Global Information Assurance Certification Paper

The Spy with a License to Kill

GIAC (GSEC) Gold Certification

Author: Matthew Hosburgh, matt.hosburgh@gmail.com
Advisor: Rob VandenBrink
Accepted: *TBD*

Abstract

Industrial espionage, malware, and targeted attacks bring about a certain stigma. These terms have been around for decades and in many cases become cliché. Yet, they bring a new meaning when dealing with Industrial Control Systems (ICS). ICS systems provide a myriad of functions such as pipeline control, monitoring of the fermentation process in a brewery, and traffic light control. These systems are no longer contained. They are connected, exposed, and vulnerable. Successful exploitation and malicious manipulation of these systems can cause loss of life, physical damage, and lost revenue for many organizations. Havex is a recently discovered piece of malware that targets ICS systems exclusively. Traditional defenses have a difficult time detecting and mitigating this type of targeted threat. This paper will examine this attack and will discuss two of the SANS 20 Critical Security Controls that will help to mitigate this threat.

1. Introduction

> A plane does a fly-by over a dam as a security gate slides open. A man in combat black runs across the top of the tall dam. He clips a rope to his ankle and the railing...and jumps off the side. As he sails down, he pulls out a gun-type thing and shoots it. A wire follows attaching in concrete and pulling the man down to.... "Archangel Chemical Weapons Facility, USSR" (Em, 2004).

The opening scene of *GoldenEye* underscores the skills and precision of James Bond, 007. Years of experience and training make impossible missions look routine. These skills alone would not allow 007 to succeed; rather, a calculated plan that targeted the vulnerabilities in the Archangel Chemical Weapons Facility coupled with 007's skills provided for a successful mission.

ICS represents a series of desired targets, providing a means to control, monitor and maintain some of our most critical infrastructure. A few examples of the types of systems that utilize ICS are pipelines, electrical plants, water treatment facilities, and breweries. Successful exploitation of these types of systems can cause loss of life and extreme physical damage such as a pipeline explosion. Some of these systems can be manipulated to produce financial gain or loss, depending on the motive of the attacker. If the amount of gas flowing through a pipeline is being misreported higher, a company could be charged more. A blended attack could be conducted where an attacker could cause an ICS system to fail, exploding a pipeline at a strategic location and follow that up with a physical attack due to a weakened infrastructure. Havex has a new implication for ICS malware. It specifically targets the systems that either communicate or monitor sensitive ICS systems. But what is the motivation to attack these systems? By examining why and by what means Havex targets ICS, two of the SANS Critical Security Controls can be selected to help mitigate the threat that this targeted malware poses.

2. The Mission

The mission of the Havex malware is to target and exploit an ICS for remote access. At its core, the malware is a Remote Access Tool (RAT) that will exfiltrate data from an ICS (Langill, Zambon, & Trivellato, 2014). The target of the malware is primarily the energy sector and more specifically, Open Platform Communications (OPC) systems. OPC was originally named Object Linking and Embedding (OLE) for Process Control but spans more than just process control, which is why the name change to Open Platform Communications occurred

(OPC Training Institute, 2014). "OPC is a standard for industrial communications that enables universal connectivity and interoperability. OPC technology is based on Client/Server architecture…" (OPC Training Institute, 2014). Put another way, "Originally OPC was Distributed Component Object Model (DCOM) based, and many OPC systems in use today use DCOM, although OPC has more recently been updated to use an object-oriented protocol called OPC-Unified Architecture (OPC-UA)" (Knapp, 2011). Why would an attacker want to target OPC systems? Because it is scalable, and it can be used for a myriad of functions. These functions can be seen in Figure 1 and provide connections into control, archiving, Enterprise Resource Planning (ERP), Distributed Control Systems (DCS), Remote Terminal Units (RTU), and Programmable Logic Controllers (PLC) to name a few (Murphy, 2006).

