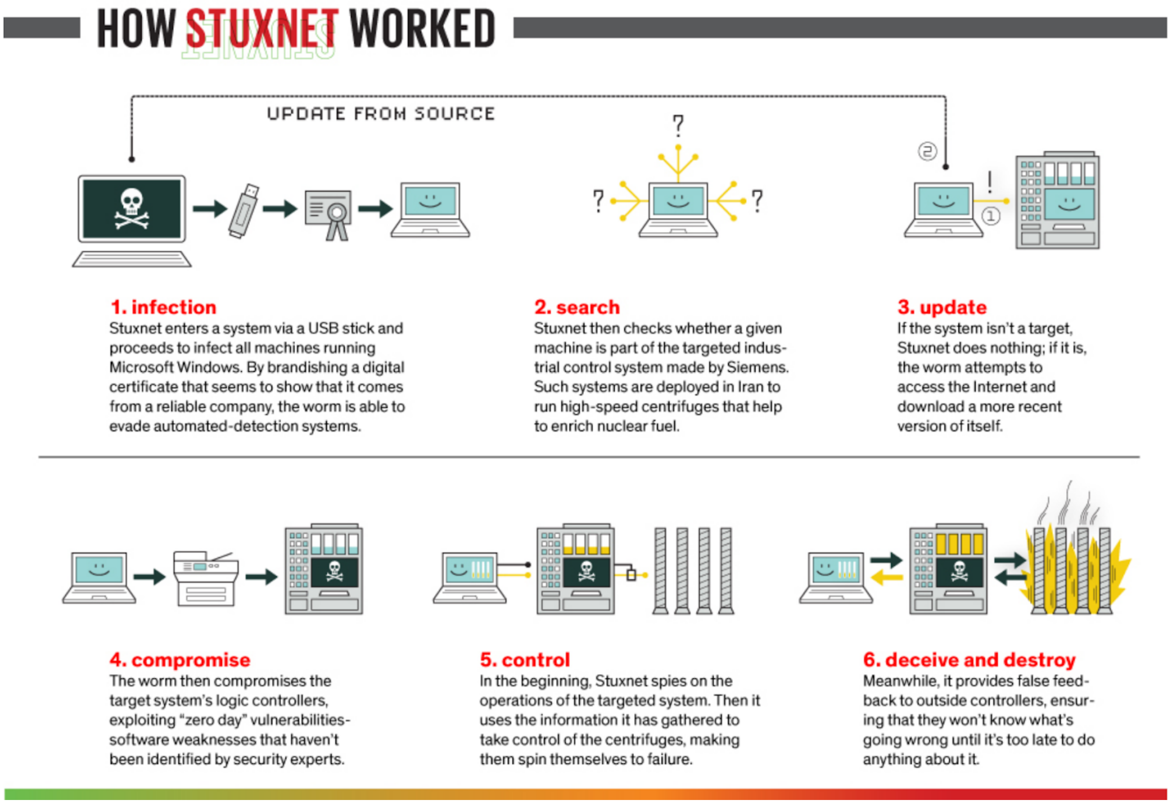
Review Stuxnet and propose a Risk mitigation Proposal

- Should cover Plan/Process of Detection, Validation and Mitigation
- Should also cover residual risk not covered by Technology like People/Process
- Also, Answer - If you find vulnerability would you ?
  - Limited disclosure, full disclosure, responsible disclosure, commercialization
  - Each has costs/benefits options



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Review Of Stuxnet and Mitigation Proposal

Review of Stuxnet

Stuxnet is a Malware that came news headlines as it surreptitiously tried to restrain Iran’s Nuclear fuel enrichment program. It is 500-kilobyte computer worm infected 14 industrial sites in iran including a Nuclear enrichment plant. Even though Stuxnet is a computer worm, the source of infection of the worm could be done only through a USB. Once Stuxnet is in a system its ready to spread on its own and being stealth.

Stuxnet is a perfectly designed computer worm and worked in a series of steps.

1. **Infection**: Targeted Microsoft windows machine and network and replicating itself.

