GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"ICS/SCADA Security Essentials (Industrial Control Systems 410)"
at http://www.giac.org/registration/gicsp

The Impact of Dragonfly Malware on Industrial Control Systems

GIAC (GICSP) Gold Certification

Author: Nell Nelson, Nell.Nelson@Pfizer.com

Advisor: Rob VandenBrink

Accepted: January 18, 2016

Abstract

Dragonfly malware infected hundreds of business computers in an often successful attempt to collect information on industrial control systems across the United States and Europe. The attack was performed in an orchestrated manner over an extended period of time and used infection methods that were difficult to detect and thwart. The malware collected information vital to the operation of the impacted systems across the energy and pharmaceutical sectors. This abstract will explore the impact of Dragonfly Malware on systems used for automated industrial control. The content will explain the manner in which Dragonfly infiltrated business systems in both Europe and the United States, how it was discovered, and the immediate and future impact of the malware on infected systems and on the ICS industry. This paper will also discuss ways in which the industry can safeguard itself against future attacks similar to the Dragonfly malware effort.

© 2016 The SANS Institute Author retains full rights.

Table of Contents

1. Introduction 3
2. ICS Cyber-espionage 3
2.1 ICS Malware Overview 3
2.2 Dragonfly Campaign Introduction 5
3. Dragonfly Campaign Details 6
3.1 Three Phased Attack 6
3.2 Dragonfly RATS 6
3.3 Havex Components 7
3.4 XP Vulnerability 9
3.5 Vendor Websites 10
4. Dragonfly Malware Impact on Industry 11
4.1 Global Impact 11
4.2 Energy Sector Target 12
4.3 Pharma Target 13
4.4 Future Impact 14
5. How to Defend Against Cyber-espionage Attacks 15
5.1 Urgent Need for Better Defense 15
5.2 Defense in Depth 16
5.3 Network Segmentation 18
5.4 Cyber Security Standards and Information Sources 20
6. Conclusion 21

© 2016 The SANS Institute Author retains full rights.

1. Introduction

During the past several years and ending in 2014, Dragonfly malware infected hundreds of business computers in an often successful attempt to collect information on industrial control systems across the United States and Europe. The attack was performed in an orchestrated manner over an extended period of time and used infection methods that were difficult to detect and thwart. The malware collected information vital to the operation of the impacted systems across the energy and pharmaceutical sectors.

This document will describe industrial control systems and cyber-espionage at a high level, and introduce the Dragonfly malware campaign. This generalized information is followed by an explanation of the manner in which Dragonfly infiltrated business systems in Europe and the United States, the malware discovery and research performed by security experts, and the immediate and future impact of the malware on infected systems and on the ICS industry. The final section of the document discusses ways in which the industry can safeguard itself against future cyber-espionage attacks.

2. ICS Cyber-espionage

2.1 ICS Malware Overview

Industrial control systems (ICS) are used throughout the world to monitor, control, and automate processes used in a host of manufacturing industries such as chemical and pharmaceutical production. These systems are also used to produce our most necessary utilities to provide electricity and water. In short, many of our most basic needs are met through use of

© 2016 The SANS Institute Author retains full rights.

industrial automation control systems. According to Hayden, et al (2014), the International Society of Automation (ISA) has stated a definition of Automation and Control Systems as being "a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process" (Hayden, et al, 2014).

In the past several years, various malware campaigns have specifically targeted manufacturing and utility processes through attacks related to the associated ICS. These campaigns can be categorized as cyber-espionage, meaning they are very targeted with respect to the victim and are purposed to steal information. Other types of cyber-attacks such as cyber-crime seem to be primarily interested in financial gain which may or may not require data to be collected from the victim. The targets are likely to be widespread in order to increase the likelihood that someone will fall victim to the attack. Cyber-crime often uses email phishing as a system entry tool. In contrast, cyber-espionage perpetrators are interested in very specific information or capabilities from a selected victim. A spear-phishing, or very selective, email campaign may be used to gain information that will allow further entry to the target. The goal is likely to be the collection of trade secrets or process information that may be used to compromise the victim's industrial concerns (Wangen, 2015).

Another hallmark of a cyber-espionage attack is that the malware is often an Advanced Persistent Threat (APT), meaning that the malware is designed to become resident on the victim's system in order to collect information over an extended period of time without being discovered. APT executed against automated industrial processes requires expert knowledge of both information technology and of the particular industrial systems used. A general assumption is, therefore, that cyber-espionage attackers probably have significant financial and knowledge resources such as that provided by a foreign government (Wangen, 2015).

© 2016 The SANS Institute Author retains full rights.