Figure 1. Common uses of OPC (Murphy, 2006)

"OPC eliminates the need for custom drivers between each new application and Data Source" (Kominek, 2009). In essence, OPC consolidates all the various data sources into one easy-to-interact-with interface. By attacking an OPC server, the attacker can gain most, or in some cases, all the data in an ICS process. According to David Lopert, an Operations System Analyst for a mid-stream natural gas company, the impact can mean financial loss. "Our metering uses OPC (so say we really flowed 10,000 gallons of liquid, but the malware made it say we only flowed 1,000 gallons, our financials would underreport compared to what actually happened)"

(Lopert, 2014). If this OPC data can be extracted, it can be very useful for mounting a more destructive, targeted attack. In simple attacks, the data could be modified to affect the financials of a company. According to Symantec, the operators behind Havex, dubbed Dragonfly, have been conducting operations for over a year starting in January 2013 through August 2014 making this operation very calculated (Symantec Security Response, 2014). Understanding how Havex targets ICS is key to a mitigation strategy.

3. Infiltration

Understanding the means by which Havex spreads will help in the development of a mitigation strategy. Havex was typically spread via three main avenues. The first approach was a spear phishing campaign. This targeted campaign attempted to trick executive users into opening a malicious PDF document (Symantec Security Response, 2014). The key difference from a generic phishing campaign is that the recipients were specifically and intentionally attacked. The individual or group behind the campaign knew exactly who they were after.

The second approach is a watering hole attack (Symantec Security Response, 2014). "In a watering hole attack, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection" (Abendan ll, 2011). The carefully selected website is chosen after the attacker collects intelligence on the target. The user visits the site and is then infected. The malware is then free to carry out its mission. Further showing the group's sophistication, this method for delivery was not kept trivial. "The fact that the attackers compromised multiple legitimate websites for each stage of the operation is further evidence that the group has strong technical capabilities" (Symantec Security Response, 2014). This evidence further highlights how the attack was successful and how the group targeted the energy sector.

Finally, the last method was the most complex of all: trojanized software. The attackers managed to insert this malicious code into the download page of three legitimate ICS vendors (Symantec Security Response, 2014). These three methods are not new, but they are tried and true methods of infiltrating an organization. An interesting note from David Lopert regarding malware and OPC systems is that he never observed an OPC system infected with malware (Lopert, 2014). This does not mean the systems are immune, but it underscores how Havex is an extremely calculated and targeted threat in an environment where security monitoring and

alerting is lacking. Looking at the most recent avenue of attack, the motivation of Havex's authors can be better understood.

3.1. Targeting the Source

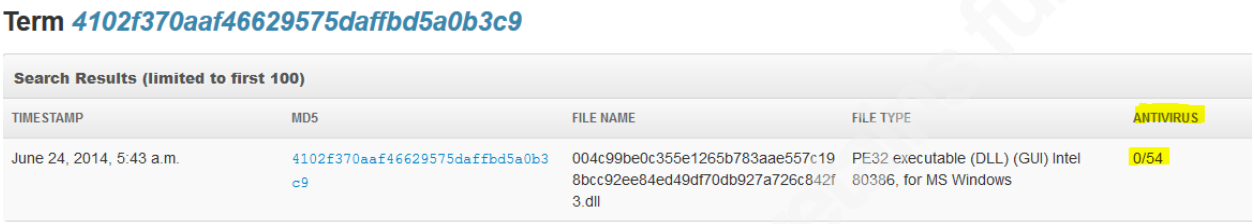
By attacking legitimate vendor download files, the motivation of the Havex authors can be realized. There were three vendors that were attacked: MB Connect Line, eWon and an un-named Swiss Company. MB Connect is a small company, operating out of Germany. According to DigitalBond, they focus on "wind turbines and biogas plants, along with other energy infrastructure systems are the applications for their products. Ironically they also highlight their mbEagle product, secure detection of Stuxnet and other manipulations, and mbSECBOX, security for S7 PLCs" (Peterson, 2014). The next company, eWon, is a top producer of Virtual Private Networks (VPN) for Programmable Logic Controllers (PLCs) in Belgium (Peterson, 2014). Finally, the third company (name has not been disclosed) is a noted to be from Switzerland (Peterson, 2014). Both MB Connect and eWon have similar integration with various PLCs. From an OPC and data collection standpoint, a myriad of specific targets could be identified with these devices. At face value, it appears as if the targets would be from the European Union (EU). This may only be a means to an end – the target could be a partner or customer in which one, or all, three of these companies have access to. (Peterson, 2014) Based on the known evidence, the ultimate targets would be broad, wide-reaching and for the purposes of gaining further information. This information could then be used to launch an even more tailored targeted attack, making detection very difficult. This type of attack can be detected and mitigated if the right controls are in place.

