International Journal of Advance Research in Engineering, Science & Technology(IJAREST),
ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2, Issue 12, December- 2015. Impact Factor: 2.125

BlackEnergy a threat to Industrial Control Systems network security

Sejal Raval

Instrumentation and Control Engineering Department, Govt.Polytechnic, Ahmedabad

Abstract

BlackEnergy is an advanced malware that has been exploiting vulnerabilities in Linux- and Windows-based human machine interface products. HMIs are software interface that provides facility to users to monitor and communicate with industrial control systems. HMI can be dashboard type or graphical interface type. BlackEnergy malware targets at critical infrastructure, these security violation cause different cooperation and communications issues than the normal theft of personally identifiable information or financial information.

Keyword *-- Industrial Control Systems (ICS), SCADA (supervisory control and data acquisition), Distributed Denial of Service (DDoS),Cyber Emergency Response Team(CERT), advance persistent threat (APT), human machine interface (HMI), Simple Mail Transfer Pprotocol(SMTP),Transfer Control Protocol(TCP), Hyper Text Transfer Protocol(HTTP), Master Boot Record (MBR), personally identifiable information (PII), Visual Basic for Applications (VBA)*

I. INTRODUCTION

For internet-connected industrial systems Security is a critical issue. Automated companies that work with industrial control systems have been regularly targeted by attackers with a malware program called BlackEnergy. BlackEnergy is malware that can be used to damage, modify or disturb the industrial control systems. The Industrial Control Systems Cyber Emergency Response Team, a division of the U.S. Department of Homeland Security; found that Number of companies working with ICS have identified the malware on Internet connected human machine interfaces.

HMI is applications that provide a graphical user interface for monitoring and managing industrial machinery. They are a component of SCADA systems that are used in industrial environments, through these HMIs attackers gain deeper access of the industrial control systems. It is observed that the BlackEnergy attackers targeted HMI products from three different vendors: Cimplicity HMI of General Electric's, SIMATIC WinCC of Siemens' and WebAccess of BroadWin's.

BlackEnergy malware also used to destruct NATO alliance, energy firms and telecommunication companies. Russian cyberegroup like Sandworm is active in such attack. In recent attack it is exposed that some group exploited a zero-day Windows vulnerability.

II. MALWARE AND MALWARE AGENT

The malware is program code that is executed without target's permission and causing harmful functionality. The objectives of this software is 1) C**lose watch** of the system and/or its operators, including important information, such as passwords and private data. 2) S**tealing of data or intellectual property,** such as proprietary information of a business or confidential information of a government or military. 3) **Destruction** of one or more of the Data or executable code on the system, or other systems connected within network, sometimes damage of computer hardware, in the extreme case, it can damage to either an electromechanical machineries or process control system. In some case serious industrial accident results in loss of life or property or major economic damages.

2.1 Types of virus program

A virus is a program that infects target programs by copying destructive code into targets.

- Boot sector viruses are stored in disk boot sectors, and executed automatically at the boot time.
- Executable viruses are stored in executable files, that affects data and disrupt the flow-control of program.
- Macro viruses that are stored in non-executable data and started by opening a script or document.

A worm is a program that actively propagates over computer networks, with or without human involvement.

- Mass-mailers propagate with manual interaction and SMTP protocol.
- When a worm in memory it does propagates over TCP/HTTP, automatic execution on vulnerable systems and is very fast in nature.

A trojan horse is a program carrying a hidden functionality behind a useful one.

- It steals data from the system, this program have anti-detection mechanisms like encryption and polymorphism.
- combination of various malware types and techniques

2.2 Target of malware

Boot sector

In such attack malware saves the original MBR in a safe location than overwrite the original MBR with an infected one so then next boot time Bootstrap a system using the new MBR with virus infected MBR.

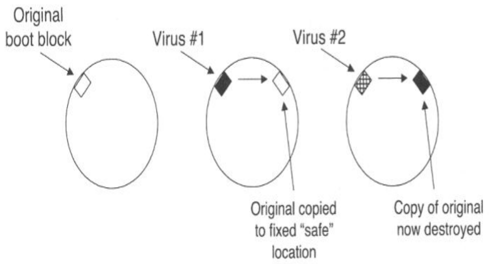

Original boot block
Virus #1
Virus #2
Original copied to fixed "safe" location
Copy of original now destroyed

Figure 2. *Boot sector virus*

COM Files

In such attack virus appends a virus body to a program than it saves original entry point of a program in a virus body. It replaces a program entry point with a jump to a virus body so this destructive code executed before original program than virus code restores the original entry point and jumps to it after its own execution

EXE Files

In this attack virus appends a virus body to a program than it overwrites a program header to switch the entry point to a virus code and jump to the original entry point during execution.