2. **Search**: Performed a reconnaissance of Siemens Step7 software, a vulnerable software based on windows and used to program control systems and operate industrial equipment such as centrifuges.
3. **Update**: If a vulnerable system could not be found then Stuxnet would do nothing malicious. However it would update itself, to a newer version of itself, if internet was accessible.
4. **Compromise**: It would compromise the programmable logic controllers, exploiting the ‘zero day’ vulnerability in the software running in industrial systems.
5. **Control:** It would spy on the information on the operations of the targeted systems and then would take control of the industrial system, and cause malfunction, like increased the angular velocity of the centrifuges to a point of failure without cognizance of the industrial systems monitors.
6. **Deceive and Destroy**: While it takes control of the industrial system, Stuxnet continues to send false information to the controllers ensuring that the Industrial systems are not recoverable.

Stuxnet took advantage of four zero-day exploits (vulnerabilities previously unknown to the white-hat community, computer security researchers who breaks into protected systems and networks for testing)

Security Flaws used by Stuxnet

Stuxnet used the common security flaws in the computers and lack of knowledge about information security in humans, to imprint itself. Stuxnet designers had researched about their target and understood them and exploited them. Like any criminal

- It can only be installed through USB, so it starts with *human gullibility and lack of knowledge*
- Zero-day Vulnerabilities, *exploit unknown vulnerabilities*. This is an area which the designers of stuxnet have spend considerable man months to identify as this is the *Achilles heel* that they would base their attack vector on.
- Being stealth in the operating system (Windows in this case), even though it was a process it was able to hide itself from process monitors.
- Targeting an application which had *vulnerabilities*..
- Being stealth in the Network infrastructure by *minimizing it’s network activity*, by being able not to be detected by any network monitoring software or security appliance. Since stuxnet was updating itself and communicating with other windows devices in the network, there would have been traces of packets originated by Stuxnet.
- From an organization perspective lack of security audits which would ensure and protect physical and intellectual assets. Regular upgrades of devices with more secure version of software and patches are encouraged.

Planning to Detect a Worm Like Stuxnet

The previous section illustrates the security flaws used by Stuxnet. The financial cost for the plan to detect a worm like stuxnet is beyond the scope of this proposal. The scope of attack for Stuxnet were industrial complexes, infrastructures etc.
So in order to secure an industrial complex with people and automated machines it has to be a *dual* approach factoring into Humans and Machines.

Mitigation of the Stuxnet Worm

Like in Stuxnet, majority of the *cyber-attacks* are *initiated* with targeted attack through Humans. We will look into both the aspect of Human factor and the Machine (hardware and software) factor in the plan to detect a worm like Stuxnet. No systems are '*completely secure*'. *Security can only be improved by making the threats visible. Visibility can be achieved through protecting the system, monitoring for any malicious activity and being aware of the weaknesses.* The section below highlights the steps that would make the organization visible from a worm like stuxnet.

Human Factors in Information security

No	Actionable Item	Actions	Threats prevented
1	Train people on information security	● Have an awareness about how people are gullible. ● Impart a consciousness about devices and their pitfalls (USB drives, spam emails, online downloads etc)	● Stuxnet would not have spread if the people in *did not use* USB. ● Also *sanitizing* USB with a *software security scanning tools* could have prevented it.
2	Frame and enforce policy on hardware, software usage on the industrial complex	● Create levels of authorization, access and accounting among the employees. ● The accessibility of devices should be restricted based on the authorization. ● Reward people for demonstrating cyber	● Security awareness among people may lead to fewer mistakes ● Access on a need basis helps *accountability* and *ensure*

		security awareness. • Having signboards helped improving industrial safety, so having *signboards on cybersecurity* might improve cyber-security awareness.	*responsible behavior*