4. Malware Defenses

The first SANS Critical Security Control that can be used to mitigate this attack is #5: Malware Defenses. Malware detection and response is critical for preventing (at most) and detecting (at least) not only known malware, but unknown malware. In the case of Havex, a signature based anti-virus provider may not have been able to detect this threat early on. This was mainly due to the fact that the malware was not widely known and that it was utilizing unknown or zero day exploits. Wilhoit (2014) of FireEye noted the known file hashes from this campaign are:

- 6bfc42f7cb1364ef0bfd749776ac6d38
- ba8da708b8784afd36c44bb5f1f436bc
- 4102f370aaf46629575daffbd5a0b3c9

As of August 3, 2014, these hashes were detected by 44 of 54 anti-virus vendors, according to VirusTotal. But on June 24, 2014 per malwr.com, no Anti-virus vendor had detected this, as shown in Figure 2.



Term *4102f370aaf46629575daffbd5a0b3c9*

Search Results (limited to first 100)

TIMESTAMP	MD5	FILE NAME	FILE TYPE	ANTIVIRUS
June 24, 2014, 5:43 a.m.	4102f370aaf46629575daffbd5a0b3c9	004c99be0c355e1265b783aae557c198bcc92ee84ed49df70db927a726c842f3.dll	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	0/54

Figure 2. Malwr.com detection rates of early Havex malware.

This means that in the early stages of the attack, anti-virus coverage was non-existent or limited. Malware defenses must go beyond just signature-based detection. A form of sandboxing and outbound traffic analysis is also a useful supplement. One example is the Cuckoo Sandbox, which looks beyond just a file hash. Instead, it analyzes the network behavior, registry modifications, file behavior and the memory of the analyzed machine. (Cuckoo Sandbox, 2014)

Havex used three vectors of infection: spear phishing, watering hole, and malicious code inserted into legitimate ICS software. SANS Critical Security Control #5 looks at the whole picture, when dealing with malware defense. Anti-virus and other methods such as the Enhanced Mitigation Experience Toolkit (EMET), email attachment scanning, disabling auto-run, leveraging the cloud for threat intelligence, incident response and Domain Name Service (DNS) query logging are all necessary components to successfully mitigate malware. (SANS, 2014) In an interview with Rock Lambros, a former Security Engineer for eBay, Rock noted that a risk based model coupled with several technical countermeasures was an effective approach. (Lambros, 2014) Leveraging one defense and not the other would allow for Havex to slip through the cracks, which is why a layered approach is necessary.

4.1. Layered Malware Defenses

To enable effective malware defenses, a layered approach is necessary. In the case of Havex, there was not one method of infection, but three. As time goes on, there could be several

others, which is why having a layered approach to malware defenses can help to add coverage to the environment. Further, anti-virus is not a silver bullet and can be evaded. One tool that can be used is Veil-Evasion. "Veil-Evasion is a Python framework that automates creating antivirus-evading payloads, giving users the choice of multiple techniques" (Weidman, 2014). This framework can make it easy for an attacker to change the payload, resulting in a new hash, which further complicates signature detection. Many of today's users have multiple devices, such as a laptop, mobile smart phone, and occasionally a desktop. In addition to that, many organizations have enabled their users to work from home or while traveling. This diverse landscape makes malware detection exponentially more challenging, but not impossible. When Havex was initially released, it was not detected by traditional signature based anti-virus. A holistic approach would include an anti-virus (AV) capability on all devices that are part of the network of value. This may not have detected the initial infection, but would have alerted and sped up the eradication of Havex from the infected network. For the sake of simplicity, the network in this example will represent a corporate type network hosting many typical systems (wireless, wired, email, and AV) and some atypical (OPC, IPS and IDS). At the user level, all systems must have an AV solution installed. This would include AV for laptops, mobile devices and desktop users. Ideally, this software would be distributed via a packaged deployment or be included in the core system image. At the server level, all servers would need the same AV client. If at all possible, the security tools (appliance and) can run AV, they should do so with the latest signatures. In the best case, the network firewall should also have an AV component and URL filtering. This will allow for known (and in some cases) unknown malware to be stopped before it can even enter the environment. As an additional line of defense, downloaded files and URLs can be submitted, on the fly, from an IDS to a malware sandbox for review. In this case, open-source solutions are the tools of choice. For instance, once the traffic leaves the firewall, it is reviewed by the IDS, Security Onion (SO). Within this distribution, which is maintained by Doug Burks and supported by the larger security community, there are many useful tools. One of these tools is Bro. By default, "Bro with SO logs MD5 hashes of binaries downloaded over HTTP" (Bejtlich, 2013). This capability can further be extended to actually extract the binary and not just calculate the hash. (Bejtlich, 2013) Once extracted, and with some simple Python scripting, the binaries can be transferred on the fly to the Cuckoo sandbox. Within Cuckoo, a script can be ran