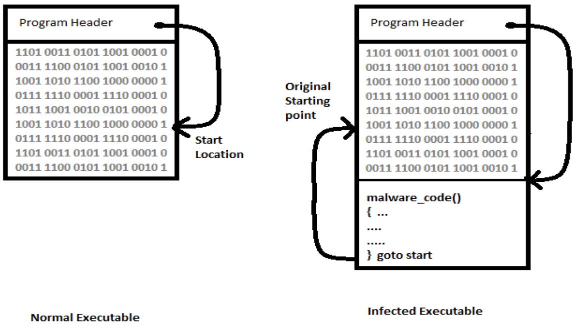


Figure 2. *Virus in EXE files*

Malware also uses MS-DOSs feature for expansion. In DOS if a command is typed without an extension, MS-DOS operating system first look for a named file with .COM extension and then look for an .EXE extension, In this process virus code injects a malicious program xyz.COM which then calls <abc.EXE> besides doing its dirty job.

Scripts and document

Malicious functionality is implemented in Visual Basic Applications. If a document template is infected it affects system memory than later on every document opened on a system will be affected.

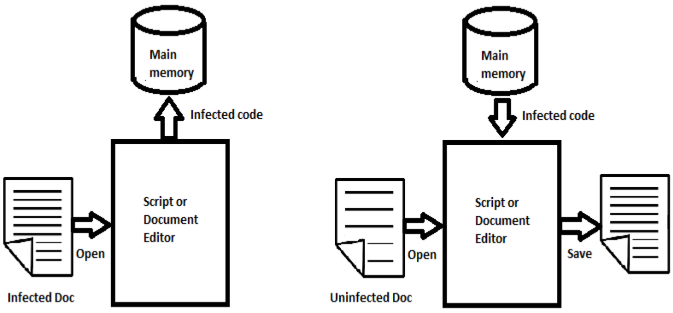


Figure 3. *Virus in script and document*

Example of macro viruses implemented in VB. A script is executed by a user by clicking at the email attachment. When user executes a VB script, the attachment name XYZ.TXT.vbs is shown in Outlook as XYZ.TXT (without extension!). As it is mass mailer the virus is spread to other outlook contact of your computer. Further destruction is possible via access to ActiveX objects. Read, write and overwrites the files, Access to ActiveX communication objects: send emails eval(), setTimeOut() ... , infection is also possible via opening of malicious web pages, automatic invocation during web browsing: Potential carriers are shell scripts, PHP, Perl, Python, Emacs, Tcl

Malware as cyberweapon

The BlackEnergy malware are initially not deployed as cyber weapons, but then later on it has been used to for military or intelligence objectives.

III. EVOLUTION OF BLACKENERGY

BlackEnergy is a malware designed to automate criminal activities, and initially that was sold in early 2007 by the Russian cyber underground. Originally, it was designed as a toolkit for creating botnets, which they use for DDoS attacks. After the years the malware has evolved to support different plugins, these plugins extend BlackEnergy malware's capabilities to provide various functions, depending on the purpose of an attack.

BlackEnergy has been used by different people for different purposes; some uses it for sending spam, others use it for thieving banking credentials. The most disreputable use may be when it was used to conduct cyberattack against Georgia during the Russo-Georgian conflict in 2008. In the mid of 2014, variants of BlackEnergy were used to target Ukrainian government institutions. The attackers using these customized BlackEnergy malware for stealing information from the targets. The use of this malware as an advance constant threat attack is interesting. In black ops important criteria is that the attack should not be attributable.