2.2 Dragonfly Campaign Introduction

The Dragonfly cyber-espionage campaign seemed to have been perpetrated by attackers with ample funding and technical know-how. The campaign began in late 2010, but was not discovered until 2013, when spear-phishing efforts alerted cyber security firms to a possible cyber-attack against energy firms in the U.S. and Europe. Although previous espionage campaigns such as Stuxnet, which attacked 1,000 uranium enrichment centrifuges in Iran, had resulted in an awareness in the manufacturing and utility sectors of the destructive capabilities of such malware, the occurrences were rare and defenses limited (Constantin, 2014). The significance of Dragonfly is that it was the first advanced attack since Stuxnet to target ICS components ("Dragonfly malware," 2014)

The group orchestrating the espionage attack was dubbed Dragonfly by Symantec, a cyber-security specialist company, and named Energetic Bear by other vendors. Dragonfly's initial targets were the aviation and defense industries in the U.S. and Canada, but expanded into the energy sector in early 2013. In February of 2013, Symantec observed a spear-phishing campaign that appeared to target specific organizations to seek confidential information. High level individuals were targeted, signifying a substantial amount of intelligence was used in planning the attack. The email campaign continued until June, 2013. Around that time, the attack began using the watering-hole technique which involved redirection of website addresses to those controlled by the Dragonfly group. Software with malicious content was hosted on the sites and unknowingly transferred to various company networks by the victims themselves. The attackers also began to use websites owned by ICS product vendors to insert the malware directly into software that would be downloaded and used by those concerned with ICS systems.

© 2016 The SANS Institute Author retains full rights.

The complexity of this targeted cyber-espionage attack was indicative of a well-funded effort (Langill, 2014).

3. Dragonfly Campaign Details

3.1 Three Phased Attack

The Dragonfly cyber-espionage effort was performed in three phases. The first used a spear-phishing campaign to infect victims computers and gain information regarding their network and business from resident files. The primary malware technique used by Dragonfly was a remote access Trojan horse (RAT). A RAT is malware that provides remote administrative control over an infected computer. Following the spear-phishing campaign, the software, named Havex by the cyber security group F-Secure, was also used in watering hole attacks. These attacks used redirection of legitimate websites, which would be visited by industry experts, to Dragonfly servers which contained software infected by Havex. Later, a third phase of the campaign included legitimate applications which had been hacked into by Dragonfly on industrial control vendor websites from which businesses would download the Havex infected software (Symantec Security Response, 2014).

3.2 Dragonfly RATS

Havex was used to extract information from victims' computers regarding network details, and from Outlook email, including contact lists, and send the data to servers used by the Dragonfly group (Goodin, 2014). The network detail collected was that required by the infected computer for remote access into the control networks. Some Havex software also targeted OPC (Ole for Process Control) information. OPC is used as a communication interface to ICS applications. As is typical for the RAT type of malware, Havex acted as a conduit for entry of

© 2016 The SANS Institute Author retains full rights.

other malware sent by Dragonfly servers to the compromised computers and as the installer of the software. One example of the payloads was Karagany, an additional Trojan Horse ("Industrial Control Vendors," 2014). The Karagany RAT used on some infected computers could collect passwords and take screenshots. Karagany was able to upload and download files for collection and send them to Dragonfly servers (Langill, 2014). Additionally, Karagany could run shells and load DLLs. Dragonfly also employed a password stealer module that had an embedded browser password decrypter and a network scanner that looked for SCADA software (Wangen, 2015).

Havex appears to have been developed by the Dragonfly group. According to Goodin (2014), "The group bears the hallmarks of a state-sponsored operation, mainly in its organization and high degree of technical sophistication. Its primary motive appears to be espionage, although additional capabilities suggest that sabotage is also of interest. Fingerprints left inside the malware show the attackers mostly worked Monday through Friday during a nine-hour period that corresponded to 9am to 6pm in Eastern Europe, leading Symantec researchers to theorize that was the region where the most Dragonfly members worked" (Goodin, 2014).

3.3 Havex Components

Havex used an OPC malware scanning module to gather information about ICS devices and send that data back to Command and Control (C&C) servers used by the Dragonfly group. The malware used an industrial protocol scanner to find networked devices on TCP ports 44818, 102 and 502. Automation companies such as Siemens and Rockwell Automation use these ports for ICS system communication. The industrial processes using the protocols are found in consumer goods manufacturing and packaging applications (Virgillito, 2014). As stated by F-Secure personnel studying Dragonfly, "It appears that this component [Havex] is used as a tool

© 2016 The SANS Institute Author retains full rights.

for intelligence gathering. So far, we have not seen any payloads that attempt to control the connected hardware" (Constantin, 2014).

Nevertheless, the attack was an ambitious undertaking in that it used industrial software suppliers in order to propagate the malware to the victims. The main components of Havex are the remote access Trojan and a server module written in PHP ("Havex Hunts," 2014). Figure 1, below, shows the compromised installer files from one of the vendor victims. Note the normal installer does not contain a file called mbcheck.dll. That is Havex. A user who downloads and executes this software package will have an open backdoor into his system.