that will automatically process (analyze) and run the binaries in a safe area, shown in Figure 3 and 4.

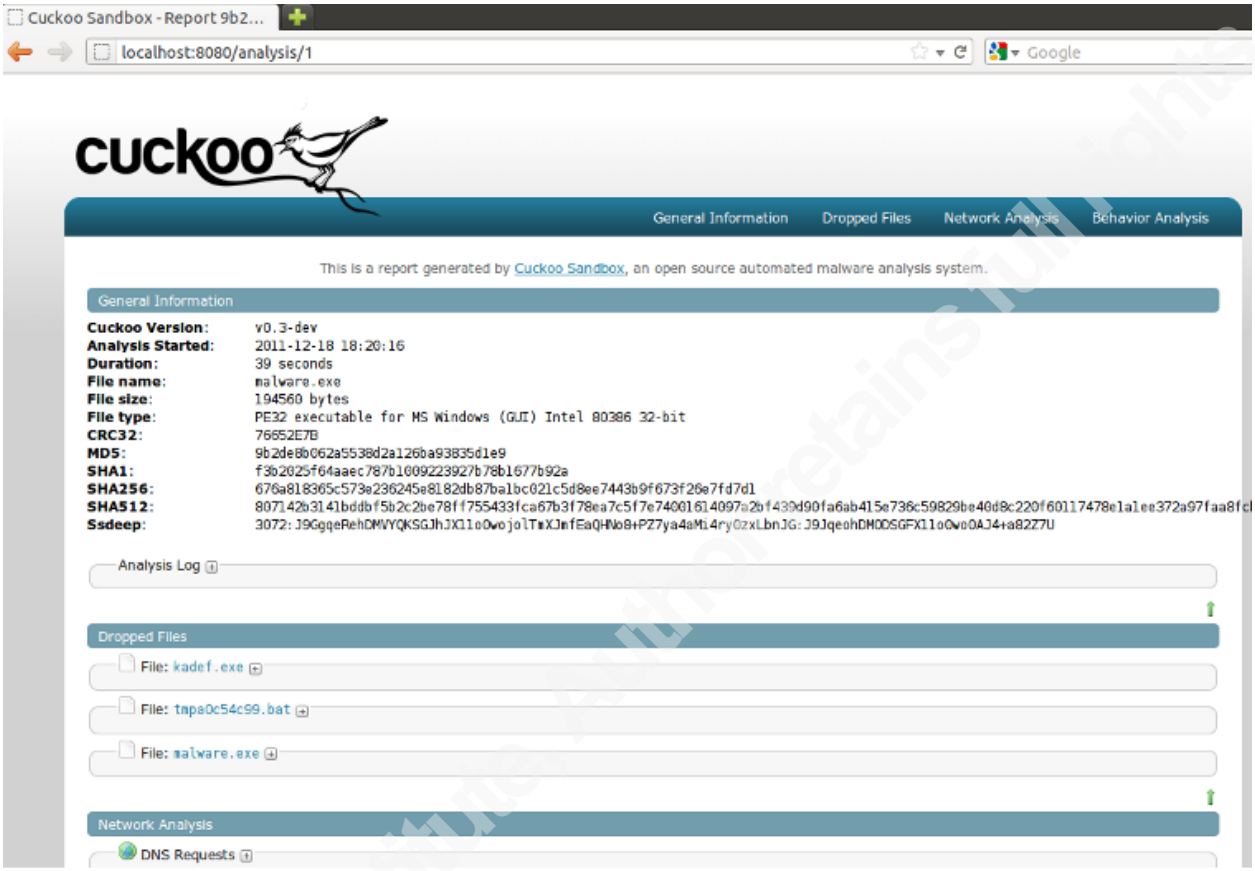


Figure 3. Cuckoo web interface. (Cuckoo Sandbox, 2014)

