Report on link stuxnet worm

Law, Security

Abstract

The prevalence of information system and networked infrastructures brings huge advantages for the organizations however these infrastructures also impose greater vulnerability in terms of intrusions and virtual attacks. The entire industries and government worldwide are dependent on the interconnected array of critical networks and resources that can be accessed or entered from anywhere in the world. Cyber security uses different tools, policies, risk assessment and management practices and technologies to protect the information and the communication infrastructure from any illegal or unwanted intrusion or modification. The assessment of cyber security vulnerability assists the IT managers to ensure that no loop hole or missing link is present that can provide an opportunity to the intruders or malware to enter the system.

Since most of the infrastructures are interconnected today with other networks and systems the probability of broken or weak links is all more ubiquitous. The reporting of Stuxnet Worm in 2010 has opened new threats to the cyber security of huge industrial infrastructures.

This paper discusses the worm and the possible damages it can do to industrial systems. The paper shall also discuss the weaknesses in these systems that will make them prone to such attacks in the future.

Symantec reported a new type of worm, called “ Stuxnet” in 2010 , emerged as the first software that could be used as a cyber weapon thus opening a new era of cyber crime now referred to as cyber war.

The research on the worm implied that the worm was specially designed to

monitor, control and even operate industrial plant machinery and infrastructures abnormally that could make them causing physical damage of unknown sorts.

The cyber worm Stuxnet first struck the Iranian Nuclear facility in Natanz in June 2010. The worm caused the centrifuges in uranium enrichment facility to fail at an abnormal rate. The worm damaged about 10000 centrifuges that invoked a panic in the facility.

The success of Stuxnet brought several eye openers, firstly it publicized the security breaches and vulnerabilities in the SCADA(supervisory control and data acquisition) that controls power circuits, pumps, motors and valves in industrial facilities. Upon entering a system the worm can send irregular instructions to the system and can control these machineries that can cause unimaginable destruction to the system

Stuxnet, represents the new breed of malware or worms that have the special techniques that keep them hidden and unnoticed. The modern era malware are developed without any packing thus they get installed easily as a system utility and provides backdoor for the attackers.

The Evolution Of Stuxnet

According to the research by Semantics, Stuxnet 0. 5 is the oldest version of the worm developed or tested in 2007. The older version was not as aggressive or as destructive as the current version Stuxnet 1. 0 and could only spread through infected Semantics Step 7 project files. The goals of the earlier version of the worm are unclear thus it is unknown if that version was successful or not. The earlier version only intruded the communication between computers and the command and control systems. Although the

earlier version too had code to attack valve systems while the current version can make modifications through the valve system The current version of the worm is however thought to be one of its kind and is capable of controlling sensitive machinery by commanding them to operate abnormally.

Threats From Stuxnet

Stuxnet, is considered to have digital certificates for authentication and exploits the Windows & zero-day vulnerabilities 2 of which do not have patches yet. These tools make it more dangerous as it can enter a system undetected and authorized.

The prior experience from the worm at the Iranian nuclear facility suggests that if left unattended the worm could claim irreversible damages to any industrial or power plant. This fact also implies that a terrorist attack in future might target a power plant such as the electricity power grid station or the telecommunication system of a country that may cause panic and uncontrollable damages to the nation. Thus the related authorities need to be more aware and vigilant to assess the vulnerabilities of their system.

According to a report prepared by the Department Of Homeland Security regarding the cyberspace security measures and programs, though the worm Stuxnet has done most damages to Iran’s nuclear facility however there have been other minor attacks on other countries as well. The graph (fig 1 shows the percentage of the hits by the worm during a single year. In the report DHS also emphasizes that the threat like the worm need collective efforts across the world while partnering with other countries to find and mitigate the probable risks to cyber security aimed at any country.

The head of cyber security at DHS, Sean McGurk, believes that the worm is considered to have complex and very diverse capabilities that are almost unknown at this point. The worm could be a new era of cyber crime and can change the face of it completely. The limited research and knowledge that the experts have about it right now cannot inform whether it was designed to attack and demolish the nuclear facility only or can be an annihilator for any machinery based system that can provide an access route for it to enter. This points in the direction that the authorities in cyber security are still unclear on what could be the right solution or path to restrict and eliminate this threat. Since no law is in place for such threats the liabilities at stake are even more.