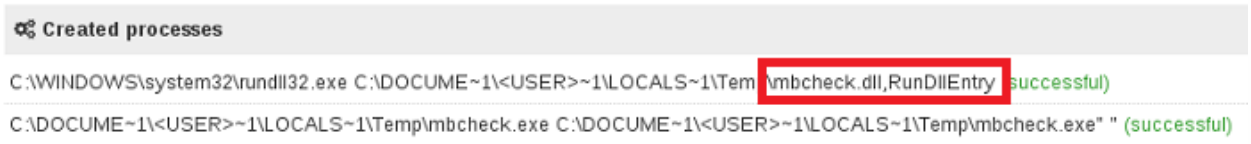

Figure 1 Havex installer files ("Havex Hunts," 2014)

In Figure 2 below, the name 'Havex' clearly written in the source code captured in the article, "Havex Hunts," (2014).

```
define("PATH_BLOCKFILE", "block.tmp");
define("PATH_LOGFILE", "testlog.php");
define("DATATAG_START", "<html><head><mega http-equiv='CACHE-CONTROL' "
       "content='NO-CACHE'></head><body>No data!<!--havex");
define("DATATAG_END", "havex--></body></head>");
define("NODATA", "<html><head><mega http-equiv='CACHE-CONTROL' "
       "content='NO-CACHE'></head><body>Sorry, no data corresponding your request."
       "<!--havexhavex--></body></html>");
define("ANSWERTAG_START", "<xdata d='%s' u='%s'>");
define("ANSWERTAG_END", "</xdata>\n");
define("FILE_OUTPUT_BLOCK_SIZE", 16384);
```

Figure 2 Havex source code excerpt ("Havex Hunts," 2014)

According to research, described in the article, "Havex Hunts," (2014), the backdoor is then used by a C&C to download and execute further components. It was confirmed by "Havex Hunts," (2014), the malware enumerates the local area network devices as it looks for connected

© 2016 The SANS Institute Author retains full rights.

resources and servers. It also uses Microsoft Component Object Model (COM) interfaces (CoInitializeEx, CoCreateInstanceEx) to connect to specific services. The Havex executable made many references to 'OPC;' and was configured to gather details about connected ICS equipment and upload the information to Dragonfly servers ("Havex Hunts," 2014). As Langill (2014) points out, "The problem is that without taking additional security measures, Havex-infected users may also be able to connect to OPC servers and perform unintentional actions, such as writing new values to the process database. The Havex OPC module did not include these capabilities, but given the proof-of-concept code that is now available, it would be a trivial task for the attackers to extend the functionality of the Havex OPC module to include other more destructive OPC calls" (Langill, 2014).

3.4 XP Vulnerability

Vulnerabilities existing in computers using the Windows XP operating system were exploited by Dragonfly. More than fifty percent of the infected computers were running XP. Industrial processes use XP in many of the automation systems due to a reluctance to modify operating systems. This situation can be attributed in part to the expectation that industrial equipment will operate as installed for many years, and, therefore, computers are not updated as often as might be the case in the business world. Another large issue for regulated processes, such as those used in the pharmaceutical industry, is that any change to a system may trigger validation, which is an extensive and expensive reexamination and testing of the modified process. A government regulatory requirement for validation of a system is often the reason XP computers are left in place in ICS systems, even when the operating system is no longer supported by the OS manufacturer. Of significant concern, though, is that Windows XP does not provide advanced security mechanisms as do more modern Microsoft (MS) Windows operating

© 2016 The SANS Institute Author retains full rights.

system versions. Dragonfly Havex was able to install new or updated applications on XP computers even when the user was not authorized to do so. Research proved the malware executed and functioned properly even when restricted user accounts were used (Langill, 2014).

3.5 Vendor Websites

Three vendor websites were used to propagate the infected Dragonfly malware, and vulnerabilities existed in each of these locations that were exploited by the cyber-espionage group. The eWon Company reported its website had been attacked in January of 2014. The perpetrators used the website's content management system to insert the malware file into the Talk2Me application setup package. Talk2Me was used to provide virtual private network (VPN) access to ICS equipment known as programmable logic controllers (PLC). The link for download of the software was changed to point to the modified package. The company estimates approximately 250 users downloaded the corrupt software, before it was discovered ("Industrial Control Vendors," 2014).

Another compromised vendor was a European manufacturer of PLC devices. The malware was inserted into the driver package for the vendor's software and was available for download for six weeks in June and July of 2013. The third vendor used by Dragonfly manufactured control systems for energy infrastructure, such as wind turbines. The malware was available for about ten days in April, 2014. Obviously, the Dragonfly group was thinking strategically by attacking vendor websites that are typically left unsecured for access by industrial manufacturing and utility experts. Why attack one victim at a time when hundreds can be had so easily (Symantec Security Response, 2014)?