Example: submit a local binary:

```
$ ./utils/submit.py /path/to/binary
```

*Figure 4. S*ubmitting a binary for analysis via a Python script. (Cuckoo Sandbox, 2014)

Taking it a step further, URLs can also be extracted by Bro and sent to Cuckoo for analysis. The analysis logs can be sent to a Security Information and Event Management (SIEM) system and the appropriate alerting can be generated. "SIEM platforms are often used in Security Operations Centers (SOCs), providing intelligence to security operators that can be used to detect and respond to security concerns" (Knapp, 2011). Detection without response is like ignoring your engine light. Response to the security alerts produced from the SIEM can lead to swift and

effective defense. This layered infrastructure can be seen in Figure 5 and is crucial in detecting and defending against more skilled and advanced attackers. Another scenario for this type of architecture can be found in *The Security Onion Cloud Client Network Security Monitoring for the Cloud,* by Joshua Brower. (Brower, 2014)

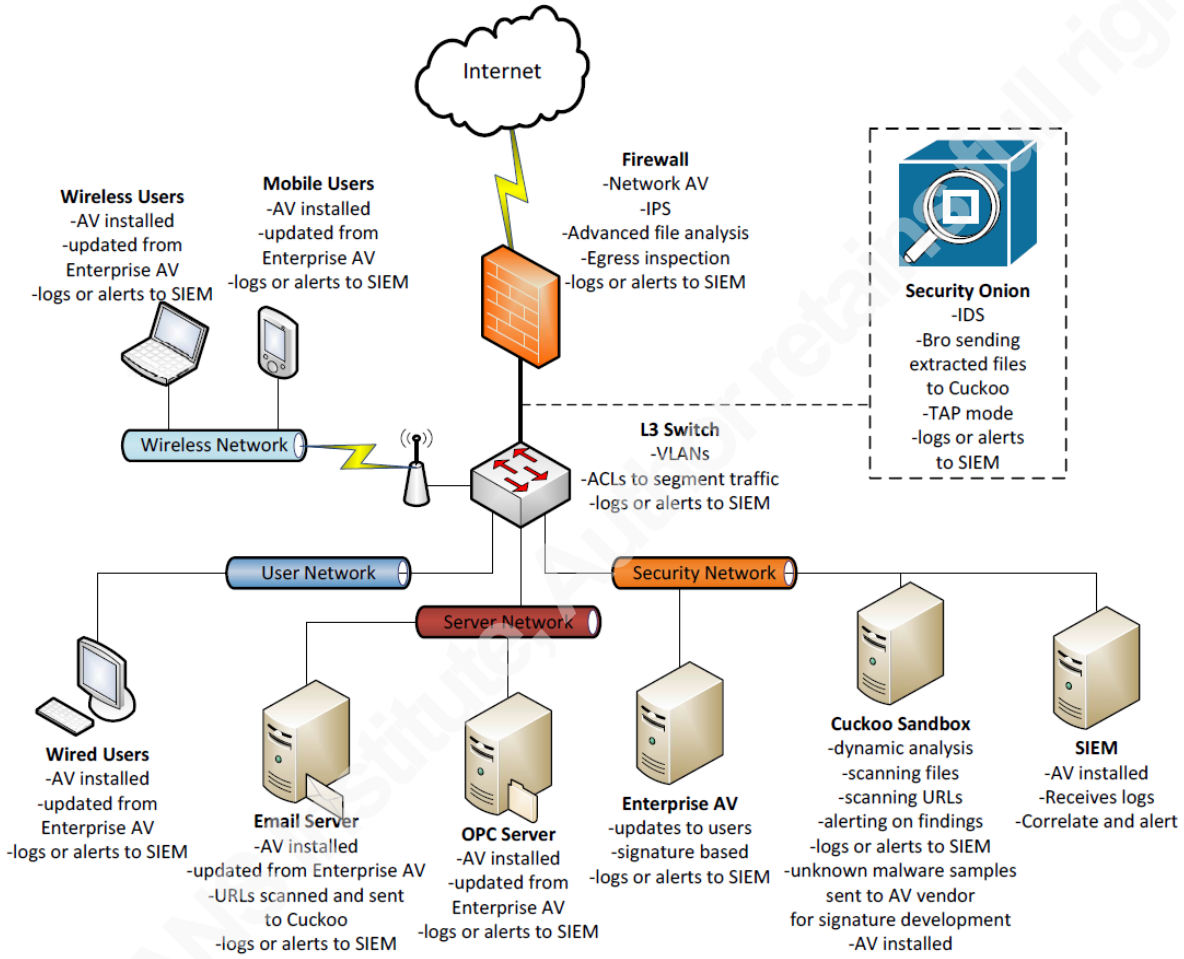


Figure 5. Basic infrastructure leveraging layered malware defenses.

What if these layers fail? What would the next level of detection look like? In the case of targeted attacks: the human sensor.

5. Security Skills Assessment

The second SANS Critical Security Control that can be used to mitigate an advanced, targeted attack is #9: Security Skills Assessment and Appropriate Training to Fill Gaps. This control addresses the ever-changing element of security: people. People can get complacent, can be naïve, trusting and overzealous. These qualities are exactly what the Havex author is

counting on. Without the human interaction, the efficacy of Havex to infect its target is reduced greatly. Understanding where the average user is in regards to security awareness will help shape the education plan for all required parties. Providing the traditional security awareness training is a must, but because not everyone learns the same way, active scenario testing is a viable and lasting way to get the security message across. "Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise" (SANS, 2014). Educating the user can go a long way. In the case of ICS, the operator of that system will know when