Cyber Security: SEC_RITY is not complete without U!

B.TECH. Computer Science, 3rd year, G.L Bajaj Institute of Technology & Management, Greaternoida (U.P.)

Email:Sunnyvales789@gmail.com

ABSTRACT-

With the explosion of the public Internet and e-commerce, computer networks, if not adequately secured are increasingly vulnerable to damaging attacks. So to protect this we need Cyber Security. Scope of Cyber Security is same around the world. State departments responsible for IT SEC and Cyber Security on national level (such as Indian CSIRT under the Ministry of Communications and Information Technology).So Basically the purpose of Cyber Security is to Protect networks, computers, programs and data from attack, damage or unauthorized access. So our main aim is to find the vulnerabilities in networks and troubleshoot them.

Index terms-History,Security,Vulnerablity,Attacks,Malwares..

What is Malware-

It is a"malicious software": virus, trojan, spyware, etc.

History of Malware-

The beginnings of Malware can be traced as far back as 1949 when John von Nuemann wrote an article on his "Theory of self-reproducing automata." This article was based on a lecture he gave earlier that year in the University of Illinois titled: "Theory and Organization of Complicated Automata." In his article we can see the concepts and beginnings of what Malware would become. Around 1962, some researchers from Bell Telephone Labs created a game that destroys software programs, although it wasn't used for malicious purposes, it was still potentially harmful to a computer. However, it wasn't until 1971 when the first true, self replicating malware was created at BBN Technologies by Bob Thomas. It was called "The Creeper." It was an experimental, selfreplicating program to infect DEC PDP-10 computers running the TENEX OS. Using ARPANET, it was able to spread and once it infected your system, the message "I'm the creeper, catch me if you can!" would be displayed. They later had to create a program called "The Reaper" to delete The Creeper. But it wasn't until 1982 when Richard Skrenta became responsible for the first large-scale virus outbreak in history. He wrote the program named "Elk Cloner" for the Apple II system, which was the predominant PC at the time, and after the 50th boot, it would display a poem that he wrote. The year after, 1983, Frederick Cohen coined the term 'virus' to describe a self-replicating computer program. This term was a suggestion by his teacher Leonard Adleman because you could describe the operation of a "virus" as an "infection." We can see that most of these viruses or malware were created as practical jokes, things that would scare the average user into thinking they may lose their information or worse, their computer. Richard Skrenta was actually infamous for this with his friends; before creating the Elk Cloner, he would scare them by making weird messages come up whenever they used a floppy drive he lent them. But as more vital information began to get stored on personal computers, people realized these viruses could be used for malicious purposes. Trojans and worms that can steal information or monitor what you type began appearing as early as 2001. However, the first well known Trojan was the Zues Trojan, which was created around 2007. It became well known for targeting Windows-based PCs to steal banking information using key logging and it was able to compromise over 74,000 accounts on different websites.

Technical Examples of Malware-

1-**GameOver Zeus**

It is a sophisticated evolution of the ZeuS malware that cybercriminals created to steal usernames and passwords from users on infected system

GameOver Zeus, or GOZ, initially spread via a malicious spam and phishing campaign that sent out e-mails appearing to come from reputable organizations such as the Federal Reserve Bank, the Federal Deposit Insurance Corporation (FDIC) and the National Automated Clearing House Association (NACHA).

A link in these e-mails, if clicked upon, would open a fraudulent website where the GOZ malware would then be downloaded and run on the system, subsequently opening the infected computer for financial information and login credentials to be obtained.

ZeuS variants have been used for stealing banking credentials and financial fraud.

“To keep your financial information safe (from Zeus, and from other malware designed to steal your money), just follow these simple rules:

- Don’t click on links you receive from unknown senders (by emails or in social media networks).
- Don’t download, open and keep unknown files on your device.
- Don’t use open unsecured (public) Wi-Fi networks for any transactions. Use openVPN traffic encryption.
- Always double-check the webpage before entering any of your credentials or confidential information – phishing sites are deliberately designed to look authentic.
- Work only with websites with the ‘https’ prefix; they are more secure than those with ‘http’.
- Make sure you have up-to-date anti-malware protection installed.
- If you don’t currently have any Security Software installed you can download it from our online store.

2-**Deserf Malware-**

You would be wise not to visit Japanese websites at present as security researchers from Symantec discovered a persistent spear phishing attack perpetrated by a group of hackers calling themselves Tick. Another malware called Daserf, is used to gather information. Tick set out by sending spear-phishing emails that contain harmful links and attachments intended to expand the number of its victims. The group is also said to employ a variety of tools designed to spy on the network of a victim organization and expand its access through privilege escalation tactics

Once installed in a machine, the malware would create an install directory where the hackers would deploy several hacktools like Mimikatz, GSecdump, and Windows Credential Editor to escalate their privilege deeper into the network. Based on the results of a forensics investigation conducted by Symantec, the attackers have managed to steal crucial data in the form of PowerPoint presentations from various organizations in Japan.

3-**Dogspectus(Mobile Malware)-**

Dogspectus is a new malware designed for Android devices. It serves itself in an Android device through a Javascript or malicious advertisements published on several porn websites. Unlike other Ransomware, it doesn’t encrypts any data but simply locks the phone and demands ransom. The victim is deprived of all access over his phone, except of paying ransom.

Usually it ask for ransom in the form of two $100 Apple iTunes gift card codes. This mode of payment sounds unusual for Ransomware, since so far it has been using untraceable mediums. However, using iTunes gift card codes is traceable and can help suspect the criminal. With Apple’s assistance, card code user can easily be traced which may help in further investigation.