None of the websites required authorization for access to the ICS software available for download. During research into the vendor website infiltration method used by Dragonfly, and

© 2016 The SANS Institute Author retains full rights.

described in "Havex Hunts," (2014), investigators collected and analyzed 88 different versions of Havex and revealed 146 Command and Control servers used by the software. The C&C servers were primarily compromised websites used for blogs and the like ("Havex Hunts," (2014).

Investigation also led to the discovery of around 1500 IP addresses of probable victims. The assumption being that IP addresses communicating with the C&C servers were infected with Havex. All of the IP addresses that were investigated and led to the identification of an infected system were, according to "Havex Hunts," (2014), associated with "the development or use of industrial applications or machines. The majority of the victims are located in Europe, though at the time of writing, at least one company in California was also observed sending data to the C&C servers. Of the European-based organizations, two are major educational institutions in France that are known for technology-related research; two are German industrial application or machine producers; one is a French industrial machine producer; and one is a Russian construction company that appears to specialize in structural engineering" ("Havex Hunts," 2014).

4. Dragonfly Malware Impact on Industry

4.1 Global Impact

As stated in Langill (2014), Eric Byres, CTO of Tofino Security and a world authority on industrial cyber security, made these remarks concerning the Dragonfly cyber-espionage attack:

"While Dragonfly's creators appear to have intended this attack to be non-destructive and for intellectual property theft only, it is clear that the malware design makes it potentially far more dangerous to live process control operations."

© 2016 The SANS Institute Author retains full rights.

"At some point, should they wish it to be a destructive attack, it will be trivial for them to modify the downloaded modules and seriously impact their victims' operations. Since we don't know the Dragonfly team's motives, any company facing an attack like this must assume the worst-case scenario in their risk analysis and proceed accordingly" (Langill, 2014).

Clearly, although Dragonfly did not cause destruction of property, the impact was and is potentially great. Victims included industrial and energy entities across the globe. Figure 3, below, shows the impact by country:

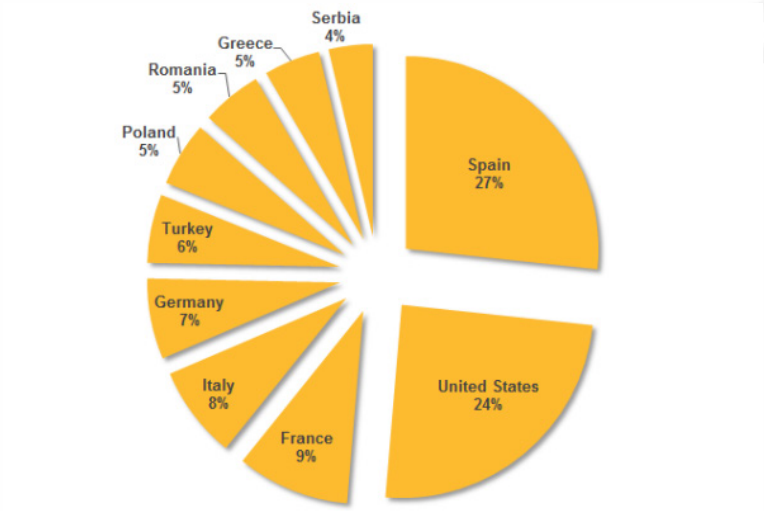

Figure 3. Top 10 countries by active Dragonfly infections (where attackers stole information from infected computers) (Symantec Security Response, 2014).

4.2 Energy Sector Target

The Symantec Company was among the first to be aware of and to research the Dragonfly cyber-espionage effort. Their information led them to believe the attack was targeting the energy sector; specifically, "energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers." ("Industrial Control Vendors," 2014). Another security intelligence company, CrowdStrike, associated the Havex Rat with the energy sector, as well, and dubbed it, Energetic Bear. CrowdStrike believed

© 2016 The SANS Institute Author retains full rights.

the attackers were linked to the Russian Federation and were active as early as August, 2012 (Constantin, 2014).

Our modern world depends on electrical power for most communications, water delivery, food processing, and industrially produced goods. The security of the energy sector is paramount to our civilization; we can hardly function without it. According to Soifer and Gouré (2014), the U.S. electrical grid endures 10,000 cyber-attacks every month. Three continents have had major issues with such attacks, which have shutdown utilities in some cases. The costs associated with these attacks in the U.S. is in the billions of dollars each year. The Dragonfly cyber-espionage group "compromised the computer systems of more than 1,000 energy companies in the United States and Europe" (Soifer and Gouré, 2014).