something is awry. If they notice that anomaly and report it in a timely manner, the damage from a targeted attack can potentially be reduced. Network segmentation can help when the human sensor fails to detect or block an attack. In other words, requiring a need-to-know will help to limit the attack surface. For example, an accountant should not have access to the engineering server if they do not have a valid need-to-know. This principle helps to fortify and increase the detection and prevention ability. Keeping up with emerging threats and keeping technical skills sharp, the Security Team will be equipped to notice the signs and early warnings of a targeted attack, such as Havex. Operational Technology (OT) and traditional Information Technology (IT) must work together for detection to be effective. Often the IT Security Team does not have the experience or training on the ICS devices. For these sensors to be effective, they will be required to be maintained and updated.

5.1. Updates for the Human Sensor

An effective "human sensor" that is properly maintained can be invaluable in mitigating an advanced and targeted threat. Havex relies heavily on user interaction to be successful. Without a user, Havex would have to seek alternative means to infect its targets. Because the user was the target, the user can also be an effective sensor to assist with detection and often, prevention. In many penetration tests (pentests), the tester exploits the basic trust of the user to gain a foothold. Post exploitation, the tester will often pivot to other systems for further exploitation. In some cases, the tester may only need to exploit the user to retrieve the targeted information. "It is a common saying in information security that users are the vulnerability that can never be patched. Put all the security controls in place that you want, but if an employee can be convinced to give up sensitive company information, it is all for naught. In fact, many of the

most famous hacks include no system exploitation at all" (Weidman, 2014). What if the user was not considered a vulnerability, but a tuned Intrusion Prevention or Detection System? That could mean the difference between a successful attack and not, clicking on a link or not. Figure 6 illustrates a human sensor architecture.