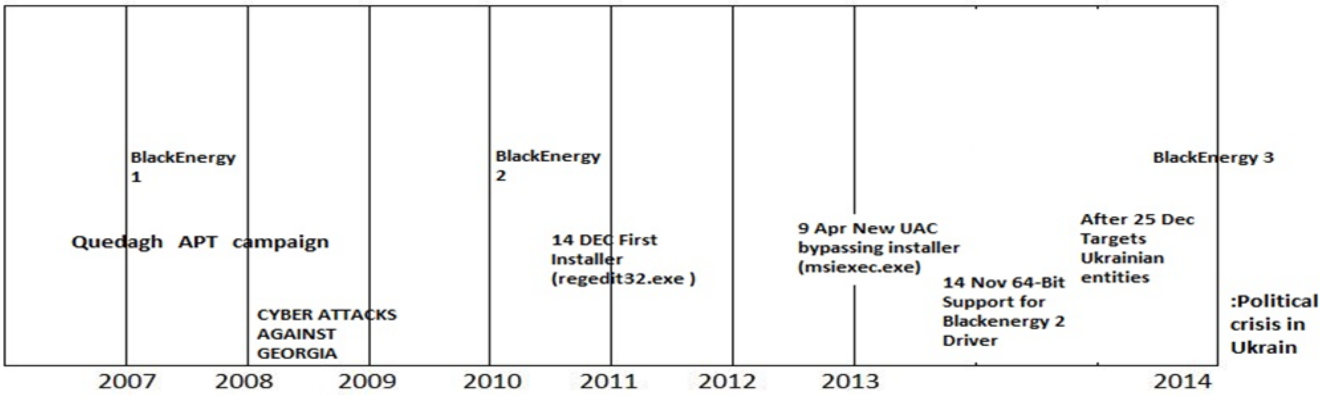

BlackEnergy 1
Quedagh APT campaign
CYBER ATTACKS AGAINST GEORGIA
BlackEnergy 2
14 DEC First Installer (regedit32.exe)
9 Apr New UAC bypassing installer (msiexec.exe)
14 Nov 64-Bit Support for Blackenergy 2 Driver
After 25 Dec Targets Ukrainian entities
BlackEnergy 3
:Political crisis in Ukrain
2007
2008
2009
2010
2011
2012
2013
2014

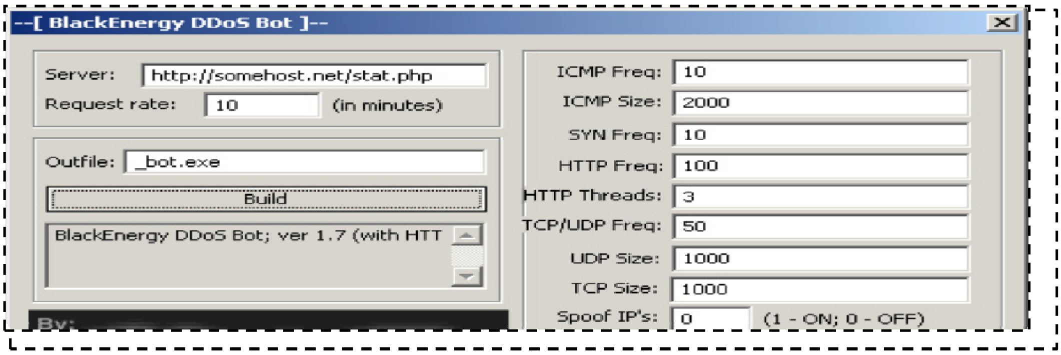
Figure 4. *Time line for BlackEnergy development*

BlackEnergy is a toolkit that has been used for years by various criminal groups. In the summer of 2014, certain samples of BlackEnergy malware used for stealing information from Ukranian government organizations. These samples were identified as the work of one group referred as "Quedagh", This group has a history of targeting political organizations. The use of BlackEnergy for a politically motivated attack is an interesting union of criminal activity and surveillance. As the kit is being used by multiple groups, it provides a greater measure of probable deniability than is afforded by a custom made piece of code.

The BlackEnergy toolkit first emerged in 2007 and is referred as BlackEnergy 1. A later variant of the toolkit (BlackEnergy 2) was released in 2010, And some unseen variant, which had been rewritten and uses a different format for its configuration. BlackEnergy3 is a latest malware that can affect ICN and does not require driver component to propogate.

IV. ATTACK

Industrial control systems are receiving the malware via targeted emails containing malicious attachments. The BlackEnergy toolkit comes with a builder application. This application is used to generate the code that the attackers use to infect target machines. Server-side scripts are also included in this toolkit. The attackers use these scripts to set up in the command and control server.


--[BlackEnergy DDoS Bot]--

Server: http://somehost.net/stat.php
Request rate: 10 (in minutes)

Outfile: _bot.exe

BlackEnergy DDoS Bot; ver 1.7 (with HTT

ICMP Freq: 10
ICMP Size: 2000
SYN Freq: 10
HTTP Freq: 100
HTTP Threads: 3
TCP/UDP Freq: 50
UDP Size: 1000
TCP Size: 1000
Spoof IP's: 0 (1 - ON; 0 - OFF)

Figure 5. *BlackEnergy Builder from 2007*

The scripts also provide an interface where an attacker can control his bots. The main features of this toolkit are simplicity and convenience because of that anyone who has access to the kit can build his own botnet with the ease.