4.3 Pharma Target

Due to the importance of the critical energy infrastructure and the belief that other industries may have been impacted, in 2014, the Belden Company contracted Joel Langill from Redhat Cyber, an independent expert in cyber security, to investigate the Dragonfly attack in order to understand the full impact to industry and provide advice to aid in protecting ICS networks against future attacks. The investigation was performed by executing the Havex code as it would have been in the real world and analyzing the results. Interestingly, Mr. Langill's research revealed a previously unknown primary target of the Dragonfly cyber-attack to be the pharmaceutical sector ("Dragonfly malware," 2014).

The reasons for determining the actual target of Dragonfly was confidential knowledge of the pharma industry were three fold, as stated by "Dragonfly malware" (2014):

> "1. Out of thousands of possible ICS suppliers, the three companies targeted for trojanized software were not primary suppliers to "energy" facilities. Instead, all three

© 2016 The SANS Institute Author retains full rights.

offered products and services [were] most commonly used by the pharmaceutical industry.

2. The Dragonfly attack is very similar in nature to another campaign called Epic Turla and is likely managed by the same team. Epic Turla has been shown to have targeted the intellectual property of pharmaceutical companies.

3. The Dragonfly malware contained an Industrial Protocol Scanner module that searched for devices on TCP ports 44818 (Omron, Rockwell Automation), 102 (Siemens) and 502 (Schneider Electric). These protocols and products have a higher installed base in packaging and manufacturing applications typically found in consumer packaged goods industries, such as pharmaceutical, rather than the energy industry" ("Dragonfly malware," 2014).

"My research, coupled with my knowledge of the pharmaceutical industry, led me to conclude that it [pharma] was the target of Dragonfly," remarked Langill. "The potential damage could include the theft of proprietary recipes and production batch sequence steps, as well as network and device information that indicate manufacturing plant volumes and capabilities" ("Dragonfly malware," 2014).

In support of Joel's proposal that pharmaceutical companies were targeted, Virgillito (2014) points out the three vendors targeted by the website RATS, out of thousands of possibilities, were primarily suppliers of software used by the consumer goods production sector (Virgillito, 2014).

4.4 Future Impact

The impact of the Dragonfly cyber-attack was not tangible in regards to loss of energy infrastructure function or industrial processes, but that potential impact still exists for the victims

© 2016 The SANS Institute Author retains full rights.

who were infected with the Havex malware. The software enabled the espionage group to collect network and equipment information valuable for the execution of a later attack. Additionally, the malware module that allowed scanning of OPC devices and VPN settings could be used to compromise suppliers of ICS maintenance agreements. eWON reportedly has a million remote connections in order to provide support to customers. As stated by Mr. Langill (2014), "Once these remote systems are connected, it is probable that they are directly connected to ICS networks. Without additional security measures, there is little that can be done to restrict the impact of these infected remote clients" (Langill, 2014).

5. How to Defend Against Cyber-espionage Attacks

5.1 Urgent Need for Better Defense

Eric Byres, CTO of Tofino Security, and a world authority on industrial cyber security made the following statements regarding the need for industry to guard against ICS attacks:

"Security researchers and hackers have identified numerous vulnerabilities in the products used in industrial operations. Post Dragonfly, it is important that manufacturing companies secure core ICS through up-to-date best practice policies and industrially focused security technologies," Byres added. "We know now that Stuxnet and Flame remained hidden in their target networks for years – by the time worms like these do damage or steal trade secrets, it is too late to defend against them" (Virgillito, 2014).

"The combination of Dragonfly's 'Offense in Depth' strategy and the fact that it circumvented traditional desktop security controls highlights the urgent need for matching Defense in Depth security on the plant floor. Not only do we need to defend the ICS devices, but industry also needs to consider better defenses for the ICS network...The fact that the Dragonfly

© 2016 The SANS Institute Author retains full rights.

campaign ran for almost a year without detection shows that the monitoring and control of ICS traffic (especially outbound traffic) is still unacceptably poor in many industries" (Langill, 2014).

Many of cyber security tools traditionally used for defense against malware attacks would not have worked against Dragonfly's Havex, because it was inserted into software that was obtained by users authorized to install such software on the their company's network. Additionally, no virus scanning or intrusion detection appliances were armed against Dragonfly until after it had been active for well over a year. Application whitelisting, blacklisting, host firewalls, network user accounts, and VPNs were all ineffective security defensives against the cyber-espionage attack. Important to note is that Havex was designed to be installed on a computer in a remote access network VPN configuration and, from there, identify ICS related services (Langill,2014).

The situation is not hopeless, however, and ICS networks can be hardened against attacks such as that perpetrated by Dragonfly. For instance, industrial combination VPN/stateful firewall routers are available that can limit the IP addresses and TCP destination port traffic allowed in the VPN tunnel. Although this tool may not have stopped Dragonfly entirely, the point is that the malware may have been limited in its ability to scan and/or infect an entire ICS network, thereby limiting its future sabotage capabilities (Langill, 2014).

