истите не се користат како стандардна опција. Секој напад користи еден или повеќе различни C&C сервери. Моментално познати C&C сервери се 206.183.111.97 хостиран во Индија, 77.241.93.160 хостиран во Белгија и 123.30.137.117 хостиран во Виетнам. Сите овие IP се неактивни. C&C серверите се конфигурирани така што само едноставно го препраќаат сиот сообраќај од портите 80 и 443 кон сите сервери. Овие сервери може да го препратат сообраќајот понатаму до други сервери, што го отежнува идентификувањето и обновувањето на вистинските C&C сервери. C&C серверите за препраќање на информации биле отстранети од употреба на 20 октомври 2011 година, поради што е откриен само ограничен број на инфромации. Дури и ако серверите не беа тргнати од употреба, многу малку

информации би се пронашле, пред сè поради лимитираната примена за едноставно препраќање на сообраќајот.
Преку C&C серверите, напаѓачите биле во можност да симнат дополнителни извршни програми, вклучувајќи и програма за крадење на информации (infostealer) која може да извршува акции како што се означување на мрежата, снимање на пишувањето на тастатурата и собирање на информации за системот. Информациите се најавени на лесно криптирани и компресирани локални фајлови, а потоа мора да бидат ексфилтрирани. Дополнително на овој infostealer, од страна на сервер, на 18 октомври се вметнати уште три DLL.
Заканата користи прилагоден C&C протокол, кој примарно симнува и прикачува нешто што наликува на.jpg фајлови. Сепак, дополнително на лажните .jpg фајлови, се додаваат криптирани податоци за ексфилтрација и такви се примаат. Употребата на .jpg фајловите е за да се сокрие преносот на корумпираните фајлови во мрежата.
Како што веќе споменавме, оваа закана не се само-реплицира, но базирајќи се на форензичките анализи на компромитираните компјутери, на заканата и е наложено, најверојатно преку C&C сервер, да се реплицира и на други компјутери во мрежата преку размената на податоци во таа мрежа.



Слика 7.Ширење на Duqu низ мрежата

За овие инфекции конфигуриран е не-стандарден фајл, кој и дава инструкции на мрежата да не го користи надворешниот C&C сервер, туку да користи peer-to-peer C&C модел. Во овие случаи, новиот компромитиран компјутер добива инструкции да комуницира со компјутерот кој го инфицирал, кој го проксира сиот C&C сообраќај назад кон надворешниот C&C сервер. Со употреба на peer-to-peer C&C модел се овозможува заканата да пристапи кон компјутери кои може да не се конектирани директно кон надворешниот Интернет и исто така да се избегне детектирањето на потенцијалниот сомнителен надворешен сообраќај од повеќе компјутери.
На крај, заканата е конфигурирана да работи 30 дена. После 30-тиот ден, заканата автоматски се отстранува од системот. Сепак, Duqu симнува дополнителни компоненти кои може да го пролонгираат овој период. Така, ако се откријат напаѓачите и ако тие ја изгубат способноста за контрола на компромитираните компјутери (на пример, ако C&C серверите се исклучат), инфекциите сами автоматски ќе се отстранат, со што би се спречило нивното откривање.

5. ЗАКЛУЧОК И ПРЕПОРАКИ ЗА ПОДОБРУВАЊЕ НА БЕЗБЕДНОСТА ВО СЛУЧАЈ НА ИНДУСТРИСКИ САЈБЕР НАПАДИ

Stuxnetи Duqu со сигурност не се последните црви од овој тип со кои ќе се соочи SCADA/ICS индустријата. Ако Stuxnet и Duqu беа успешни во оштетувањето на целта, која и да е целта на овие два напади, не може да се очекува од оштетениот да одговори на ист начин. Дури иако Stuxnet и Duqu не беа успешни, стана повеќе од јасно дека инфраструктурата на развиените земји и на земјите во развој е осетлива на напади со malware-и кои се софистицирани како и овие два црви, и дека непријателите од различни држави и култури сега

имаат пример за тоа како да структуираат сопствен malware кој би го искористиле за реализирање на нивните злонамерни цели. Иако во оваа анализа е покажано дека Stuxnet е реализиран врз производи на Siemens, веќе е докажано дека истиот или слични напади можат да се реализираат врз контролни системи на било кој производител.