Stuxnet As the Most Important Threat To Cyber Security

Cyber security is a continual process of assessing, designing and managing tools and techniques to protect the systems from any unwanted entry or intrusion. The defensive process for cyber security concentrates on 3 main components that are access, vulnerability and payload. The strategy for restricting cyber attacks is built around 2 or more of these components. According to the description of the Stuxnet worm, it is mainly targeted towards Industrial Control Systems (ICS) and exploits the vulnerabilities in these systems to enter and then control the machinery. Thus the first requirement for the IT managers of such industrial plants is to look into the vulnerabilities in these systems that can give an entry point to this destructive worm. The first attack of Stuxnet suggested that the worm had been designed to target SCADA with ease and managed to successfully enter and control the system. Security experts reveal that SCADA was not

originally designed for being interfaced with cyber space therefore key issues regarding cyber security were not focused or considered for the product. The security experts also believe that the attack on SCADA urged the experts to focus on the flaws of SCADA however certain prior projects have exposed serious vulnerabilities in the industrial PLCs by leaders such as GE, Rockwell and Schneider etc. this imposes extra threats as any system other than SCADA could easily be targeted in any industry.

ICS by any vendor are designed into different components working at various level with the data , operations or the system users. Hence attackers have various points of entry. The end user components are usually on simple terminals with commercial OS such as Windows. It has already been proven that Stuxnet could exploit Windows 7 zero-day flaw to enter the system. Similarly, the entire system is interfaced with various components thus an intrusive program can be sent through several channels such via network, via interfaces like USB etc. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of DHS reported discovering 3 instances of a malware from a USB drive terminal which was used for system backup. Also ISC-CERT reported spreading of an infection through a USB drive causing damage to 10 computers linked to the turbine of a Power & Energy company. For the awareness of the IT managers ICS-CERT has issued a list of common and most probable vulnerabilities in the ICS products as given in the figure 2.

Vulnerbilities Targeted By Stuxnet

Like any malware or worm, some specific vulnerability is targeted in commercial solutions. The prior experience with Stuxnet showed that the worm typically exploited the Siemens based industrial controllers to enter

the systems. Likewise, it has been researched and shown by a security researcher Beresford , working with ICS-CERT that the Siemens industrial control system was found to have a hard coded password left unattended that would easily let any malware/worm to enter and reprogram the system and send any commands. The researcher specifically tested several models of Siemens programmable logic controllers that are widely used in commercial industrial and manufacturing environments and were the same model used in the Iranian nuclear plant that were targeted by the attacker. The worm exploited the Siemens step 7 program files that monitors and programs the PLCs and utilized the hardcoded password passage to send malicious commands to gain control of the entire system. The experts believe that due to this vulnerability the attackers can even restrict administrators or authorities to enter the system. The authentication procedure to program PLCs from Step 7 was also found to be weak and if the attacker could only get control of the authentication packet he could bypass the authentication process completely and could easily program the PLCs. Furthermore, this packet could be used over and over. ICS-CERT team had send the password issue to Siemens and the following versions were updated to fix the error however most of the industrial controllers are using the previous version thus the loop hole is still present.

In addition to this security team at SOPHOS has announced that Stuxnet root kit exploits windows zero-day vulnerability to auto play and auto run itself from a USB even if the pc is fully patched.

Cyber Attack Trends

In order to effectively assess and manage system vulnerabilities the IT managers need to be updated on the current trends of the cyber attackers. Several reports have been published with different perspectives. A recent report on the cyber security trends showed that most attacks were targeted towards the web applications or websites, that being most prone for vulnerabilities. The other common targets were CGI scripts and IIS servers both have a history of vulnerabilities and breach. Mostly the middleware was found with vulnerabilities attracting intruders. The report also reported that most of the attacks detected by IDS were low risk (57%) such as scans and harmless intrusion, 39% attacks were medium risk level and only 4% were high risk attacks. The assessment and monitoring should be focused to detect requests from attacks.