Dogspectus is the only android Ransomware that outbreaks without user interactivity. It gets installed silently in the device without any prior notice. Android devices that are still operating under 4.x versions and use in-built browser apps are the hit point of Dogspectus. Another cause of inviting this Ransomware is through certain porn websites, containing malicious advertisements.

ATTENTION! YOUR DEVICE HAS BEEN LOCKED REASONS INDICATED BELOW.

Remaining time to pay a fine

71:29:34

Otherwise the case file will be transferred to the

All actions are illegal, are fixed. History query stored in the database of the U.S. Department of Homeland Security

Offender Information

Excerpt from the database of the Department #173-17214

Name: [redacted]

IP: [redacted]

Country: United States

4- **GozNymonly –**

The banking malware GozNymonly a few weeks after the hybrid Trojan was discovered, it has reportedly spread into Europe and begun plaguing banking customers in Poland with redirection attacks. The malware has started targeting corporate, SMB, investment banking and consumer accounts at banks, including some in Portugal and the U.S., in addition to Poland, according to researchers at IBM's X-Force team.

In the attacks, bank customers are redirected to a replica of their bank's actual page and tricked into giving up sensitive information such as credentials and authentication codes. With GozNym, attackers dupe users by showing them the actual bank's URL and SSL certificate. An overlay mask, facilitated by a Moscow-based server, covers the page, hiding any malicious content on the phishing page, something that makes it look normal to users and researchers alike.

Trends in Malware-

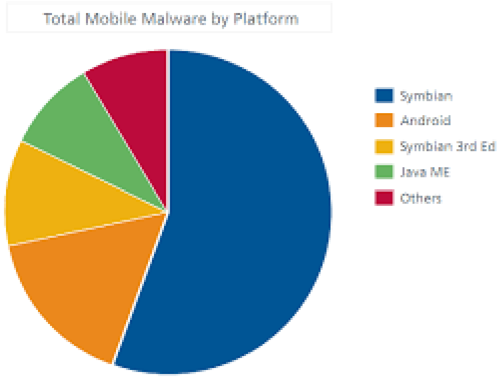
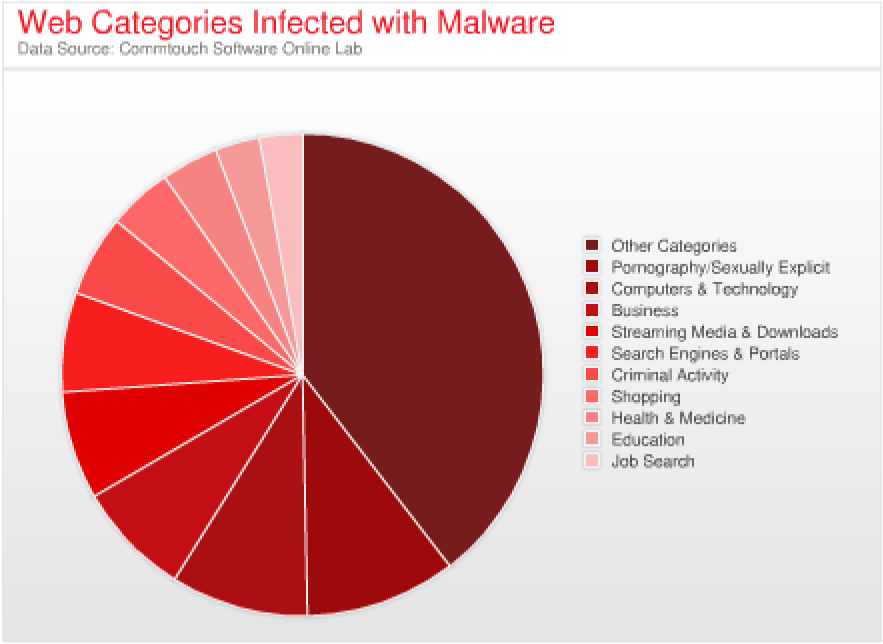


Fig1.Mobile malware



Web Categories Infected with Malware

Data Source: Commtouch Software Online Lab

Conclusion-

No organization can do without antivirus and anti-spyware software. New threats are emerging all the time, so you should always download up-to-date definitions from your software provider. While nothing is a guarantee against infection, antivirus and anti-spyware software can go a long way towards helping protect your organization.

Finally, using antivirus and anti-spyware software is only part of a comprehensive security plan. The additional resources listed below can help you dig deeper.

Reference-

http://www.webopedia.com/TERM/G/gameover-zeus.html

http://www.techwalls.com/hackers-targeted-japanese-websites-with-spear-phishing/?utm_source=hs_email&utm_medium=email&utm_content=29125765&_hsenc=p2ANqtz--J6hE-4xe2k2ellZxLVkV1du0MA2u2BckWuUiQERL5R3h4ENJbsWjhKjuYnXjIa0siOB-cbIfjvjAv2iKFvvCkLdB_pw&_hsmi=29125765

http://blogs.systweak.com/2016/04/dogsepects-android-ransomware-infect-old-android-devices/?utm_source=hs_email&utm_medium=email&utm_content=29120439&_hsenc=p2ANqtz-9EuXzkO0fI76imnYzXkyOhrazWFFBwIFFqh9mfMOT-vNpd-rjdLhLqjHgtqSv7pZ4o7E83DWqQ2g31Oeo-Pp58r2PrSw&_hsmi=29120439

https://threatpost.com/attackers-behind-goznym-trojan-set-sights-on-europe/117647/?m=xla&utm_source=hs_email&utm_medium=email&utm_content=28901903&_hsenc=p2ANqtz-9FBa8q-m4Zr8VZTQri8HNTwZ-OAwpAFPIq_Hw5Q-3YiDsMmXe0Gixeay4BqybSdiFf-iyOVe6bxQqxsoRLwN0wSnQJgA&_hsmi=28901903