Како потенцијални жртви не се јавуваат само владините агенции. Сите најнови извештаи покажуваат дека во последните години организираните криминални банди во многу географски подрачја наголемо прикажуваат дека вештините за да се конструираат најголем дел од компонентите на овие два црви се лесно достапни на црниот маркет.

Стекнување на останатите PLC програмерски вештини е прашање на идентификување на целните технологии, набавка и посетување на обука на производителите во еден од многуте области каде што се нуди ваквата обука. Овој вид на malwareќе биде моќна нова алатка за изнудувачки закани против главните инфраструктурни провајдери – вид на напад со кој банкарската индустрија се справува скоро една декада.

Интегрирање на индивидуалните компоненти во еден производ како што се Stuxnet или Duqu е нешто што не е претходно видено, но потребните вештини може да се споредат со оние кои се потребни за да се произведе било која комплексна апликација. Креирањето на други закани слични на Stuxnet или Duqu за секоја организација со многу финансиски сретства и малку време и не е толку сложена работа.

Модифирањето на копиите на Stuxnet или Duqu црвите со цел да се нападнат други индустриски платформи е можно и би било многу поефтино, отколку наново да се пишува целиот нов вирус.

Ако се знае дека крититичната инфраструктура во светски рамки треба да е сигурна и безбедна, ова значи дека сопствениците и операторите треба да станат свесни дека нивните контролни системи во денешно време се цел на софистицирани напади и декае потребно прилагодување на нивните безбедносни програми според најновите закани. Конкретно, безбедносните програми треба да [24]:

- Ги разгледаат сите можни патишта на инфицирање и да имаат стратегија која повеќе се стреми кон намалување на овие патишта, отколку да се фокусира на единечна патека, како што е инфекцијата преку USB надворешна меморија,
- Препознаат дека нема совршено безбедносно решение и да превземат чекори за агресивно сегментирање на контролните мрежи за да се лимитираат последиците од компромисот,
- Инсталира ICS (Industrial Controlled Systems) - соодветни технологии за детектирање на упади за да се детектираат нападите и да се зголеми нивото на предупредување кога опремата е компромитирана или постои ризик од компромитирање,
- Се распоредат, работат и одржуваат ICS - соодветни безбедносни технологии и практики со максимална ефикасност, вклучувајќи firewall-и, антивирус програми и бели листи дизајнирани за SCADA/ICS, со цел да се направи нападот од софистициран malware многу потежок,
- Погледнат надвор од традиционалните firewall-ина мрежно ниво, и да се насочат кон firewall-ите кои се способни за длабока инспекција на пакетите кај клучните SCADA и ICS протоколи,
- Се фокусираат на обезбедување на критичните системи, посебно на безбедносно интегрираните системи (SIS),
- Вклучат безбедносни проценки и тестирања, како дел од развојот на системот и периодичните процеси за одржување. Да ги идентификуваат и намалат потенцијалните повредливости, со што се намалува веројатноста за успешен напад, и
- Се стремат да ја подобрат културата на индустриската безбедност меѓу менаџментот и техничките тимови.

Овие промени за подобрување на безбедноста на индустриските системи за контрола е потребно итно да се направат. Чекањето на иден сличен вирус (црв) може да биде премногу доцна.

КОРИСТЕНА ЛИТЕРАТУРА:

[1] "GCHQ chief reports 'disturbing' cyber-attacks on UK", BBC News UK, 31.10.2011, http://www.bbc.co.uk/news/uk-15516959

[2] "Cyber attacks take down two Israeli websites - is cyber warfare the next front in the middle east conflict?", FORBES, 16.01.2012, http://www.forbes.com/sites/erikkain/2012/01/16/cyber-attacks-take-down-two-israeli-websites-is-cyber-warfare-the-next-front-in-the-middle-east-conflict/