According to the report prepared by the ICS-CERT every sector of industry is a target for cyber attack, Stuxnet’s advent has proven that the target of the cyber war is the critical infrastructure of any country regardless of the industry. The main aim of the attackers is to prove their level of skill and abilities as they managed to enter a highly secured nuclear facility and were successful to command and damage the centrifuges, an act that was impossible to perform by a person. The industry wise cyber attack data provided by the DHS cyber security cell indicates that there were approx 198 reported cyber attack incidents against critical infrastructure in 2012 while that in year 2011 were 130. The most vulnerable sector was energy facing 41% of incidence and the next was water accounted for 15% incidences. The data from DHS suggests that the attackers were very focused on where

to attack. This implies to the fact that more focus is needed by the IT managers in ensuring the presence of appropriate defense system and strategy for controlling the access to the infrastructure. As the figure 2 also shows that loose policies of access control, authentication and authorization and improper configuration all contribute as major vulnerabilities in these systems. A tool often believed to be used by the hackers or intruders is Shodan Computer Search Engine that reveals servers, routers or other machines exposed to the internet. A survey by 2 security specialists along with DHS assessed the devices from critical infrastructures and found that 500, 000 devices from these were exposed to Internet without any proper security measures. These devices belonged to infrastructures such as communication, energy and water utilities using SCADA and also HVAC systems, traffic control systems and building automation control systems. This data also shows that the organizations or the plants are at the risk of losing their operational capabilities if attacked by such worms. The attack on the nuclear facility proves that the worm is capable of operating plant’s machinery which if operated abnormally could be a threat to the human life and could result in damages comparable to a bomb attack.

Conclusion

The above description shows the extent of damage that can be caused by Stuxnet worm or its later version or likes. The previous experience of the worm suggests that the IT managers and related authorities of cyber security need to be very proactive in designing and implementation the security and defensive strategies against any attackers. The infrastructure and systems of any organization today are vulnerable to cyber attackers due to the need of

increased interconnectivity, automation and complexity. Therefore to serve better, the IT managers have the added responsibilities to perform thorough and continual vulnerability checks especially for the components with interface with internet or the user terminals. Since the risks associated with these worms against the critical infrastructures are too high to be neglected the provisions need to be extra vigilant as well. Unlike the security breaches of the past where the worms or viruses attacked for information the next breed of cyber attackers are focused to destroy and malfunction the entire system. The risks associated with these damages can be matter of irreversible damages for the organization as well as for the country.

Resources

Benson, P. (2010, November 18). Computer virus Stuxnet a 'game changer,' DHS official tells Senate. Retrieved from CNN. com: http://edition. cnn. com/2010/TECH/web/11/17/stuxnet. virus/index. html

Geoff McDonald, L. O. (2013). Stuxnet 0. 5: The Missing Link. Symantec Corporation.

ICS-CERT. (2012). ICS-CERT Monitor. INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM- DHS.

New Scientist. (2011). Thanks, Stuxnet. New Scientist Vol. 210 Issue 2806.

NRI SecureTechnologies. (2012). Cyber Security Trends-Annual Review 2012. NRI SecureTechnologies.

OFFICE OF INSPECTOR GENERAL , DHS. (2012). DHS Can Strengthen Its International Cybersecurity Programs. OFFICE OF INSPECTOR GENERAL , DHS.

Paganini, P. (2013, February). SCADA & Security of Critical Infrastructures0.

Retrieved from InfoSec Institure Resources: http://resources. infosecinstitute. com/scada-security-of-critical-infrastructures/

SOPHOS. (2012, July). Zero-Day vulnerability allows USB malware to run automatically, Sophos reports. Retrieved from SOPHOS: http://www. sophos. com/en-us/press-office/press-releases/2010/07/stuxnet. aspx

Zetter, K. (2011, August). Serious security holes found in Siemens control systems targeted by Stuxnet. Retrieved from arsTechnica: http://arstechnica. com/security/2011/08/serious-security-holes-found-in-siemens-control-systems-targeted-by-stuxnet/