Hardware and Software Factors in Information security

No	Actionable Item	Actions	Threats prevented
1	Authentication, authorization and accounting	• Securing system access	• Unauthorized access of systems and resources
2	Use secure hardware and software in the organization.	• Account for each physical and virtual device being used in a premise. • Ensure that the hardware are crypto signature in them. • Ensure that the operating system are hardened, patched with the latest security fixes. • Ensure that the operating system being used in these devices have the latest patch • Look for the latest vulnerabilities in operating systems • Disable physical ports that would not be necessary, Like USB or serial ports etc • Identify compromised h/w & software	• Threats from insecure hardware and software • Threats from insecure software that are being used in the premise • Knowledge about latest threats alerts users •
3	Regular monitoring of the softwares that are being run in the systems	• Rootkits makes the system compromised, monitor the *cryptographic signatures* of the applications, while	• Detect a process that's running in a machine so that the machine

		monitoring them.	is not compromised.
4	Third-party software should be sanitized before using them	● Use a anti-virus/worm detector before rolling an application.	● Being alert and cautious keeps the system safe
5	Secure Network Design	● A well designed network would start with creating defined boundaries of accessibility, authorization and accounting for applications and users. ● Not all devices need to have access to the internet. ● Use firewalls for securing from attack vectors from network traffic. ● Use a IDS/IPS to generate real time alerts ● Use dynamic ACLS to reduce time to react for anomalies in networks.	● Access of the machines in network would restrict spreading of the worm. ● Detect traffic anomalies. Look for packets that does not belong to the network or from unknown applications.
6	Email security	● Emails attachments could bring in worms in a network. Sanitize before they are open. ● Detect phissing	● Eliminating the source of attack
7	Monitor	● Monitor Application logs, application signature ● Look for patterns in network traffic and applications ● Look for anomalies in network traffic and applications ● Use tools to help monitor	● Increase visibility of systems and software.

Residual Risks

In Spite of all the security measures there would be new security threats. Key among them would be

- Human mistakes like using a insecure USB
- Falling victim to a phishing email

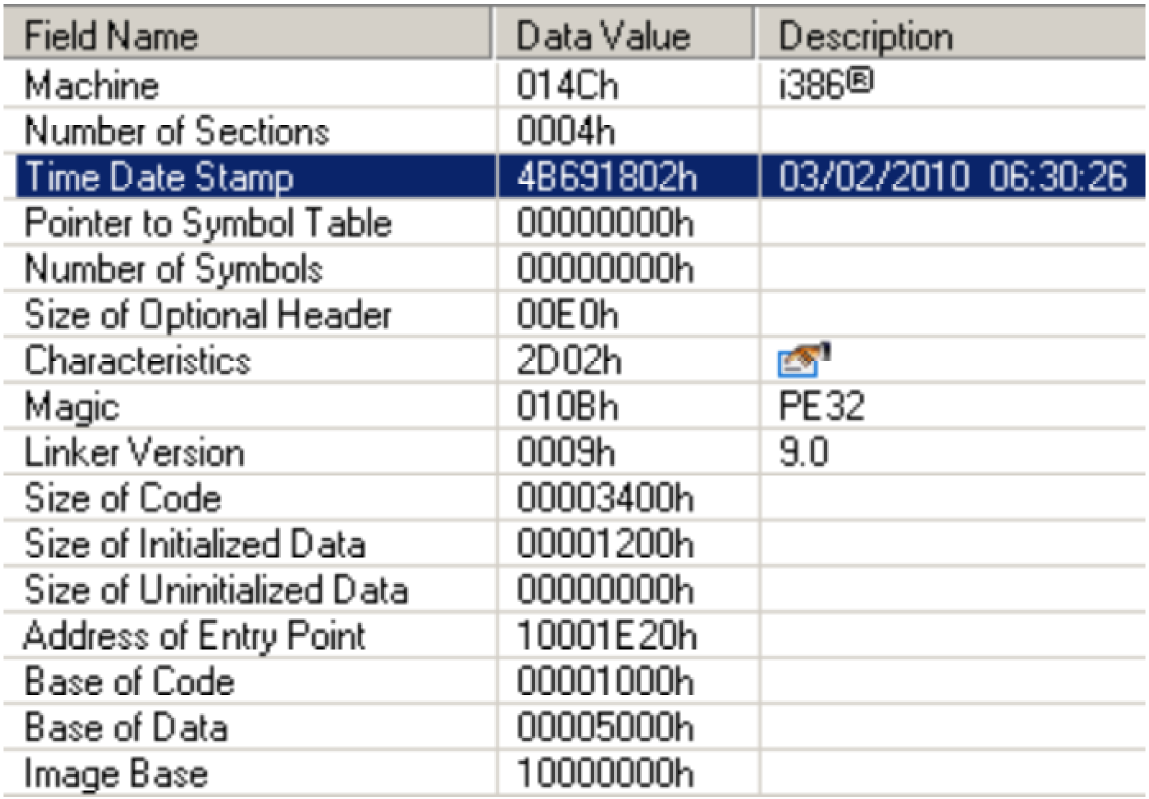
- New attack vectors being tried by black-hat hackers
- ‘Zero Day’ Vulnerabilities
- Physical security being breached

Validation of the Stuxnet Worm

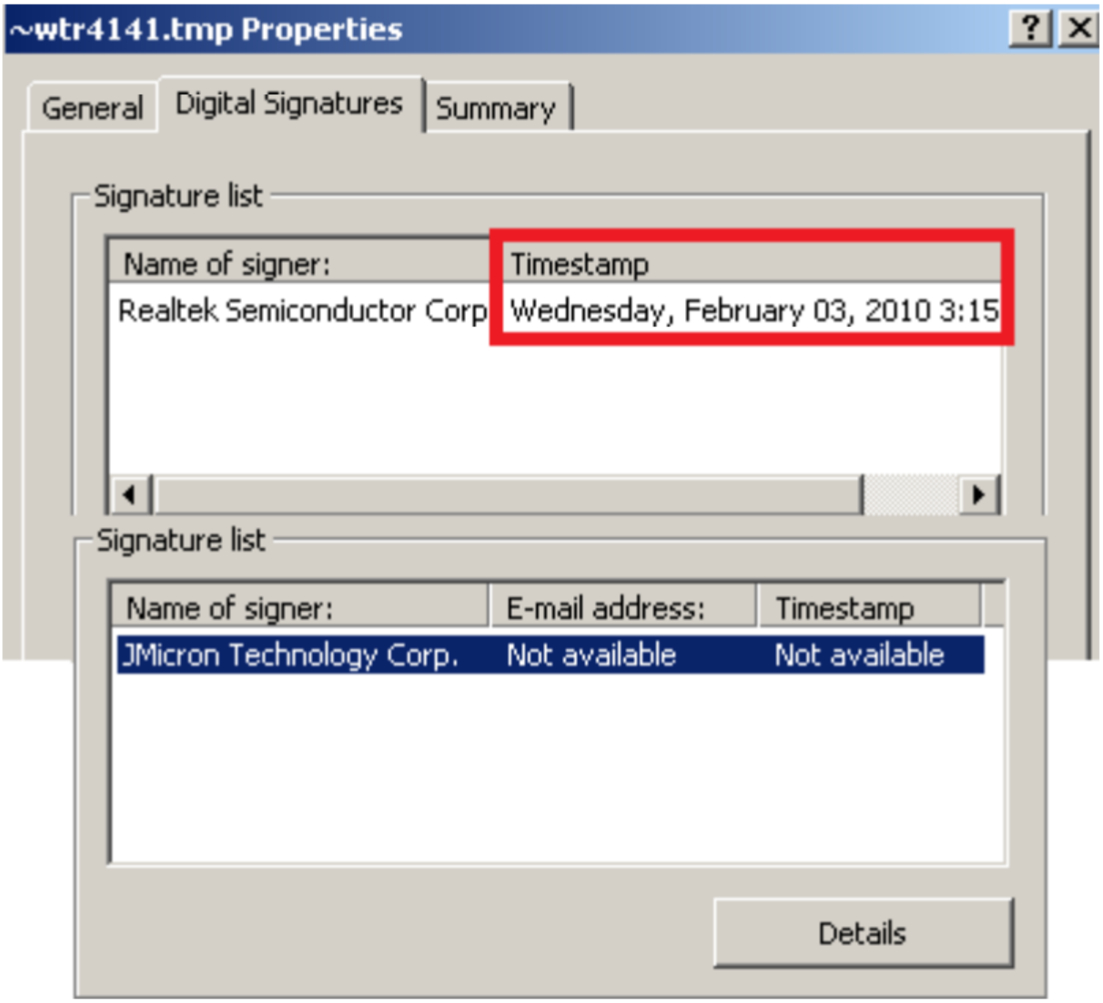
Most of the worms like stuxnet begins with an exploit, using the system vulnerabilities, followed by the steps of infection, compromise, control. In case of Stuxnet, it also intended to update itself, keep it self stealth till it found a target and could destroy the system once it found it’s target.

Since the behavior of the Stuxnet worm has been reversed engineered a well defined steps to monitor devices and network would detect the presence of the worm.

1. On a host there are tools to detect the stuxnet worm. The stuxnet worm reveals the following date and timestamp. Stuxnet detailed out a digital signature which looked authentic.



Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0004h	
Time Date Stamp	4B691802h	03/02/2010 06:30:26
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	2D02h	
Magic	010Bh	PE32
Linker Version	0009h	9.0
Size of Code	00003400h	
Size of Initialized Data	00001200h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	10001E20h	
Base of Code	00001000h	
Base of Data	00005000h	
Image Base	10000000h	



~wtr4141.tmp Properties

Signature list

Name of signer:	Timestamp
Realtek Semiconductor Corp	Wednesday, February 03, 2010 3:15

Signature list

Name of signer:	E-mail address:	Timestamp
JMicron Technology Corp.	Not available	Not available

a. STUXNET scanner from from Trends lab
b. Stuxnet scanner from symantec

2. Monitoring network traffic. The amount of traffic generated by Stuxnet makes it like finding a needle in a haystack. However there are the following information available about stuxnet which makes it detectable in the network.

“After Stuxnet infects a machine, it creates a RPC server and listen to any connections comes from the any PC on the Network. In the other PCs in the network, stuxnet establish a connection with this RPC Server. This way allows stuxnet to update itself in the isolated PCs (from the Internet) but has in its network a PC has the ability to connect to the internet. This way is to suitable while infecting companies as there are some inside PCs haven't the ability to connect directly to the internet.” source

"*Stuxnet updates itself via Internet by establishing a HTTP connection to 2 malformed websites:*

- *www.mypremierfutbol.com*
- *www.todaysfutbol.com*

It sends an encrypted data like that http://www.mypremierfutbol.com/index.php?data=data_to_send This data contains the IP, the Adaptor name and description and some other data related to the infected machine and stuxnet. After that it receives the newer version of stuxnet (in an encrypted form) begins by the imagebase then a flag and at the last the Executable Image
" source

So monitoring for RPC traffic in the network and monitoring for traffic to these 2 domain would would indicate presence of Stuxnet on devices in the network.

What would you do if you Finding Vulnerability

Software or hardware do come with bugs, known and unknowns. Being a s/w developer myself, Any unknown bugs should be recognized and be given a Mean time to repair (MTTR).
If i found any vulnerability in any software or hardware, i would be doing a "*Responsible Disclosure*", reporting it to the developer (if its a open source s/w) or to a organization which has build the software. If the bug is not resolved within the promised time then the vulnerability should be made public, So that users can take safeguard against it.
Information about a vulnerability which impacts people's life should be done with "*Full Disclosure*" with the details and possible safeguards. This would prevent a malicious hacker from using it any more. This would also make the concerned applications to be aware of the security hole and can take remediation actions.

Conclusion

Stuxnet is one of those computer worms which was designed meticulously and tried to commit a crime leaving no traces. It's damage has not only been financial for the targets but it has opened up new avenue of exploits for black hat hackers. The Stealth mode nature of the worm makes it undetectable. Since the target systems are still unknown it would be years before it finally gets eliminated from the computer systems.

References

1. https://www.codeproject.com/Articles/246545/Stuxnet-Malware-Analysis-Paper#ch4.4.2
2. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
3. https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf
4. https://searchsecurity.techtarget.com/magazineContent/How-to-write-a-risk-methodology-that-blends-business-security-needs