[3] US Today, Cyberattacks likely to escalate this year, 10.01.2012, http://www.forbes.com/sites/erikkain/2012/01/16/cyber-attacks-take-down-two-israeli-websites-is-cyber-warfare-the-next-front-in-the-middle-east-conflict/

[4] Cyber-attacks now the most feared EU energy threat, Euractive, 25 January 2011, http://www.euractiv.com/energy/cyber-attacks-feared-eu-energy-threat-news-501547

[5] "Strategic ConceptFor the Defence and Security of The Members of the North Atlantic TreatyOrganisation", Adopted by Heads of State and Government in Lisbon, November 2010, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf
[6] "A Strong Britain in an Age of Uncertainty: The National Security Strategy, United Kingdom", October 2010, http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf
[7] "National Security Strategy, Unite States of America", May 2010, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
[8] "International Strategy For Cyberpace, Prosperity, Security, and Openness in a Networked World", President of the United States, MAY 2011, http://info.publicintelligence.net/WH-InternationalCyberspace.pdf
[9] "Cyber-Attacks Are the Biggest National Security Threat", August 2011, http://www.policymic.com/articles/1519/with-shaky-future-ahead-pakistan-poses-real-danger
[10] "FBI ranks cyber attacks third most dangerous behind nuclear war and WMDs", TD Daily, 7 January 2009, http://www.tgdaily.com/security-features/40861-fbi-ranks-cyber-attacks-third-most-dangerous-behind-nuclear-war-and-wmds
[11] "Global Risks 2012 Seventh Edition, An initiative of the Risk Response Network", World Economic Forum, 2012, http://reports.weforum.org/global-risks-2012/
[12] "Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives", Frederic Lemieux, Report GW-CSPRI-2011-2, 7 April 2011, http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-2%20Investigating%20Cyber%20Security%20Threats%20Lemieux.pdf
[13] "Cyber Security Threats and Responses at Global, Nation-State, Industry and Individual Levels", H. T. Klaar, 2011, http://www.ceri-sciencespo.com/archive/2011/mars/dossier/art_htk.pdf
[14] "Modern Trends In The CyberAttacks Against The CriticalInformation Infrastructure", E. Nickolov, ITU, Regional Cybersecurity Forum, 7-9 October 2008, Sofia, Bulgaria, http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolov-modern-trends-sofia-oct-08.pdf
[15] "Panetta: Cyber warfare could paralyze U.S.", CBS News, 5 January 2012, http://www.cbsnews.com/8301-18563_162-57353420/panetta-cyber-warfare-could-paralyze-u.s/
[16] Popularity of mobile banking apps makes them cybercrime targets: McAfee, Mobile Market, 3 January 2012, http://www.mobilemarketer.com/cms/news/research/11812.html
[17] The Cyber Market 2012-2022,Visiongain, December 2011, http://www.visiongain.com/Report/725/The-Cyberwarfare-Market-2012-2022
[18] 2010 Annual Study: U.S. Cost of a Data Breach, Symantec, March 2011, http://msisac.cisecurity.org/resources/reports/documents/symantec_ponemon_data_breach_costs_report2010.pdf
[19] "5 cyber threat predictions for 2012, Defense systems", 12 January 2012, http://defensesystems.com/Blogs/Cyber-Report/2012/01/top-cyber-threat-predictions-2012.aspx
[20] Privacy Violations Will Be Biggest Security Threat in 2012, PandaLabs, 15 December 2011, http://press.pandasecurity.com/usa/news/privacy-violations-will-be-biggest-security-threat-in-2012-says-pandalabs/
[21] "2012 Threats Predictions", Report by McAfee Lab, 28 December 2011, http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf
[22] "W32.Stuxnet Dossier, Version 1.4", N. Falliere, L.O. Murchu, E. Chien, Symantec Security Responses, 23 November 2011, http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf
[23] "W32.Duqu, The precursor to the next Stuxnet, Version 1.4", Symantec Security Responses, February 2011, http://www.symantec.com/ja/jp/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
[24] "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems", E Byres, A. Ginter, J. Langil, 22 February 2011, http://abterra.ca/papers/How-Stuxnet-Spreads.pdf