5.2 Defense in Depth

A "defense-in-depth" strategy is needed to provide such limitation of access to the ICS devices, especially those that directly control industrial equipment and processes, or provide environmental safety. For this strategy to be successful, a process must be established to create and maintain operational security of the ICS network. The following lists steps to address when implementing the "defense-in-depth" approach, as stated by Rockwell Automation (2009):

© 2016 The SANS Institute Author retains full rights.

"1) Identify priorities (e.g. Availability, Integrity, Confidentiality)

2) Establish requirements (e.g. remote access must not impact control traffic, etc.)

3) Identify assets

4) Identify potential internal and external threats and risks

5) Understand capabilities required

6) Develop architecture

7) Develop and implement policies" (Rockwell Automation (2009)

Additionally, security must be built into the various ICS concerns during the design of these systems and not as an afterthought of implementation. According to Rockwell Automation (2009), areas of attention for secure systems are:

- Physical security – panels and areas that house ICS equipment and cable connections should not be accessible to unauthorized personnel.
- Network security – stateful firewalls and deep packet IDS/IPS appliances should be used, along with ruggedized switches and routers, designed for the environment in which they will be used and for communications using ICS protocols.
- Computer hardening – patch management and anti-virus protection are necessary along with change management including removal/disabling of unused ports, services, and applications.
- Application security – configuration and management of application access through authentication, authorization, and audit software Rockwell Automation (2009) is essential. Remember, though, access and auditing the software access requires a standardized process to maintain and derive valuable security benefit.

© 2016 The SANS Institute Author retains full rights.

- Device hardening – security for device management involves change control, and physical and logical access control, as well.

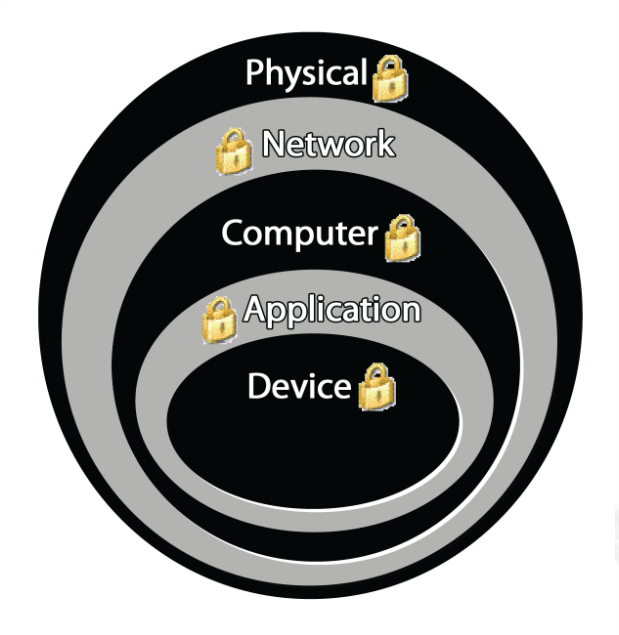

Figure 4 - 'Defense in Depth' strategy (Rockwell Automation, 2009)

5.3 Network Segmentation

Industrial processing and enterprise networks have converged to allow business enterprise access to manufacturing data for use in systems such as those used for inventory and financial management. The information is also provided to manufacturing management and process improvement personnel to aid in optimization of production. However, these communication benefits expose the industrial control systems to the same malicious cyber-espionage and crime endured by the business networks (Rockwell Automation, 2009).

Network standards, such as ISA62443 from the International Society of Automation, have been written to provide an architecture for ICS systems to provide restriction of network traffic in accordance with a functional zoning structure. The lowest network layer, or zone, houses basic control devices such as programmable logic controllers. These devices

© 2016 The SANS Institute Author retains full rights.

communicate with the industrial equipment in order to control critical process variables including temperature, pressures, and flows, and in packaging operations. Equipment such as human-machine interfacing (HMI) computers and System Control and Data Acquisition (SCADA) devices used by Operations personnel to monitor and control the process through the ICS system (shown in Figure 5 below) and located in Network #1 and #2 are often in a second separate network layer of a segmented ICS structure. Data collected by these devices are fed to batch management and data historian equipment which reside in yet a higher segment or the DMZ zone of the segmentation architecture. Finally, the highest segmented layer is the Enterprise Business Network (Langill, 2014).

The purpose of segmentation is to provide networked ICS communication flow limitation capabilities for the purpose of information and process security. For instance, if the communication within the lowest layer consists only IP/Ethernet/IP protocol packets, devices can be installed between that layer and the next to limit communication accordingly. A similar premise can be used between each of the segments to control the communication flowing into and out of the areas. Another example of communication limiting would be allowing only read access from remote access (VPN) equipment to the lower layer devices. HTTP communication can be similarly restricted (Langill, 2014).

© 2016 The SANS Institute Author retains full rights.

