Preliminary STUXNET Report V1.0

DISCLAIMER

This document may contain proprietary and controlled unclassified information requiring protection from disclosure. Ensure proper safeguarding. The following notice may apply - "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE – PROPRIETARY – Any misuse or unauthorized disclosure can result in both civil and criminal penalties."

Our CSFI Project Team

A team of twenty-six Information Security professionals, Intelligence Analysts and Engineers collaborated in a private portal towards this deliverable. CSFI believes in collaboration and sharing of knowledge as a way to shine light on the darkness in the cyber domain. Our goal is to minimize speculation through research and logical thinking. This is a preliminary foundational report from a Cyber Warfare perspective. Some of our volunteers made the choice to serve in silence due to the sensitivity of their jobs. We thank them for their contribution and hard work.

Special thanks and credit to our CSFI volunteers:

Amr Ali, Malware Analyst, OSINT
EGYPT

Chris Blask, VP Marketing, AlienVault
USA

Joel Langill, TÜV FS-Eng ID 1772-09, CEH, CPT, CCNA
Control Systems Security Consultant
USA

Joseph Patrick Schorr, CEH, CISSP
Manager, Attack and Penetration Testing Practice
USA

Jim Mulholland
OSINT Fusion/Research/Analysis - Web/Social Media Intelligence - CT Researcher/Analyst
CANADA

Jesus Oquendo
C|EH, CHFI, SGFA, SGFE, CPT IACRB, OSCP
Chief Security Engineer
USA

Izar Tarandach
Principal Security Engineer
USA

David Simpson
Federal Cyber Security Subject Matter Expert
USA

Charles A. Penn, Jr.
Network Administrator and Systems Analyst
USA

Avv. Stefano Mele
ICT Law, Intelligence & Security
ITALY

Bill Varhol
IT Specialist, Department of Defense
USA

Ehab Fahmi
Information Security Consultant
EGYPT

Our Project Scope

1- Find the source code of the attack.

2- Reverse engineer the malware code in order to understand how it works and find signs of attribution, possibly linking the code to a nation-state actor (or actors).

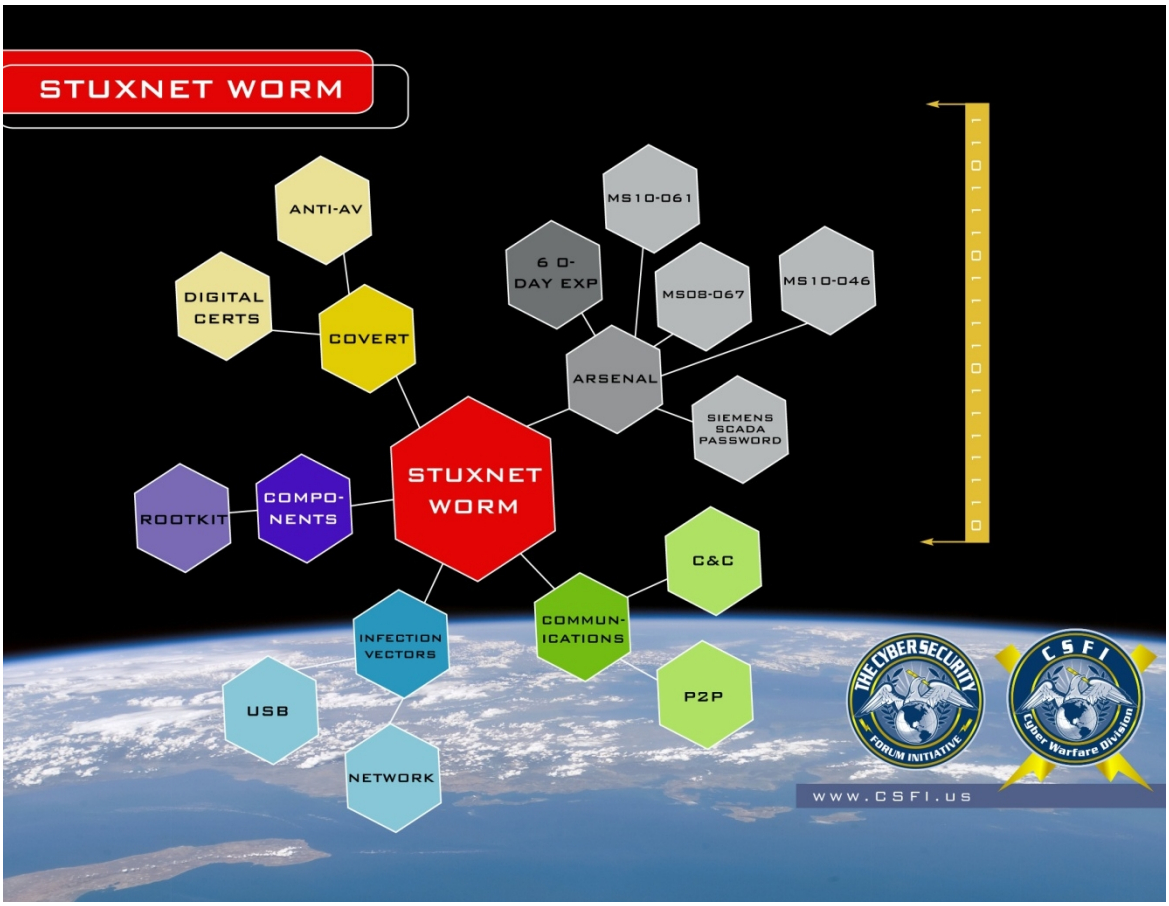
3- Create a solid countermeasure for this form of attack along with recommendations on how to secure systems against this form of attack.

4- Understand the political motivations behind this attack.

5- Explain how such a piece of malware could be used in a cyber warfare scenario.

6- Can Iran retaliate using the same form of cyber attack? What are the chances of such an attack from Iran taking place against the US and allies?

STUXNET in a Nutshell



"Stuxnet is arguably the first cyber attack specifically targeting ICS devices. It is actually an engineering attack against physical processes using IT as a vector into the controllers. It is a very sophisticated attack that gets around multiple security barriers and has defeated two-factor authentication by utilizing compromised digital keys and the default Siemens password which cannot be changed. Stuxnet has been in the wild since June 2009 and upgraded at least once in early 2010. It is not clear who developed Stuxnet, what Stuxnet is trying to accomplish, or when or how often the Stuxnet payload is to be activated. It is possible this approach could target other ICS vendors as other control system suppliers including Rockwell also utilize default passwords in some legacy systems that cannot be changed. The national security concerns are that this weaponized approach can be used against many infrastructures and many of these infrastructures use the same controllers."

Joe Weiss, CSFI member and CSFI STUXNET Project Contributor

Mr. Weiss provided expert testimony to the October 17, 2007 House Homeland Security Subcommittee and provided control system cyber security recommendations to the Obama Administration

Source Code

Our studies have concluded there are variations of the STUXNET code on the Internet, which creates confusion for readers when trying to understand the threat.

