International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 12, ISSN No. 2455-2143, Pages 93-96
Published Online October-November 2016 in IJEAST (http://www.ijeast.com)

CYBER ATTACKS: OPERATION AND PREVENTION

Pankit Arora
Department of IT
Amity University, Noida,
Uttar Pradesh, India

Akshath Dhar
Department of IT
Amity University, Noida,
Uttar Pradesh, India

Abstract— **Flame, Stuxnet and Duqu which are very harmful and have made much loss to the computer network, economy etc.**
Flame-It is also known as sky wiper or flamer. It was discovered in 2012. It is a malware that attacks on computers operating on Microsoft windows. It was used for cyber espionage in Middle Eastern countries. It is the most sophisticated malware.
Stuxnet -it was discovered in June, 2010. A computer worm designed to attack PLCs (Programmable Logic Controllers) which allows the automation of processes used to control machinery used on amusement rides- factories or centrifuges for nuclear material. It has destroyed almost one-fifth nuclear centrifuges of Iran. It was created by Israeli agencies and United States to attack Iran's nuclear facilities. Symantec noted in August 2010 that 60% of the infected computers worldwide were in Iran.
Duqu- It was discovered on 1 September 2011, a collection of computer malware. It was thought to be related to stuxnet worm. The name Duqu was derived Cryptography and system security laboratory of Budapest University of technology and economics in Hungary analyzed the malware, discovered the threat and wrote a report.

Keywords— **Cyber Attacks, Flame, Stuxnet, Duqu**

I. INTRODUCTION

Cyber-attack can be defined as a malicious computer code or any other act made to change, exploit, deny, or destroy useful data and information residing in computers and networks.
The purpose of cyber-attack is to destroy the integrity of the data and also to steal the information. Cyber-attack can be for example installing a spyware to destroy the infrastructure of the system. It is done by hacking. In different context, these can be termed as cyber terrorism or cyber warfare.
Cyber warfare is basically motivated hacking done to conduct espionage and sabotage. Espionage (spying) is to gather confidential, secret information without the knowledge of the owner. Sabotage means aim to weaken a polity by destruction, obstruction. The saboteurs try to hide their identity because of the results of their action.

Cyber terrorism in simple words is using internet in terrorist activities such as using viruses for disruption of computer systems on a large scale.

Factors for cyber-attacks:

- Fear factor- it is the most common factor in which one creates fear among the individual or organization.
- Vulnerability factor-an organization can be easily vulnerable to DOS (denial of service)
- Spectacular factor- actual damage of the attack

There are no. of methods to use in cyber-attack and many ways to implement them. They are classified into two types:

- Syntactic attack- includes worms, viruses and Trojan horses. They are straight forward and are malicious software.
  - Worms: they do not need any host to copy itself. They use protocols to replicate over network.
  - Viruses: they are self-replicating. They change their digital signatures each time they reproduce.
  - Trojan horses: they can be the medium of many viruses and worms installing onto the computer. They take entry through backdoor.
- Semantic attack- it manipulate human users perception of computer generated data to obtain valuable information such as passwords, details etc.

<u>Effects of cyber attacks</u>
Infrastructure as a main target
Energy resources, control systems, transportations, telecommunications, finance, water facilities are critical infrastructure targets.

- Energy resources- energy can be divided into two parts, electricity and natural gas. Electricity is used to power machines which we use in our daily life and is also known as electric grids. Take an example of U.S cyber terrorists, in a conflict can access data through system status that shows the main power flows throughout the systems. They can point out the

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 12, ISSN No. 2455-2143, Pages 93-96
Published Online October-November 2016 in IJEAST (http://www.ijeast.com)

busiest sections of the grid. They can cause confusion, backlog, and mass hysteria by shutting down the grids. Foreign attackers with no prior knowledge of system can attack with highest accuracy and without any drawbacks, this can be utilized as a major advantage when cyber-attacks are being made.