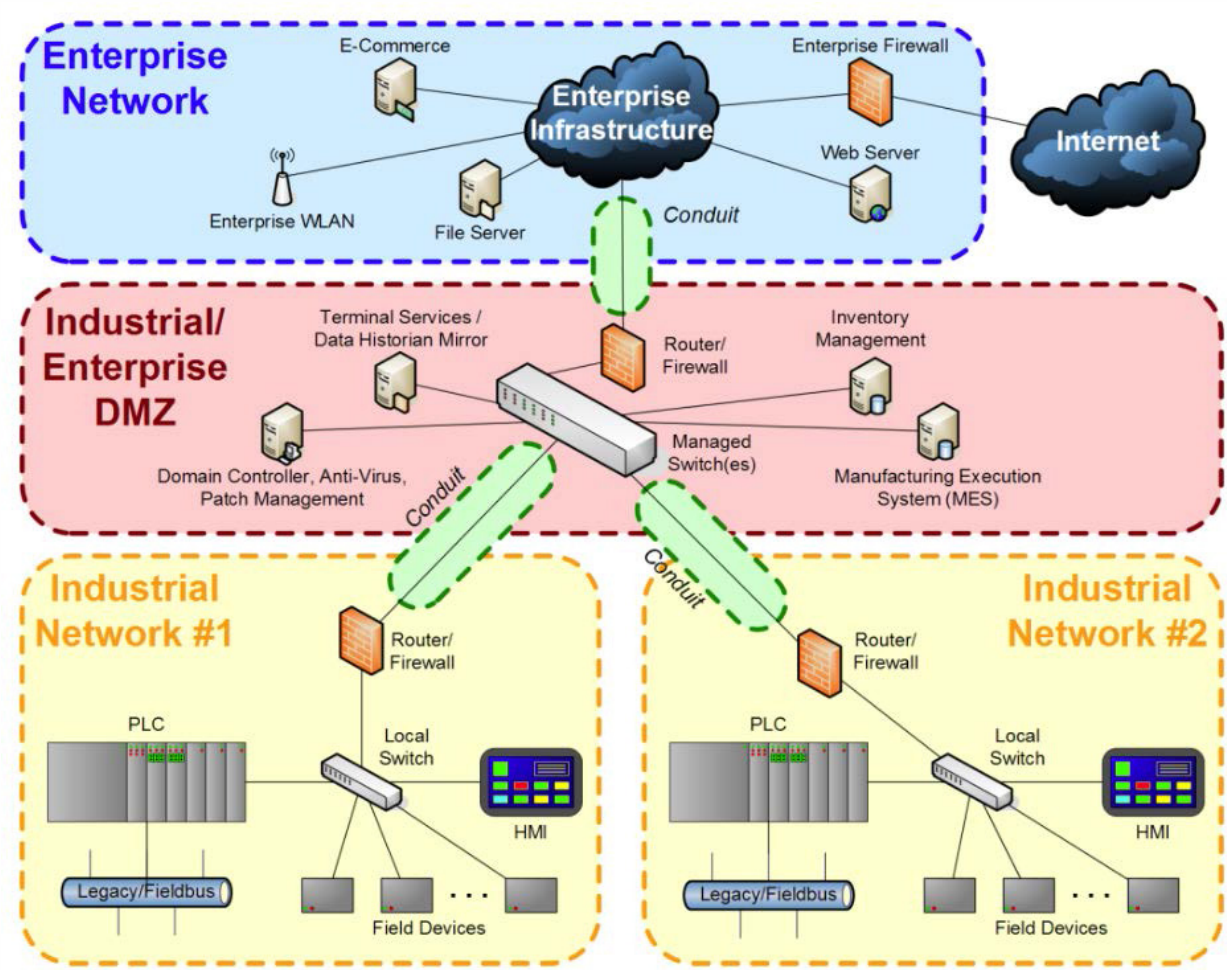

Figure 5: ICS Reference Architecture – Zones and Conduits (source: isa.org) (Langill 2014).

5.4 Cyber Security Standards and Information Sources

Standards for industrial control system security is a concern of the International Society of Automation. ISA has been developing standards for representing the security value of ICS devices. Two certifications from ISA, listed below, may be applied to indicate a device meets certain security requirements.

"• The Security Development Lifecycle Assurance (SDLA) is a certification program that assesses a supplier's product development lifecycle processes for ICS.

© 2016 The SANS Institute Author retains full rights.

• The Embedded Device Security Assurance (EDSA) certification focuses on the security of embedded devices, and addresses device characteristics and supplier development practices for those devices" (Langill, 2014).

Instruction to aid in the understanding of the security provided during procurement of components of control systems can be found in a document from ICSCERT called, "Cyber Security Procurement Language for Control System." The information will aid the reader in understanding, during the procurement process, the functionality provided by a device and associated security concerns. An example given by Mr. Langill (2014) is the discussion in the document regarding "semi-trusted demilitarized zones for VPN landing, and how vital information (such as passwords) should be protected in storage and in transit." Definitely a topic of concern to those trying to avoid a Havex-like attack (Langill, 2014).