Our research concludes that there are 4 variants of STUXNET matching with Symatec's research.

v1: Installer component had a size of 513,536 bytes.
v2: An exact copy of v1 + 4KiB of junk data.
v3: An exact copy of v1 + 4KiB of junk data + 80KiB of nulls.
v4: Is significantly different from v1. As for C&C URLs, it has the original set and corresponding IPs

NOTE: V2-V3 is widely accepted as being the same with the only difference being the addition of junk and nulls to the files, which does not typically qualify them as a variable. V1 and V4 are in fact different with a file size difference of roughly 100kb in both the installer component and the payload DLL.

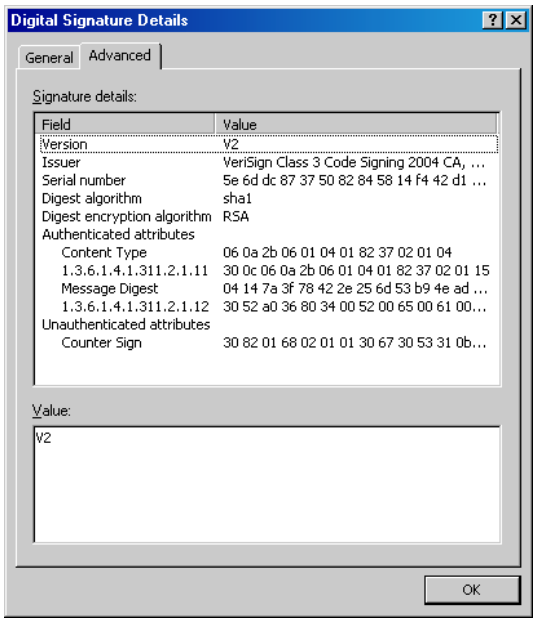
More detailed information on the variants from Symantec:
http://www.symantec.com/connect/blogs/w32stuxnet-variants

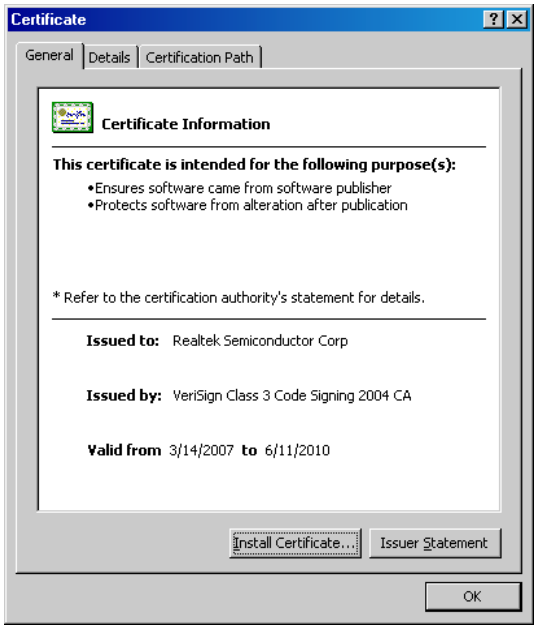
Stuxnet had 1 “known” variant; the original worm used the drivers signed by Realtek while the variant released within days of the first being discovered had the same drivers signed by JMicron. Verisign revoked the first certificate on July 16 and the variant was found on July 17.

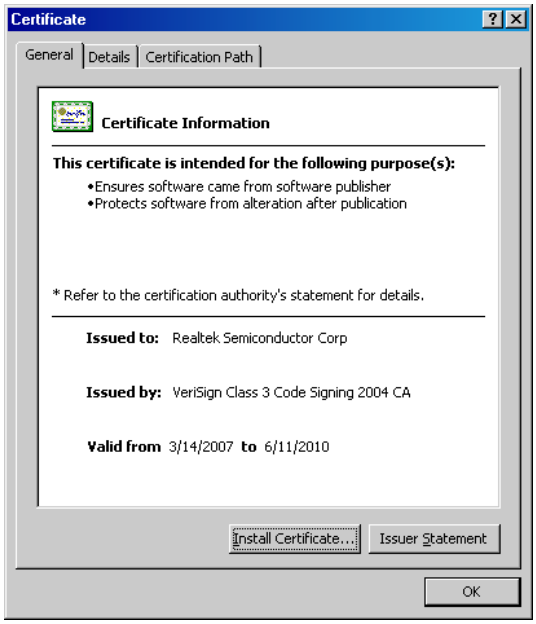
STUXNET is a complex attack code with a variety of files, including some files that are signed.

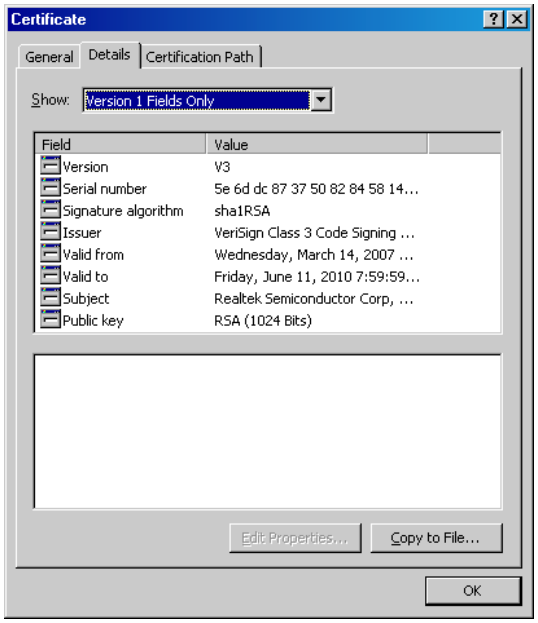
HERE ARE SOME IMAGES OF THE SIGNING AND VERSIONS:

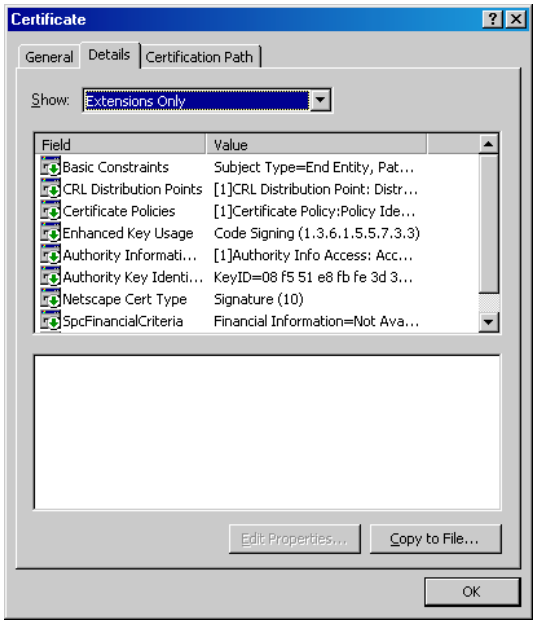
c:\windows\system32\drivers\MRXCLS.SYS

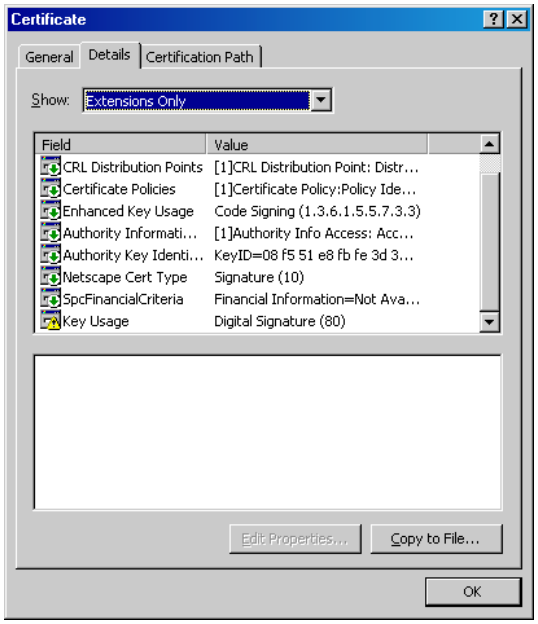


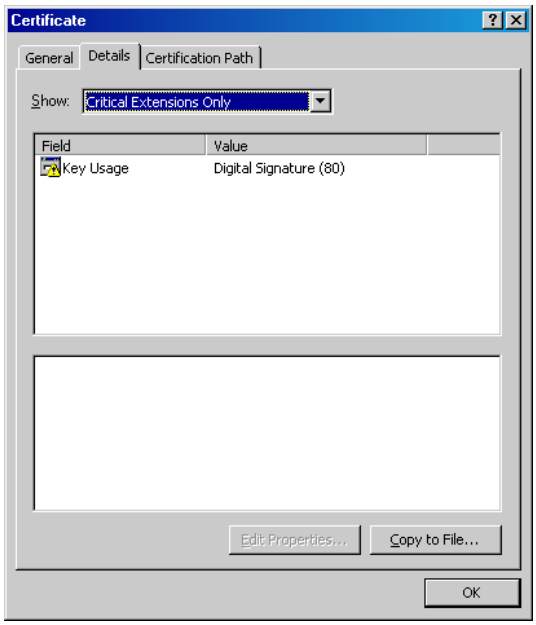


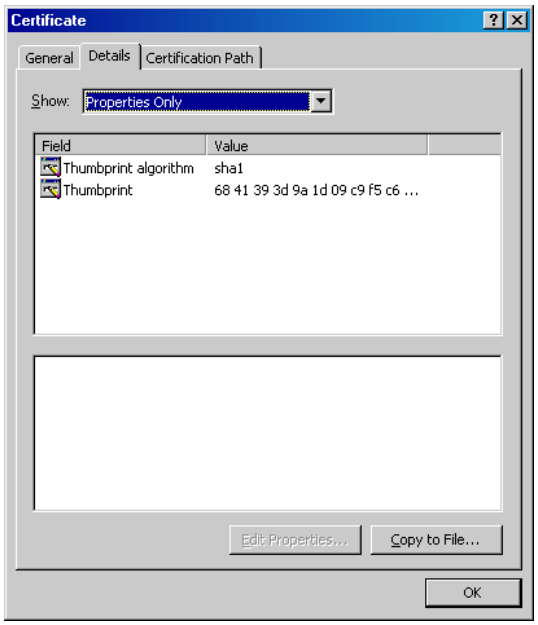


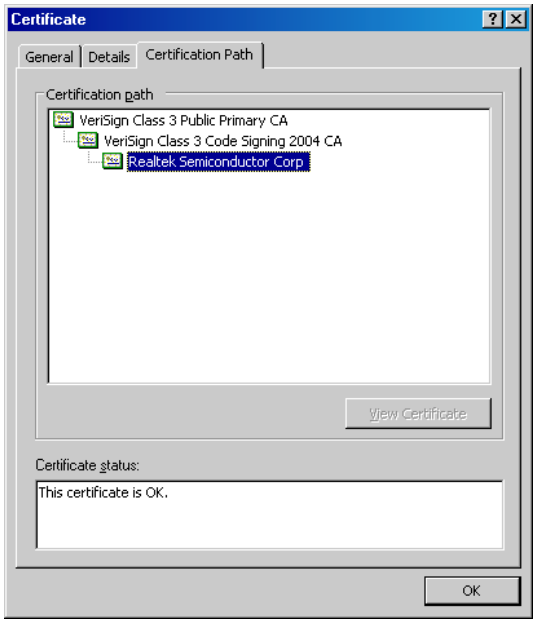


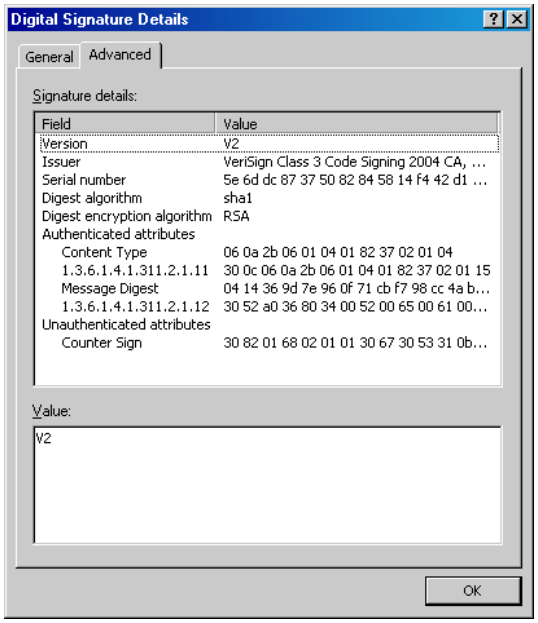




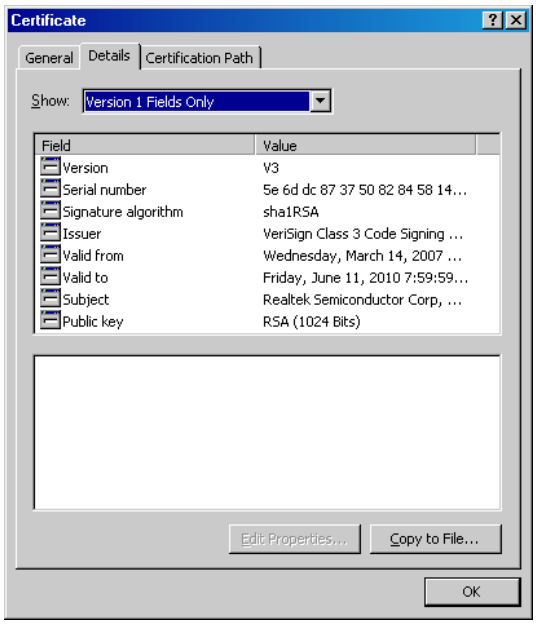


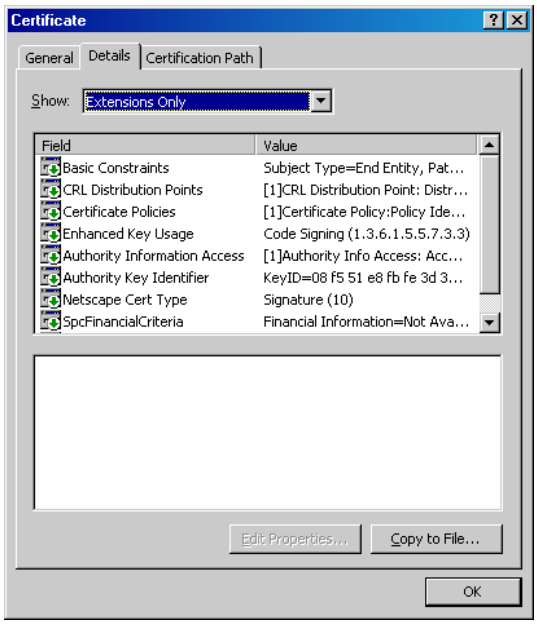


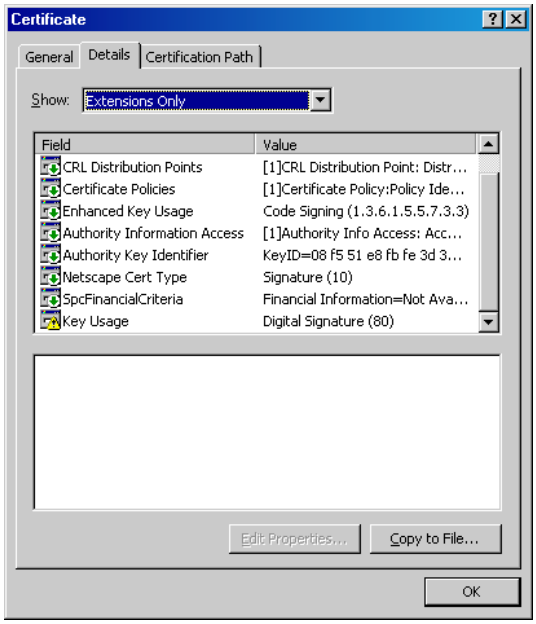


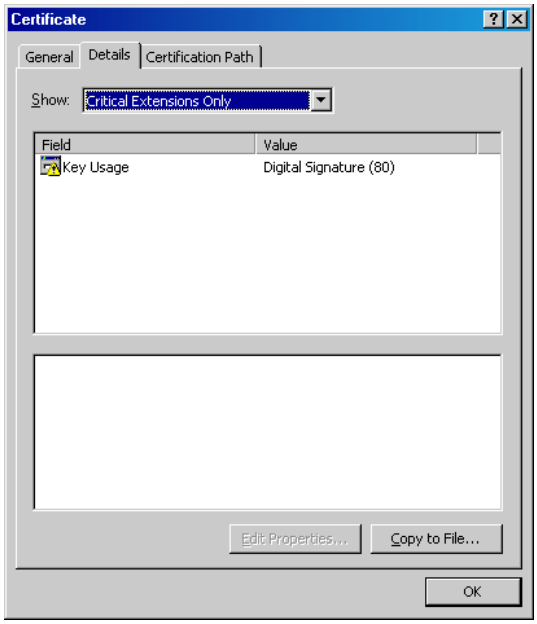


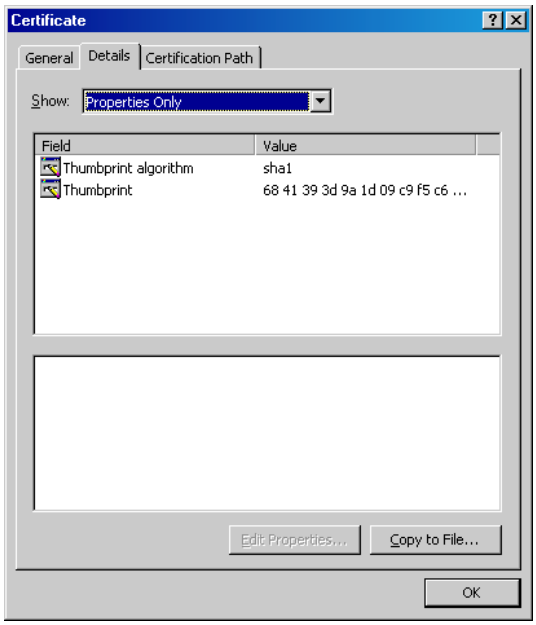
c:\windows\system32\drivers\MRXNET.sys

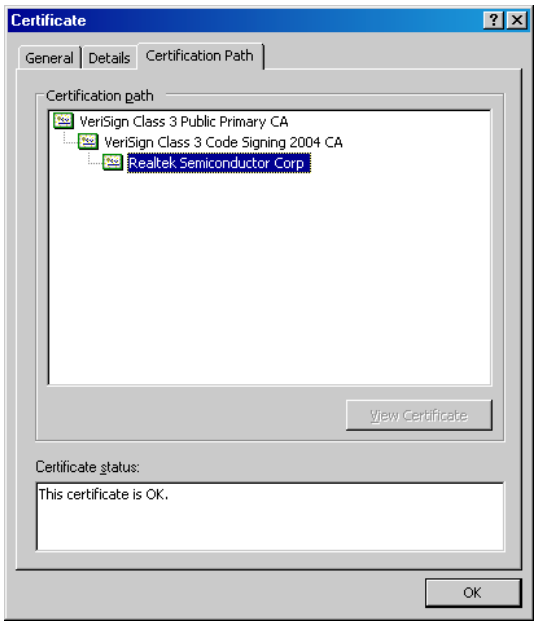




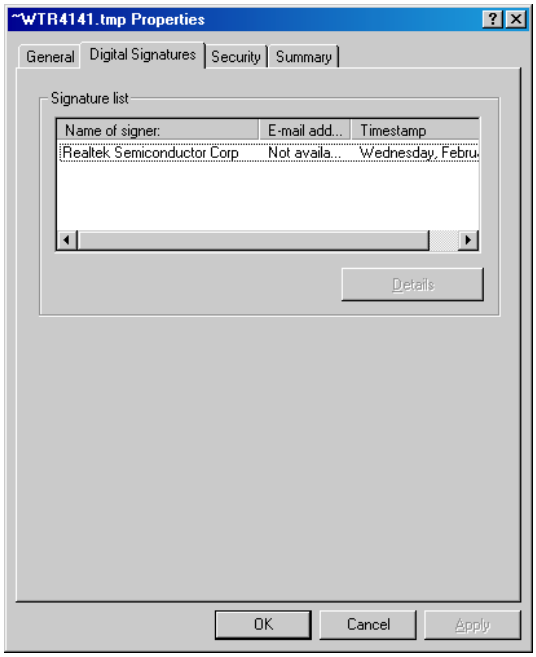


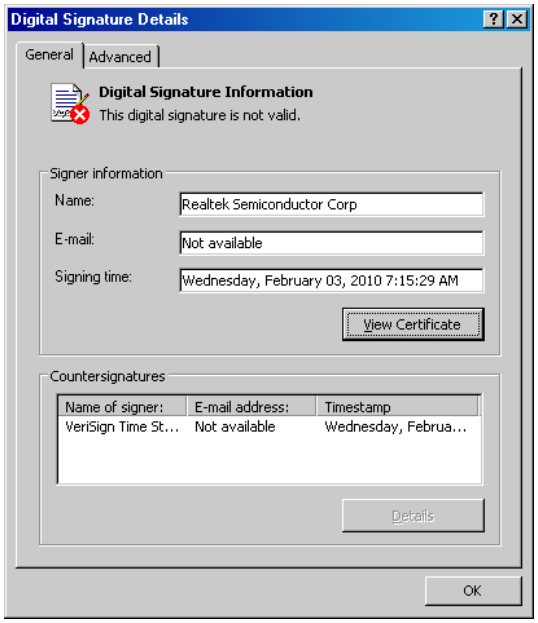


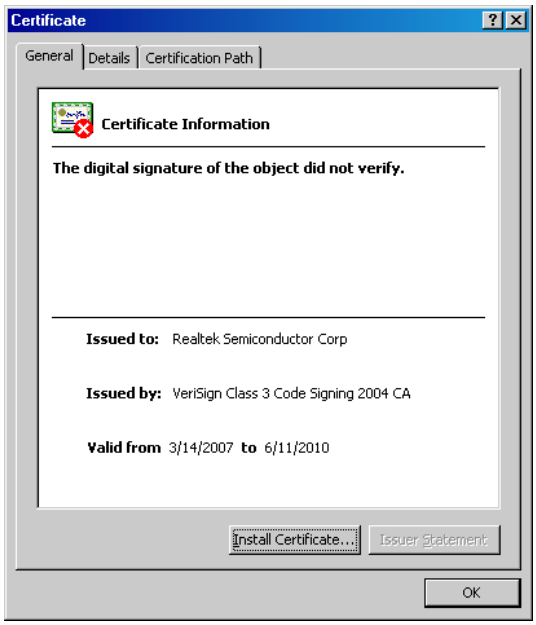


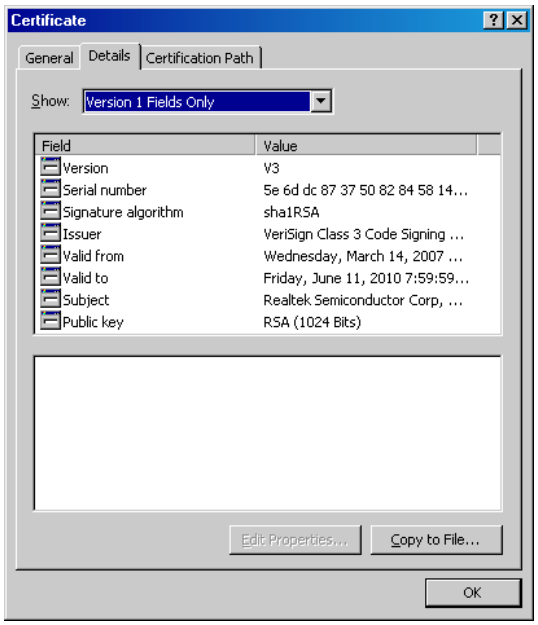


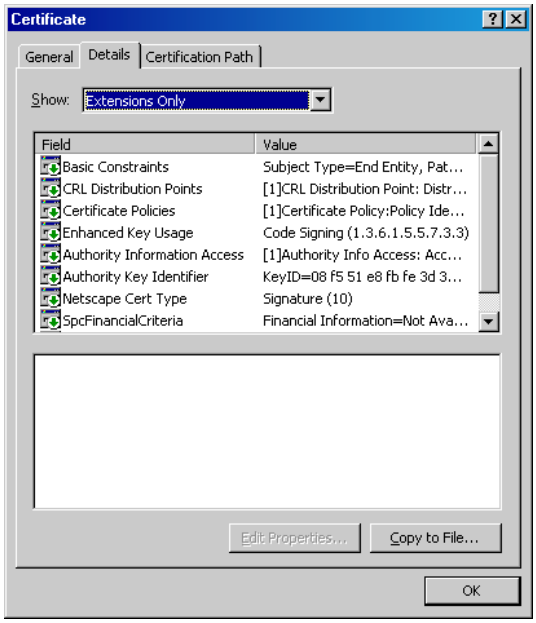
~WTR4141.tmp

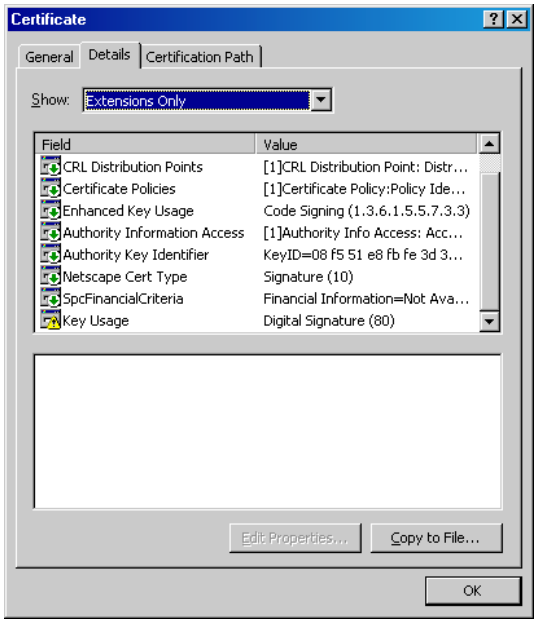


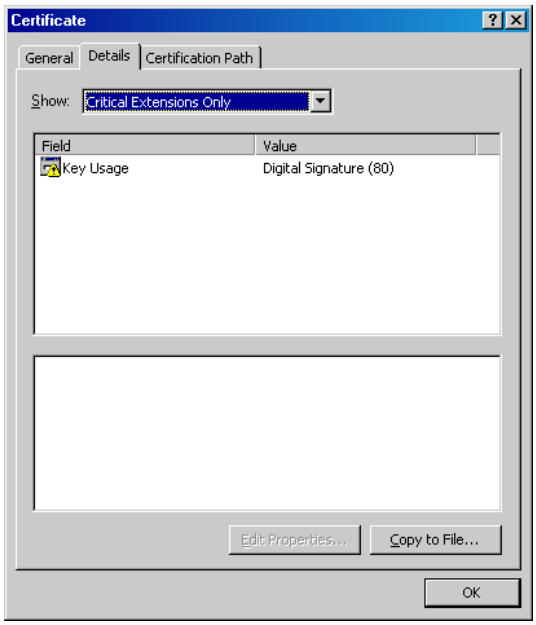


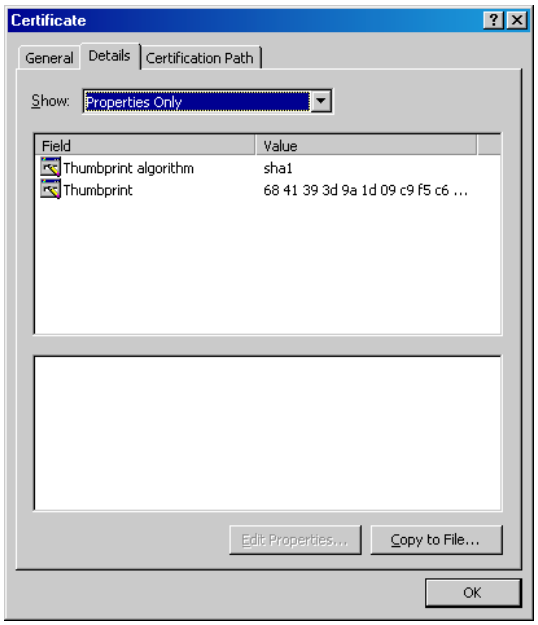


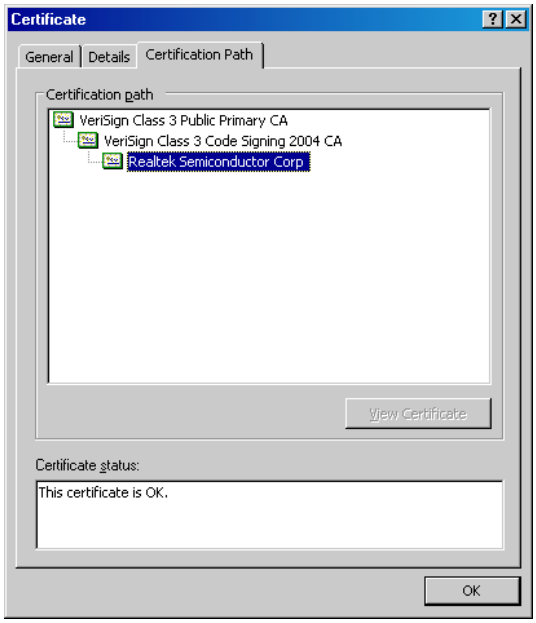


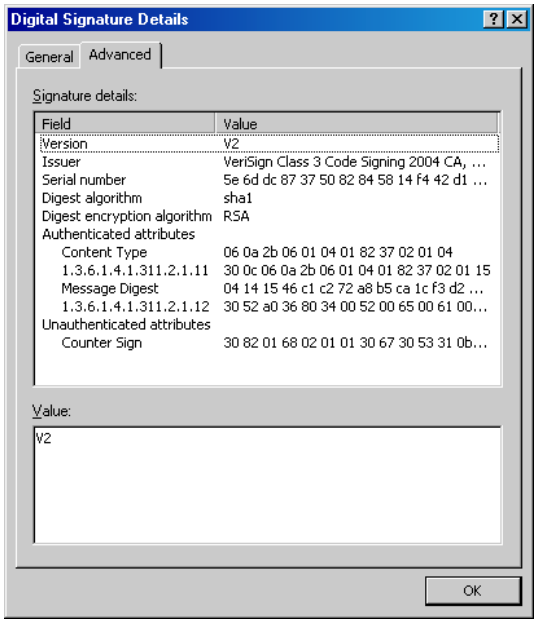












The 4 main files which constitute the STUXNET attack are:

1- .lnk file
2- ~WTR4141.tmp
3- ~WTR4132.tmp
4- Encoded payload .dll file with 13 functions and a variety of files (.dll, .exe, .lnk, .dat, .sys and .tmp)

The main encoded payload is a UPX packed .dll file.
NOTE: UPX is a free, portable, extendable, high-performance executable packer for several executable formats.

The UPX packed .dll is contained inside one of the files present on the infected removable drive.

How it Works