Most of the recent BlackEnergy installers collected are named msiexec.exe. They are either dropped by another executable that uses social engineering tricks to mislead the user and executes infected installer, the document that contains malware code that silently perform the installation.

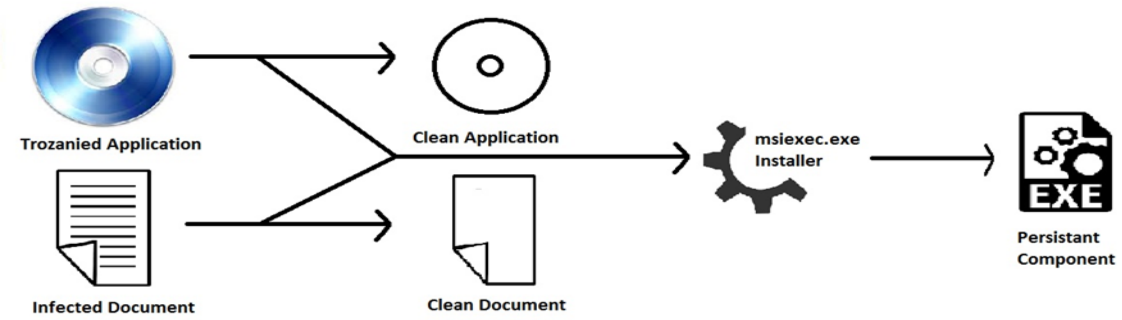
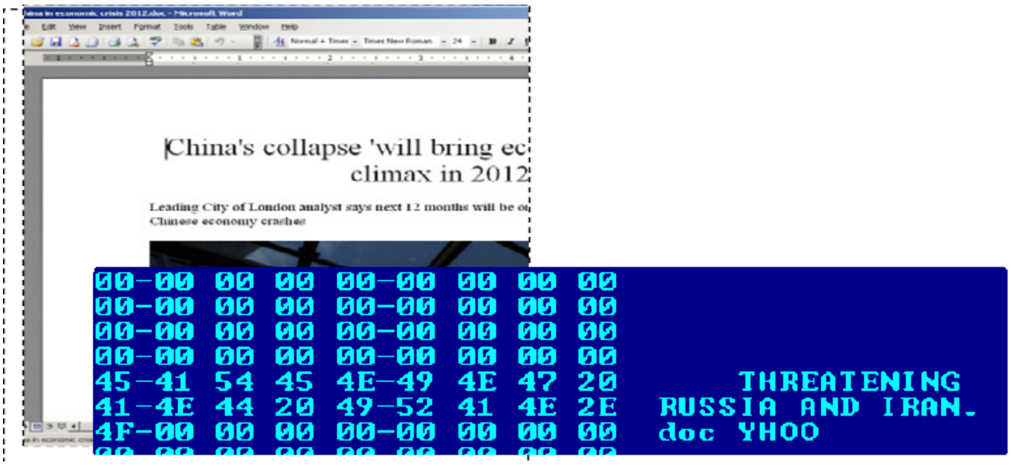


Figure 6. *Infection process*

Attack using Document

It is found that at least 2 trojanized legitimate applications that execute the installer in addition to their regular tasks as shown in figure 7. Trojanization is an effective infection method, as most users unaware about infected code are being installed simultaneously with a legitimate program.

Earlier installer variants later on named regedt32.exe, were distributed by documents exploiting software vulnerabilities, one of which was CVE-2010-3333. These documents drop the installer and execute it, then open a trap document. It is believed that a similar approach is used to deliver the recent installer variants.
The installer filename of BlackEnergy 3 is still msiexec.exe. However this executable file delivered and executed by a dropper, which opens a fake document in the foreground. It is also noticed that a standalone, non-persistent sample that pretends to be well known application installer, and when user going to proceed with installation this malware damages the system. It does not use any fake document or application and does not run after reboot.


hina in economic crisis 2012.doc - Microsoft Word
Edit View Insert Format Tools Table Window Help

China's collapse 'will bring ec
climax in 2012

Leading City of London analyst says next 12 months will be o
Chinese economy crashes

```
00-00 00 00 00-00 00 00 00
00-00 00 00 00-00 00 00 00
00-00 00 00 00-00 00 00 00
00-00 00 00 00-00 00 00 00
45-41 54 45 4E-49 4E 47 20       THREATENING
41-4E 44 20 49-52 41 4E 2E   RUSSIA AND IRAN.
4F-00 00 00 00-00 00 00 00   doc YHOO
```

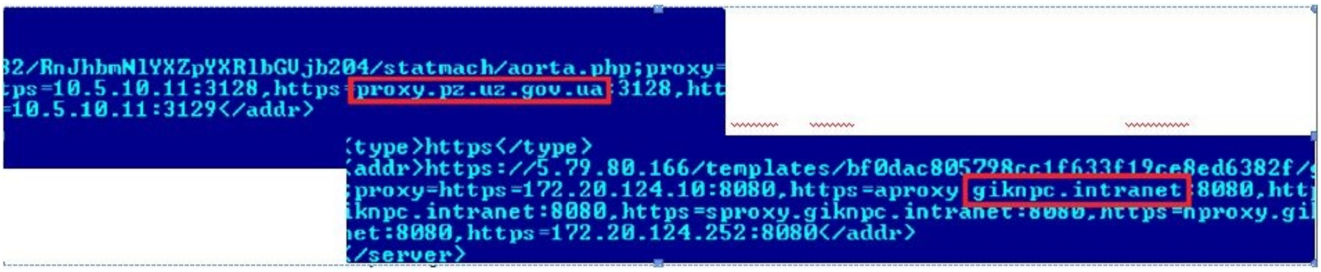
Figure 7. *Circa (document) and string embedded inside document*

For example, one document found in 2012 about discussion of a political/economic situation but in real it contained decoy dropper for targeting European audiences. In another sample from 2012 strings found that again clearly indicates a political intention behind the attack. Mostly decoys used contents are latest news article taken from news sites.

Attack using Proxy Server

During BlackEnergy monitoring, it is noticed that new samples found in current year had been updated to support the use of proxy servers while connecting to their C&C servers. While earlier BlackEnergy 2 variants does not have capabilities to manipulate proxy servers. In network setups, a use of proxy server is very common to allow internal users to access the Internet. BlackEnergys attack where use of a proxy server detected may indicate that the attacker has sufficient knowledge of the target organization.

Example below shows malware sample where configuration uses the proxy server associated with the Ukrainian Railway (Figure 4). The configuration from another sample also shows it using an internal proxy under the giknpc domain. The domain giknpc.com.ua in turn hosts 3 domains(Table 4,5).



```
32/RnJhbmN1YXZpYXR1bGUjb204/statmach/aorta.php;proxy=
tps=10.5.10.11:3128,https=proxy.pz.uz.gov.ua:3128,htt
=10.5.10.11:3129</addr>
                          <type>https</type>
                          <addr>https://5.79.80.166/templates/bf0dac805798cc1f633f19ce8ed6382f/
                          proxy=https=172.20.124.10:8080,https=aproxy.giknpc.intranet:8080,htt
                          iknpc.intranet:8080,https=sproxy.giknpc.intranet:8080,https=nproxy.gi
                          net:8080,https=172.20.124.252:8080</addr>
                          </server>
```

Figure 8. *Configuration using Ukrainian Railway's proxy*

Table 1. Network Information

IP Address	195.64.190.1
Reverse DNS (PTR record)	Relay.glknpc.com.ua
DNS server (NS record)	ns.glknpc.com.ua (195.64.190.1)
	ns2.glknpc.com.ua (195.24.137.86)