6. Conclusion

The first section of this document provided an overview of ICS and cyber-espionage, along with an introduction to the Dragonfly attack. By showing in subsequent sections the manner in which the Dragonfly group infiltrated manufacturing and utility networks and stole vital information, an understanding can be gained of the great need for risk management in designing and maintaining networked control systems. Implementation of ICS network firewalls and virus scanning software alone are not enough to thwart cyber-espionage perpetrators. In order to secure industrial processes which may be critical to the world, or at the least, imperative to ensure the continued manufacturing capabilities of a company methods of defense such as network segmentation and defense in depth must be integrated into the design of ICS systems.

© 2016 The SANS Institute Author retains full rights.

The Dragonfly campaign provided the collection of ICS network and access information to a well-organized and funded group foreign to the countries from which the data was collected. The example of Stuxnet has taught us that penetrated systems can provide data to cyber-espionage perpetrators for years without detection and result in nefarious and damaging activities to processes controlled using automated equipment. Administrators and owners of industrial control systems used in manufacturing and utilities are well advised to take action now to demand securely made products from vendors of automation components and to update industrial processes to reduce their risk of becoming a cyber-espionage victim (Mackenzie, 2014).

©2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.

References

Burger, Andrew (2014, July 4). Dragonfly Malware Highlights Vulnerability of Energy Infrastructure. Retrieved from http://www.triplepundit.com/2014/07/dragonfly-malware-highlights-vulnerability-energy-infrastructure/#

Constantin, Lucian (2014, June 24). New Havex malware variants target industrial control system and SCADA users. Retrieved from http://www.pcworld.com/article/2367240/new-havex-malware-variants-target-industrial-control-system-and-scada-users.html

Dragonfly malware targeting pharmaceutical companies (2014, Sept. 15). Retrieved from http://net-security.org/malware_news.php?id=2865

Goodin, Dan (2014, June 30). Active malware operation let attackers sabotage US energy industry. Retrieved from http://arstechnica.com/security/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/

Havex Hunts For ICS/SCADA Systems (2014, June 23). Retrieved from https://www.f-secure.com/weblog/archives/00002718.html

Hayden, Assante, & Conway (2014, August). SANS-Cybersecurity An Abbreviated History of Automation & Industrial Controls Systems and Controls Systems and Cybersecurity. Retrieved from https://www.sans.org/reading-room/whitepapers/physical/abbreviated-history-automation-industrial-controls-system-cybersecurity-35697

Hernández, J. M., Ferber, A., Prowell, S., & Hively, L. (2015, April). Phase-Space Detection of Cyber Events. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference* (p. 13). ACM. Retrieved from

© 2016 The SANS Institute Author retains full rights.

https://www.researchgate.net/profile/Jarilyn_Hernandez_Jimenez/publication/278025286_Phase-Space_Detection_of_Cyber_Events/links/55798fa508ae752158717277.pdf

Industrial Control Vendors Identified In Dragonfly Attack (2014 July 4). Retrieved by https://securityledger.com/2014/07/industrial-control-vendors-identified-in-dragonfly-attack/

Langill, Joel T. (2014, Dec. 10). Defending Against the Dragonfly Cyber Security Attacks v3. Retrieved from http://www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf

Mackenzie, Heather (2014, August 8). Dragonfly Malware Targets ICS Systems. Retrieved from https://www.tofinosecurity.com/blog/dragonfly-malware-targets-ics-systems

Rockwell Automation (2009, May). Securing Manufacturing Computing and Controller Assets. Retrieved from http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp005_-en-e.pdf

Symantec Security Response (2014), Dragonfly: Western Energy Companies Under Sabotage Threat http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

Soifer, D., & Gouré, D. (2014, July). Keeping the Lights On. Retrieved from http://lexingtoninstitute.org/wp-content/uploads/2014/07/Keeping-The-Lights-On.pdf

Virgillito, Dan (2014 Sep 16). Dragonfly Malware Targets Pharmaceutical Sector. Retrieved from https://vpncreative.net/2014/09/16/dragonfly-malware-targets-pharmaceutical/

Wangen, Gaute (2015, April 9). The Role of Malware in Reported Cyber-espionage: A Review of the Impact and Mechanism. Norwegian Information Security Laboratory, Center for

© 2016 The SANS Institute Author retains full rights.

Cyber and Information Security, Gjøvik University College, Teknologivn. 22, 2815 Gjøvik, Norway. Retrieved from http://www.mdpi.com/2078-2489/6/2/183/pdf

©2016 SANS Institute, Author retains full rights.

© 2016 The SANS Institute Author retains full rights.