One of the best explanations on the Internet for understanding the details of how STUXNET works has been published by **Liam O. Murchu** (Supervisor of Security Response Operations for NAM at Symantec, CSFI-CWD – Cyber Warfare Division Member).
http://www.symantec.com/connect/blogs/distilling-w32stuxnet-components

CSFI has released an educational video of how STUXNET works in a lab environment:
http://www.csfi.us/?page=stuxnet

Attack Countermeasures

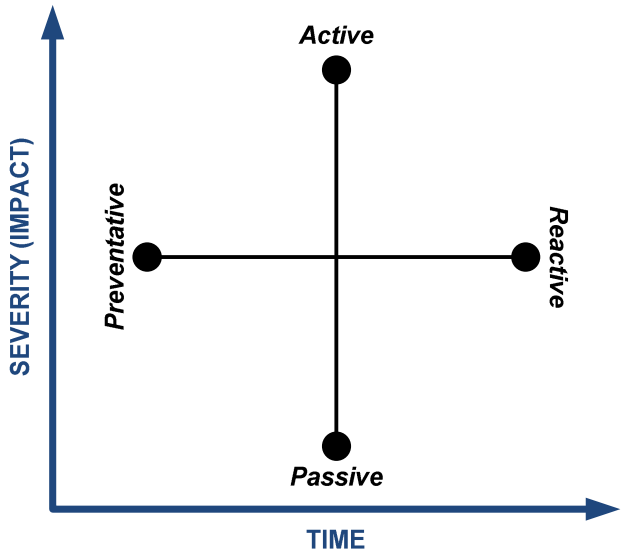
Many experts, some with and some without any relevant control systems experience are offering up advice on how to handle Stuxnet and Stuxnet-like attacks. While there are many different opinions[1], a point of general agreement is that a multi-layered approach is necessary to defend against an attack like Stuxnet.

Knowing this in advance means any mitigation needs to be based on a solid defense-in-depth strategy that utilizes multiple, independent layers of protection. The idea is that flaws can more easily be found in any one solution, but it should be increasingly difficult to find flaws in a comprehensive solution that depends on multiple protective measures.

A developing concept breaks the situation down into two distinct phases. The first set of countermeasures should be preventative in nature and designed to minimize the likelihood that a control system could be infected by such an attack. The second, and equally important, set of countermeasures should be reactive in nature, and designed to minimize any negative consequences to the control system should the system be compromised. Each of these sets of countermeasures should also possess both passive and active components that utilize direct and indirect methods in responding to the event. These countermeasures are then implemented in

real-time based on the severity of the attack (impact) and the duration the system has been under attack (correlating directly to the likelihood of greater damage or more negative consequences).

This is shown in the figure below:



This concept is further explored as countermeasures are now applied. This list is meant to be used as guidance to possible countermeasures that could be deployed and should not be interpreted as a list of which all items are required for every installation.

Preventative – Passive
These "preventative" countermeasures have revealed the general lack of an existing strong security policy within the control systems environments and reflect security controls that should be implemented on all systems prior to a Stuxnet-like event. These countermeasures include:

- Effective security policies and procedures (that cover all aspects of a security program, including training, security awareness, forensics, business continuation, etc.) are the first step to securing control systems. These policies and procedures then need to be reviewed and updated as part of a continuous improvement program.
- Implement a security awareness program within the organization that provides a baseline level of education relating to control systems security and includes regular re-training as risks and technologies change.
- Disabling of USB devices within the more secure control systems "zones" (security "zones" as defined by ISA-99). Not allowing external USB devices in these critical areas should be common knowledge, and hopefully Stuxnet will justify the need to become more diligent in use of these deadly little demons!
- Implementation of Software Restriction Policies (SRP) that prevent the execution of code on remote and removable media (USB, CD/DVD, network shares, etc.). Exceptions can be granted on a limited basis when required to support software maintenance and upgrades. Microsoft introduced this with Windows XP for a reason, yet few know it exists let alone

implement its policies. Until the control systems world is completely off of Windows 2000 and Windows XP platforms (which may take a very long time), this is a very viable countermeasure.

- Security Policies should be created that address specific host-to-host, and zone-to-zone communication requirements, including protocols, ports, etc. This information is vital and will be used in subsequent countermeasures to identify suspect traffic and is a basic requirement in complying with ISA-99 standards.
- Follow the vendor's recommendations for disabling of all unnecessary services.
- Confirm that any default username/passwords have been removed or modified.
- Utilize active vulnerability scanners on these systems (during testing or other times of non-production use) to evaluate and document the configuration against known vulnerabilities and predetermine compliance guidelines. The fact that Stuxnet is using MS08-067 shows that (1) vendors may not even be aware of the power of exploiting this vulnerability, or (2) they are assuming that no one will target these systems and there is not a need to address this patch. This vulnerability is showing up on many systems and is one of the most common vulnerabilities used to exploit control systems.