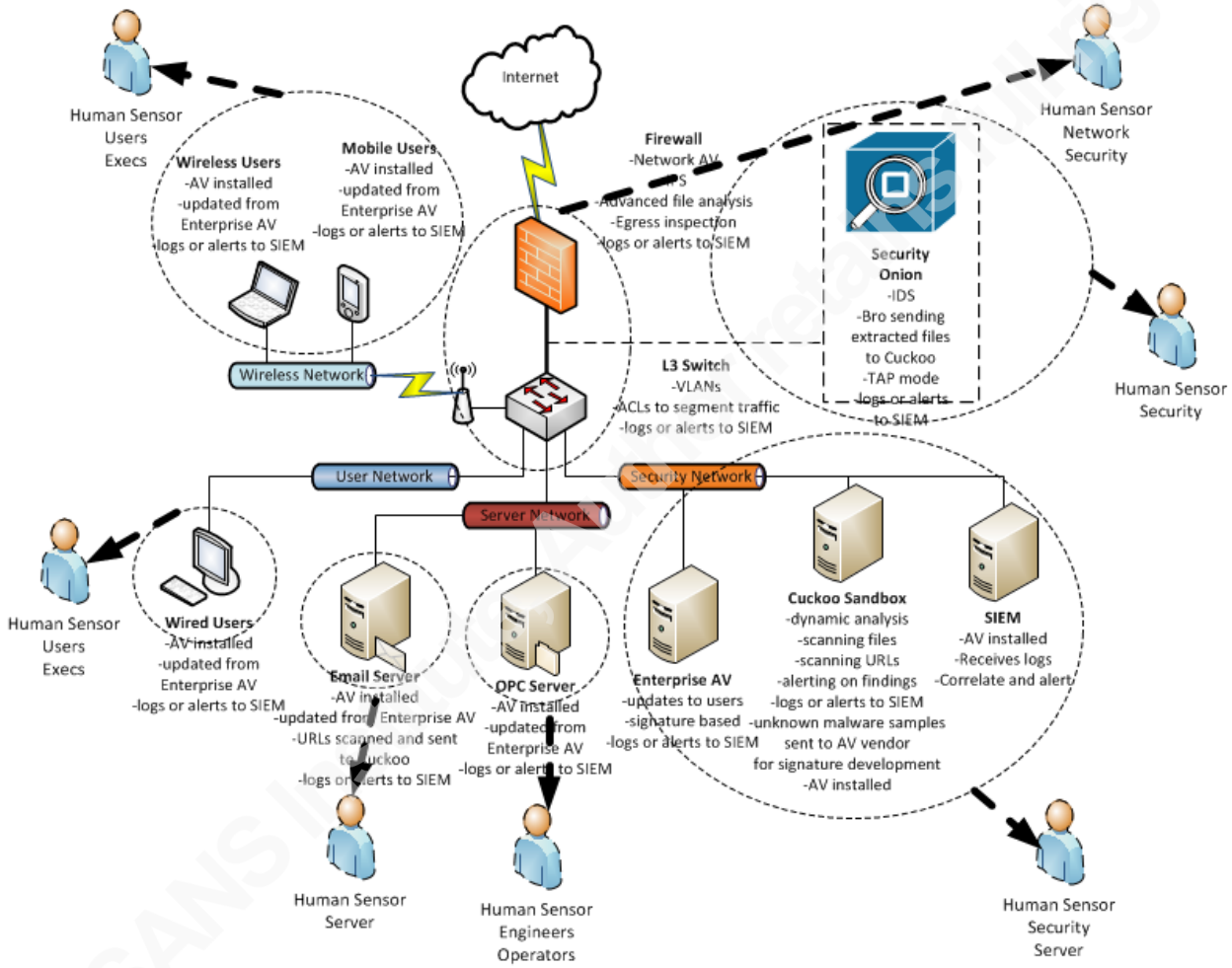


Figure 6. A simple human sensor architecture.

A sensor requires updates for it to effectively detect and threats. The human sensor can be updated and effective if two conditions are met. The first is that the user be aware that their actions can pose a risk to the organization. This can be accomplished in the form of traditional security awareness, such as videos, training sessions or security newsletters. The second condition is that a user must be tested and provided with feedback. This testing should be realistic, which increases the odds of actual real-world detection. Setting up phishing tests would be a way to effectively address an advanced threat. During the test, if a user clicks on a

"malicious" link, they should be immediately provided on the spot training. (PhishMe, 2014) This will ensure that the concepts presented in the more traditional training are solidified. Lastly, the SANS ICS 410: ICS/SCADA Security Essentials course is a way for both OT and IT Security Teams to establish a common baseline for terminology when discussing the security issues in ICS, which can help to develop a true security plan for ICS. There is no silver bullet for detection, but combining user education with technical controls will go a long way.