- Cyber-attacks on installations of natural gas go much the same way as electric grids. Cyber terrorists can shutdown these installations by rerouting the flow of gas to another area or by stopping the flow. The similar kind of case happened in Russia.
- Control systems- in today's world, many valves and gates are now controlled by computers. Control systems are designed as remote devices that connect with other devices through internet access. Cyber terrorists or hackers gain securities while dealing with these vulnerabilities.
- Transportations- cyber target flight software, target railroads by disrupting switches and also target road usage to impede more transportation problems.
- Telecommunications- due to endless speed and storage capacity, everything is on internet. The basic idea behind these cyber-attacks is to cut off communication between one another and this way to impede information. A nation can plan strikes and better counter attack measures against enemies by controlling flow of communication and information.
- Finance- cyber terrorists reroute huge money transactions and steal money. This would lead the civilians without the job and the industry would collapse.
- Water- Water could be one of the most critical infrastructures to be attacked. Most of the water infrastructure are well developed making it difficult for the cyber terrorists to cause any damage.

Flame- It is otherwise called sky wiper or flamer. It was uncovered in 2012. It is a malware that assaults on workstations working on Microsoft windows. It was utilized for digital undercover work as a part of Middle Eastern nations. It is the most modern malware.

Flame does not focus on a specific industry rather a complete toolbox which was intended for digital undercover work. It spread through framework over LAN or by means of USB stick. It can record screenshots, sound, system movement, Skype discussion

Stuxnet- it was found in June, 2010. A workstation worm intended to assault Plcs (Programmable Logic Controllers) which permits the mechanization of techniques used to control hardware utilized on beguilement rides, processing plants or axes for atomic material. It has annihilated just about one-fifth atomic rotators of Iran. It was made by Israeli orgs and United States to assault Iran's atomic offices. Symantec noted in August 2010 that 60% of the contaminated workstations worldwide were in Iran. The worm was initially recognized by security organization Virusblokada in June 2010.

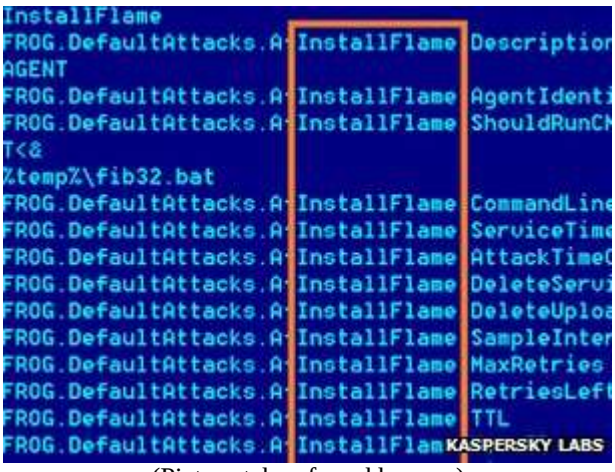
It was discovered on 1 September 2011, a collection of computer malware. It was thought to be related to stuxnet worm. The name Duqu was derived Cryptography and system security laboratory of Budapest University of technology and economics in Hungary analyzed the malware, discovered the threat and wrote a report.

II. METHODOLOGY

Flame- It is otherwise called sky wiper or flamer. It was uncovered in 2012. It is a malware that assaults on workstations working on Microsoft windows. It was utilized for digital undercover work as a part of Middle Eastern nations. It is the most modern malware.

Flame does not focus on a specific industry rather a complete toolbox which was intended for digital undercover work. It spread through framework over LAN or by means of USB stick. It can record screenshots, sound, system movement, Skype discussion

It is part of the way composed in Lua scripting dialect with aggregated C++ code joined in and permits other assault modules to be stacked after starting contamination. It utilizes five distinctive encryption routines and a Sqlite database to store data. The malware modules don't show up in a posting of the modules stacked into a methodology and malware memory pages are ensured with READ, WRITE and EXECUTE authorizations that make them blocked off by client mode applications. It establishes that what antivirus programming is introduced and alter its conduct like by transforming its filename augmentations to diminish the likelihood of recognition. Fire is not intended to deactivate consequently, however backs a "murder" work that makes it take out all hints of its records and operation from a framework on receipt of a module from its controllers.



(Picture taken from bbc.com)

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 12, ISSN No. 2455-2143, Pages 93-96
Published Online October-November 2016 in IJEAST (http://www.ijeast.com)

The latest versions of Kaspersky Lab's business and consumer anti-malware products detect and cure all known variants of Flame, categorized as Worm.Win32.Flame.