Preventative – Active

- If allowed by the system vendor, all hosts should be installed with applicable host-based firewall, anti-virus and anti-malware applications.
- Host-based intrusion detection applications should be utilized where allowed. Unfortunately, many vendors are not embracing the value of HIDS on control systems, yet some tests have shown that certain activities of Stuxnet would have triggered HIDS alerts, including DLL injection and rootkit installation attempts.
- "Whitelisting" based applications should be considered over "blacklisting" or "heuristic" based solutions whenever possible to increase the likelihood that zero-days will be detected. Again, it will take customer influence to drive vendors in this direction.
- Firewall rules should be implemented to deny by default all outbound traffic from the control system networks and zones. Justification needs to be given for outbound access, just like it is required for inbound, and when outbound traffic must be allowed, it should be between specific hosts AND for specific services.
- Outbound SMB traffic should not be allowed.
- Utilize code signing of all critical systems (in addition to whitelisting). Updates and changes should go through a unique traceable process at which code should be compared to an out-of-band provided signature from the vendor. Unless verified, code should not be allowed to run on the system.

Reactive – Passive

Identification of a threat is a valuable aspect of minimizing negative consequences of an attack. It may not be possible to eliminate completely all threats that exploit zero-days, but it should be a goal to be able to identify suspect activity that could signify an attack and minimize the consequences.

- Implement intrusion monitoring sensors within the control systems network(s) that are designed to evaluate data traffic patterns between system components. For example, a SCADA server should never be attempting an external file share (SMB) connection. Use the data obtained from the security policy to map out the allowed data paths that should exist within the system architecture. These sensors can also detect traffic that is not typically allowed between

nodes and could signify a rogue peer-to-peer network within the system or a possible backdoor or callback resulting from an attack.

- Implement passive vulnerability scanners on the control systems network that can be used to observe any unusual traffic patterns and correlate this against previous patterns, and provide an alert mechanism to signal deviations from normal. PVS can be used in conjunction with IDS.
- Review the system logs in the various computer hosts and network appliances. A lot can be learned by simply reviewing these log files because if logs are not reviewed, then the realization of being under attack may not happen until it is too late.
- A security information event monitoring application needs to be installed that can automatically analyze and correlate the data generated and stored in system logs and event journals throughout the system. Without SIEM, it is next to impossible to (1) analyze all this data and (2) make any logical correlation of the data between various hosts.
- Set up test and validation systems that mimic the production systems (at least for all the critical components), and implement a recurring comparison process between the production and test systems. This is something that financial institutions have been doing for a long time and is about time to get into critical infrastructure as well.

Reactive - Active

At this point in the attack, when all the other countermeasures have failed, it is very important to not destroy forensic data that can be used for a variety of purposes. Most of these security measures are used for forensic purposes in learning what failed and what can be done to prevent a similar attack in the future.

- Once the attack has been confirmed, all non-essential communication conduits should be terminated to contain the attack.
- Incident Response and Business Continuity procedures should be in place and initiated to maintain or re-establish essential operations while recovering from an attack.
- Care needs to be taken in following established and rehearsed forensic procedures to maintain the integrity of the data contained within the infected systems.
- Plans should be in place, tested on a recurring basis, and updated in order to be effective in the event of an attack.
- As a last resort, it may be necessary to initiate a shutdown of the manufacturing process to minimize the potential for environmental or loss-of-life resulting from a potential control system failure.

Political Motivations behind the Attack

Our research points to the fact that the motivations behind the attack are of a destabilizing nature with less focus on destruction of data and more focus on disruption of operations and PsyOps. The coordinated nature of this attack, the choice of exploits and the main targets are strongly indicative of state sponsored activities.

“More and more I am convinced of the psychological effect as being the central point of this ‘exercise’.”
--Izar Tarandach, Principal Software Engineer

Cyber attacks of this nature have a “one shot, one kill” approach to things, due to the fact that after the attack takes place the security community will rush to create countermeasures and dissect the code. The attacker most likely accomplished its mission of infiltrating the Iranian nuclear facility and creating possible delays in the nuclear program and also creating uncertainty in the victim’s mind.

We believe this cyber attack to be a successful attack and not only as an attempt, like many other analysts may believe.

STUXNET in a Cyber Warfare Scenario

Due to heavy scrutiny with NERC CIP compliance, attackers may not target the grid directly or any other critical infrastructure component. The attacker would most likely keep the noise level down by creating a flanking strategy and target the level below the grid, which is not currently in the spotlight and is more vulnerable. For example, something has to feed these gas-fired power plants with fuel using the same control systems. They would target LNG re-gasification and distribution systems, which would cripple the power generation plants and produce the same end result. The attacker may target strategic refineries that would cripple not only civilians with fuel shortages, but would also affect the military - the Navy may be nuclear but the Army and Air Force need petroleum-based fuels. Many refineries have control systems that are extremely vulnerable to cyber attacks.

In case of Cyber Warfare, the US critical infrastructure and the critical infrastructure of its allies would be prime targets to well crafted and coordinated attacks resembling STUXNET.

Can Iran retaliate using the same form of cyber attack? What are the chances of such an attack taking place against the US and allies?

As long as there is a gap between policies and technical controls, this type of attack will be possible. Some organizations currently have no policies and no technical controls, others have strict policies with nothing technical enforcing the policy, and some (rarely) have both. For example, the location of the initial infection may have had a policy that stated USB drives are not allowed but nothing that actually prevented them from being used. All that to say that anyone, Iran included, could attempt such an attack by throwing a few bad USB drives in a parking lot and waiting to see who picks them up or making up some "informational" DVDs and leaving them on a table at a conference.

Since the exploit code is widely available and 2 vulnerabilities remained unpatched, we believe the U.S. is at a moderate risk level. Immunity has released exploit code for the 2 unpatched vulnerabilities, so this is easily available to an attacker of any skill level.

A large percentage of the people really do not understand STUXNET; therefore, special care should be taken at this time.

We believe that the worm would need to be modified in some manner to fool signature-based detection systems that seem to be the primary means of detection at this level. However, since many have not implemented a solid defense-in-depth strategy, the attack could be launched successfully.

The leading suppliers of distributed control systems for North America are Emerson, Honeywell and Invensys. Much attention must be placed on how secure these systems are. Variants of STUXNET could be developed to penetrate such systems.

If we look now at regions of interest like the Middle East, one player is very strong in key infrastructure control systems, and that is Yokogawa out of Japan. A lot of this is politically motivated, because the Muslim-based countries post-2001 have tended to move away from U.S. and U.K.-based companies, leaving only Yokogawa, ABB (Switzerland) and Siemens (Germany) as potential players. We already know Siemens position, but Yokogawa is one of interest. Most of the design and engineering decisions come out of Japan, and according to our intelligence they do not really seem to place security as a priority for their system design. They focus more on reliability and functionality.