6. Conclusion

In summary, Havex is a newly discovered RAT with a mission to steal data. The data is collected from OPC systems and transmitted back to a central location. The targets of this malware are alarming because OPC systems are the central hub of data collection for ICS and many other systems in an organization, making it a highly desired target. Although Havex does not have any destructive characteristics, it appears that this malware is being used to collect data that can be used for future attacks. This malware is highly targeted and skilled. Much like a secret agent, Havex is used to infiltrate the most critical and secure environments. This is achieved through spear phishing, watering hole and legitimate ICS downloads injected with malware. By combining SANS Critical Security Controls #5 (Malware Defenses) and #9 (Security Skills Assessment and Appropriate Training to Fill Gaps), the effects of Havex can be weakened. Malware defenses incorporate more than just anti-virus and can include sandboxes, monitoring system settings such as autorun, EMET and incident response. This layered approach will help to identify infections or suspicious behavior across multiple systems and platforms. Finally, SANS Critical Security Controls #9 is all about the human sensor. Education and knowing what anomalous behavior in a system looks like and then who needs be informed is an effective way of combating this type of threat. Just like a technical sensor, the human sensor must also be updated. The update, in the case of the human, is training. A blended training approach is the most effective. Combining traditional methods and more innovated education to users will help to tune the human sensor into an effective alerting system. There is no golden gun or silver bullet, but there are ways to reduce the efficacy of even the most skilled agents.

References

Abendan ll, O. (2011). *Watering Hole 101*. Retrieved from Trend Micro: http://about-threats.trendmicro.com/RelatedThreats.aspx?language=au&name=Watering+Hole+101

Bejtlich, R. (2013). The Practice of Network Security Monitoring. In *Understanding Incident Detection and Response.* San Francisco: No Startch Press, Inc.

Brower, J. (2014, July 30). *The Security Onion Cloud Client Network Security.* Retrieved from SANS Institute InfoSec Reading Room: http://www.sans.org/reading-room/whitepapers/scada/protect-critical-infrastructure-systems-whitelisting-35312

Cuckoo Sandbox. (2014). *Cuckoo Sandbox*. Retrieved from About: http://www.cuckoosandbox.org/about.html

Em. (2004, January 22). *GoldenEye Script.* Retrieved from Universal Exports: http://www.universalexports.net/scripts/goldeneye.shtml

Knapp, E. D. (2011). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.* Waltheim: Elsevier Inc.

Kominek, D. (2009). *Guide to OPC.* Retrieved from Automation: http://www.automation.com/pdf_articles/Guide_to_OPC.pdf

Lambros, R. (2014, September 4). RE: Interview Questions for Research ISE5100 - Rock. (M. Hosburgh, Interviewer)

Langill, J., Zambon, E., & Trivellato, D. (2014, July 8). *whitepaper havex US.* Retrieved from Security Matters: http://www.secmatters.com/sites/www.secmatters.com/files/documents/whitepaper_havex_US.pdf

Lopert, D. (2014, September 3). RE: Interview Questions for Research ISE5100 - Dave. (M. Hosburgh, Interviewer)

Murphy, E. (2006, June 27). *OPC DA Timestamps: Where do they come from?* Retrieved from OPC Exchange.

OPC Training Institute. (2014). *What is OPC.* Retrieved from OPC Training Institute.

Peterson, D. (2014, July 2). *Havex Hype & Unhelpful Mystery*. Retrieved from digital bond: http://www.digitalbond.com/blog/2014/07/02/havex-hype-unhelpful-mystery/

Matthew Hosburgh, matt.hosburgh@gmail.com

PhishMe. (2014). *PhishMe*. Retrieved from What is PhishMe?: http://phishme.com/product-services/what-is-phishme/

Sandbox, C. (2014). *Cuckoo Sandbox*. Retrieved from Submit an Analysis: http://docs.cuckoosandbox.org/en/latest/usage/submit/

SANS. (2014). *Critical Security Controls: 5*. Retrieved from SANS.org.

SANS. (2014). *Critical Security Controls: 9*. Retrieved from SANS.org http://www.sans.org/critical-security-controls/control/9

Symantec Security Response. (2014, June 30). *Symantec - Security Response - Dragonfly v1.0.* Retrieved from SCADAhacker: http://www.secmatters.com/sites/www.secmatters.com/files/documents/whitepaper_havex_US.pdf

Weidman, G. (2014). *Penetration testing A hands-on introduction to hacking.* San Francisco: No Starch Press, Inc.

Wilhoit , K. (2014, July 17). *FireEye Blog*. Retrieved from Havex, It's Down With OPC.

Matthew Hosburgh, matt.hosburgh@gmail.com