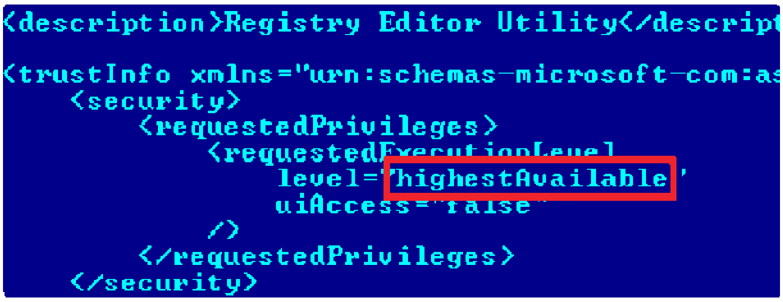
Table 2. Hosting Information

No of Domains hosted	3
No of mail server hosted	1
No of name servers hosted	1

Domains on 195.64.190.1 - adm.dp.ua, gknpccom.ua, dp.gov.ua

Attack using regedit32

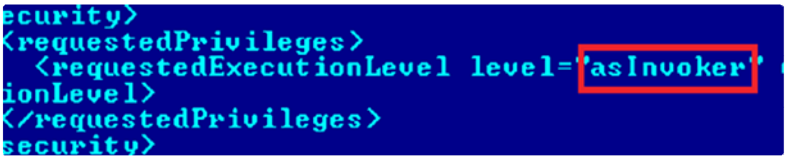
Initially, filename of the Windows registry editor (regedt32.exe) used for malware, presumably because the installer needs administrator rights to install its driver component and therefore would try to request for the highest available rights (Figure 5). As this triggers a notification message visible to the user, said user is more likely to grant permission because it appears to be the registry editor that is requesting for some permission, since it is normal run it with administrator rights. Experienced users though are less likely to be taken in, thereby decreasing the likelihood of a successful infection.



```
<description>Registry Editor Utility</descript
<trustInfo xmlns="urn:schemas-microsoft-com:as
    <security>
        <requestedPrivileges>
            <requestedExecutionLevel
                level="highestAvailable"
                uiAccess="false"
            />
        </requestedPrivileges>
    </security>
```

Figure 9. *Installer requesting highest available rights*

Starting April 2013, modified installers appeared showing that the Quedagh group found a way to bypass the default User Account Control (UAC) settings. With this change, the user's permission is no longer required (Figure 7). At this point, the gang also began to use the Windows installer program filename msiexec.exe.



```
ecurity>
<requestedPrivileges>
  <requestedExecutionLevel level='asInvoker' 
ionLevel>
</requestedPrivileges>
security>
```

Figure 10. *Installer execution level amended*

The Quedagh-related customizations to the BlackEnergy malware include support for proxy servers and use of techniques to bypass User Account Control and driver signing features in 64-bit Windows systems.

V. CONCLUSION

BlackEnergy attacks are especially challenging from other virus that can defect communications and confidentiality perspective. Researchers have identified a plugin module called “dstr” that is use by hackers to irretrievably wipe hard disks and so they hide their presence or attack. The industrial control networks are in organizations that is fully automated and severely affected due to malware attacks because such attack can disrupt production assembly that ultimately converted into huge financial losses, as in the case of Ukraine and Georgia where political crisis are occurred.

The ISN is connected with internet and local network, so the technical challenge is to secure Internet connected automated machineries from cyber network attacks, as well as local physical attacks. A similar challenge exists for the cloud-hosted services, such as data analytics. The business challenge is to ensure that security is taken seriously and designed in by the equipment vendors, not looked at as a cost centre and patched on after the plant operation.

REFERENCES

[1]. Broderick Aquilino; F-Secure Weblog; BlackEnergy Rootkit, Sort Of; 13 June 2014; http://www.f-secure.com/weblog/archives

[2]. Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS By Tyson Macaulay , Bryan L. Singer.

[3]. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems By by Eric D. Knapp , Joel Thomas Langill.

[4]. Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and ... such as Programmable Logic Controllers (PLC) By by nist

[5]. Robust Control System Networks: How To Achieve Reliable Control After Stuxnet by Ralph Langner.

[6]. Practical Malware Analysis - The Hands-On Guide to Dissecting Malicious Software by by Michael Sikorski.

[7]. Broderick Aquilino; F-Secure Weblog; Beware BlackEnergy If Involved In Europe/Ukraine Diplomacy; 30 June 2014; http://www.f-secure.com/weblog/archives

[8]. Kafeine; Malware don’t need Coffee; BotnetKernel (MS:Win32/Phdet.S) an evolution of BlackEnergy ; 21 June 2014

[9]. http://malware.dontneedcoffee.com/2014/06/botnetkernel

[10]. Joe Stewart; DELL SecureWorks; BlackEnergy Version 2 Analysis; 3 March 2010; http://www.secureworks.com/cyber-threat-intelligence/threats/blackenergy2/

[11]. http://www.edelman.com/post/confidentiality-disclosure-considerations-dealing-blackenergy-malware by Aravind Swaminathan and David Chamberlin Published November 10, 2014

[12]. http://www.computerworld.com/article/2840164/attack-campaign-infects-industrial-control-systems-with-blackenergy-malware by Lucian Constantin

[13]. http://www.cogsys.cs.uni-tuebingen.de/lehre/ws12/introsec/11-intro-malware.pdf

[14]. The Art of Computer Virus Research and Defense by Peter Szor

[15]. Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware by Aditya Sood