Yokogawa is also installed in Iraq. Knowing that Siemens and Yokogawa are the two primary players in the region, there is a 50/50 chance of a successful attack if one targeted one of these systems. If the attacker had targeted Emerson or Honeywell, they would have had little if any penetration in Iraq. This is one piece of data that justifies the argument that this was most likely a targeted attack.

Protection against Stuxnet-Like Attempts

1. Vital points for Stuxnet success
   - 1.1. Intelligence
   - 1.2. "0 day" vulnerabilities
   - 1.3. Kernel manipulation
     - 1.3.1. Rootkit
     - 1.3.2. Digitally signed certificates
   - 1.4. SCADA systems weaknesses
     - 1.4.1. Lack of proper monitoring and check points
     - 1.4.2. Lack of proper standards
     - 1.4.3. Security as an additional feature

2. How to mitigate Stuxnet and the like
   - 2.1. Blacklist vs. whitelist approach
   - 2.2. Monitoring and incident response
   - 2.3. Virtual and physical security policies
   - 2.4. Operating system choice
   - 2.5. Humans

1. Vital points for Stuxnet success

The important aspect that made Stuxnet successful was the intelligence in its preparation. Security thorough obscurity is a concept that rarely holds strong and often fails.. Stuxnet creators exhibit thorough research and a great depth of knowledge of the schematics and internal workings of Siemens SCADA systems components, which ultimately resulted in the discovery of a hard-coded passphrase in Simatic WinCC. This is what allowed complete access to servers running the server. Vendors and administrators still have not learned to remove default settings.

1.2. "0 day" vulnerabilities

The collection of "0 day" vulnerabilities in Stuxnet is considered to be the biggest collection for any worm to have in the history of computer viruses. Although there is speculation as to the exact amount of undiscovered vulnerabilities, speculation about the initial and post-discovery payload, in the end it contained multiple unique vulnerabilities. Many perceive this to be a sign of great funding and/or great skill. Here the concept of security thorough obscurity might be an element in making the discovery of vulnerabilities a difficult task; however, once found, the authors of Stuxnet (or any other group of people that would like to make use of discovered vulnerabilities) will most likely not report these issues to the vendor.

1.3. Kernel manipulation

Stuxnet was discovered to contain a very simple yet effective rootkit that allowed the worm to be hidden completely from user-space applications. Add the methods of detecting installed AVs in the system, and the rootkit might be capable of disabling any AV installed, which effectively renders the whole system to be wide open to other types of malware. While reliance upon Antivirus is not a full-proof solution, many vendors and administrators still believe "updated" signatures to save their networks.

1.4. SCADA systems weaknesses
1.4.1. Lack of proper monitoring and check points

The Stuxnet incident showed how monitoring of such phenomena was, at the very best, minimal. Stuxnet had the capabilities of infecting PLC units from WinCC servers, which shows that WinCC had no restrictions or any kind of authentication required for such process. This raises a lot of concerns towards machinery connected to these PLC units. A solution has been presented by Chris Blask by implementing SEIM/SIM monitoring. Had SEIM/SIM monitoring been enabled along with proper "lowest privilege" access along with auditing, the discovery of Stuxnet would have likely come earlier.

NOTE: The remote instance of SQL Server has the default “WinCCConnect’ account enabled with its account enabled with its default password set. An attacker may leverage this flaw to execute commands against the remote host, as well as read the content of the WinCC database if present.
Source: http://www.nessus.org/plugins/index.php?view=single&id=47759

1.4.2. Lack of proper standards

Currently there are no "de-facto" defined standard for SCADA systems applications, physical, network or product security solely guidelines. How an environment so mission critical can end up using hard-coded passwords in software and/or hardware is boggling. Situations like these will be persistent until vendors are pressured and/or discouraged from these practices; however, even with hardcoded passwords, proper Role Based Access undertaken on the network and physical level could have mitigated against this. Summarily, a SCADA systems security standardization group must be formed and establish security standards for software, network and physical security of SCADA systems.

1.4.3. Security in general is thought of as an additional feature

In critical infrastructures and environments, security MUST always be the number one concern. Security is compromised of all layers: physical, network, application, session and hardware. Stuxnet was effective at attacking the low hanging fruit—default passwords and the lack of updated patches in the Windows platform, which ultimately exploited the SMB service in the NT kernel. Such service should have never been used or enabled in the first place; however, this is the default installation parameter for Windows. It should have been double checked post deployment. This suggests that security is an afterthought, and this type of thinking MUST change in the near future.

2. How to mitigate Stuxnet and the like

Stuxnet cannot be treated by an AV, as AVs are not practical in responding to new threats, especially when the threat is against a zero day (0 day) attack. Vendors are not aware of the vulnerability, hence no signatures being available. Immunity from such threats must be sought out by modifying policies and behavior, enforcing security training and enhancing security standards. While SEIM/SIM was mentioned before, HIPS (Host Intrusion Prevention Systems) would have alerted the administrator(s) to the changes in the checksums of the file system that was infected by Stuxnet. Layered approaches to security make compromising a machine more difficult as there are more layers to attack, which increase the risk of detection.

2.1. Blacklist vs. whitelist approach

Foreign traffic must not be tolerated in a SCADA system. Most applications are static as is the traffic necessary to operate those applications and or services. Baselines can dictate what is normal and what is anomalous. While a white or a black list of software and or connections may be created, the reality is this list may be difficult to maintain and/or subject to tampering. A network IPS configured to allow only the minimal needed traffic inside the network should be MANDATORY with alerting to those in an emergency response team. Because many ERTs can be tricked with false positives and false negatives, constant reviewing of parameters need to be enforced otherwise administrators and engineers will learn to ignore alerts.

2.2. Monitoring and incident response

Traffic must be logged at all times on a separate hardened system, which should have the capabilities of performing data, network and application correlation. If available, "flow-tools" like implementations can be deployed where entire sessions may be replayed, analyzed and assessed. This minimizes the response time, drives down the potential cost of forensics and maintains a good level of validity for evidentiary purposes when applicable.

2.3. Virtual and physical security policies

The lack of clear, definite security policies has been a major player in Stuxnet's success; policies must be in place to limit both physical and virtual access. Stuxnet exploited SMB on Windows machines, which means whoever made Stuxnet has collected information that SMB is enabled in quite a large number of machines. Of course, SMB has no use whatsoever in such environments, and even if they do, they should have isolated these weak services from the critical region of the environment because SMB is a main entry point to any Windows system.

2.4. Operating system choice

In an environment that has computers control very sensitive machinery, stability and reliability are very important, but security shares the same importance. Windows was made first and foremost for desktop users. As for stability, Windows is far from it; usually a BSD system or Linux should replace Windows on all machines that are responsible for the industrial machinery or anything related to it.

2.5. Humans

The human factor is a very important security aspect; many studies have shown that the easiest way into any organization is not their computers, but rather their employees. In Stuxnet design, it has been seen that it had an exploit for a Windows vulnerability and a technique developed to exploit a human vulnerability of curiosity by simply dropping a handful of USB flash drives around a facility. Proper security training must ensue for employees working in such facilities, along with raising their general security awareness. Regular security checks on what people bring in and out of the facility are very important.