Stuxnet-

It was discovered in June, 2010. A computer worm designed to attack PLCs (Programmable Logic Controllers) which allows the automation of processes used to control machinery used on amusement rides, factories or centrifuges for nuclear material. It has destroyed almost one-fifth nuclear centrifuges of Iran. It was created by Israeli agencies and United States to attack Iran's nuclear facilities. Symantec noted in August 2010 that 60% of the infected computers worldwide were in Iran. The worm was first identified by security company VirusBlokAda in June 2010.

Study shows the Spread of Stuxnet:

Country	Infected computers
Iran	**58.85%**
Indonesia	**18.22%**
India	**8.31%**
Azerbaijan	**2.57%**
United States	**1.56%**
Pakistan	**1.28%**
Others	**9.2%**

Stuxnet abuses numerous zero-days vulnerabilities, adjusts framework libraries, assaults Step7 establishments (Siemens' SCADA control programming) and running a RPC server, to introducing marked drivers on Windows working frameworks. It spreads promptly

•via USB blaze drives- The Plcs are joined with workstations that control and screen them, and are associated with the Internet. Along these lines, Stuxnet needs some other approach to achieve those machines, thus it is fit for engendering by means of USB glimmer drives.

•via Wincc- it scans for workstations running Siemens Wincc, an interface to their SCADA frameworks. It associate utilizing a secret word hardcoded into Wincc, and assaults its database utilizing SQL charges to transfer and begin a duplicate of itself on the Wincc machine.

•via system offers it utilizes Windows imparted envelopes to spread itself over a nearby system.

•via Step7 Projects- it contaminates Siemens SIMATIC Step7 mechanical control ventures that are opened on a tainted machine by adjusting Dlls (Windows Dynamic Link library; a library of imparted items: code, information, and assets)

Duqu-

It was discovered on 1 September 2011, a collection of computer malware. It was thought to be related to stuxnet worm. The name Duqu was derived Cryptography and system security laboratory of Budapest University of technology and economics in Hungary analyzed the malware, discovered the threat and wrote a report.

The term Duqu has been used in no. of ways:

- Duqu flaw is used in malicious files to execute malware components of Duqu. It is found in Microsoft windows. Currently one flaw is known, a TTF related problem in win32k.sys.
- The process of using Duqu for unknown goals is operation Duqu.

The variety of software components that together provide services to the attackers is Duqu malware. Some part of this malware is written in unknown programming language dubbed "Duqu framework". Evidence suggests that Duqu may have been written in Object Oriented C (OO C) and compiled in Microsoft Visual Studio 2008.

It searches for data valuable in assaulting mechanical control frameworks. Nonetheless, in view of the secluded structure of Duqu, exceptional payload could be utilized to assault any sort of machine frameworks by any methods and hence digital physical assaults focused around Duqu may be conceivable. Be that as it may, use on PC frameworks has been found to erase all late data entered on the framework, and in a few cases complete erasure of the machine's hard drive.

Much the same as stuxnet, Duqu additionally assaults Microsoft windows utilizing zero day powerlessness. The principal known installer (AKA dropper) document recuperated and uncovered by Crysys Lab utilizes a Microsoft Word (.doc) that endeavors the Win32k Truetype text style parsing motor and permits execution.

III. OBSERVATION AND CONCLUSION

Preventive measures:

- By using strong passwords.
- By securing your computer by activating firewall, using anti-virus or malware software and by blocking spyware attacks (install and update anti-spyware software)
- By securing and making your social network profiles private. Once it is on internet, it is there forever.
- By securing your mobile devices
- By protecting your data
- By securing your wireless networks by reviewing and modifying the default settings.
- By protecting your e-identity
- Avoid being scammed (one should always think before when clicking on any link or file of unknown origin)

V. REFERENCE

[1] National White Collar Crime Center. "IC3 2003 Internet Fraud Report." Retrieved 01 29, 2011, from Scribd:http://www.ic3.gov/media/annualreport/2003_IC3Report.pdf

[2] Coale, John C. "Fighting cybercrime." Military Review 78.2 (1998): 77. Academic Search Premier. EBSCO. Web. 18 Jan. 2011.

[3] Bureau of Justice Statistics. Retrieved 02 04, 2011, from BJS:http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=41

[4] http://us.norton.com/cybercrime/index.jsp

[5] Richardson, R. 2003 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2003.

[6] Wikipedia: http://en.wikipedia.org/wiki/Cyber-attack

[7] http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet