A Disquisition of Cyber-Crime

Niyati Parikh
Student
Department of Computer Engineering
Indus Institute of Technology & Engineering, Indus University, Ahmedabad, India

Deep Patel
Student
Department of Computer Engineering
Indus Institute of Technology & Engineering, Indus University, Ahmedabad, India

Roshni Patel
Assistant Professor
Department of Computer Engineering
Indus Institute of Technology & Engineering, Indus University, Ahmedabad, India

Abstract

The Internet is developing dangerously, as is the number of crimes committed against or utilizing computers. Hence, there arises the need for Cyber security. Cyber security is one of the most important parts in the field of information technology. As we think about Cyber security, first thing which comes to our minds is the increasing number of cyber-crimes. Governments around the world are taking steps to prevent these cyber-crimes. This paper focuses mainly on the problems and obstacles created by cyber-crimes. It also points out the ongoing trends about cyber security.

Keywords: Cybercrime, Ransomware, DDOS, Computer Vandalism, Cybercrime prevention, Malware

I. INTRODUCTION

As we have seen in the previous years, there has been an increase in the number and variety of cyber-attacks, ranging from low-to-high profile DDoS attacks, Data Breaching in small and big organizations, use of Targeted Phishing to trick employees of an organization, etc., resulting in significant losses of people's personal information. Considering such attacks of the previous year i.e. 2016, we have a few such examples suggesting the same, for example, the alleged hacking of party officials during the US Election; high-profile DDoS attacks using hijacked Internet-facing security cameras, etc.

II. PRESENT-DAY SCENARIO

Earlier, cybercrime was perpetrated for the individuals or small groups. Nowadays, it is noticed that there is exceedingly intricate cybercriminal systems unite people at worldwide level progressively to carry out wrongdoings.

Today, criminals that enjoy cybercrimes are not inspired by sense of self or aptitude. Rather, they need to utilize their insight to pick up benefits quickly. They are utilizing their capacity to cut, hoodwink and misuse individuals as they think that it's simple to create cash without doing a legitimate work. Cybercrimes have turned out to be significant risk today. Lets us consider following instances.

1) Botnets remain an extremely popular tool among cybercriminals nowadays. Since the Mirai botnet was released to the planet, several variations have popped up in its wake. A fresh variant of the particular botnet malware has been uncovered, which is with the capacity of performing 54-hour DDoS episodes. It would go to show the original Mirai botnet malware was simply a sign of what to come, as the problem will only worsen from here on away.
2) Misuse of the Web's intrinsically unreliable framework. All Web clients depend on old foundational conventions, and their omnipresence makes them about difficult to patch up or supplant. These bygone conventions that have for some time been the foundation of the Web and business systems are now and then shockingly flaky. For instance, assaults against BGP (Outskirt Passage Protocol) could possibly disturb, commandeer, or incapacitate a significant part of the Web. What's more, the DDoS assault on Dynin October (propelled by a bunch of IoT gadgets), brought down the DNS supplier and, alongside it, access to some portion of the web. It was one of the biggest strikes seen and those guaranteeing obligation said that it was only a dry run. Vast scale ISPs and endeavors can find a way to react, however these may well neglect to avert genuine harm if people or states abuse the Web's most profound security defects.
3) More attacks utilizing worked in administrator languages and devices. We see more exploits based on PowerShell, Microsoft's language for automating administrative tasks. As a scripting language, PowerShell sidesteps countermeasures concentrated on executables. We likewise observe more attacks utilizing penetration testing and other administrative apparatuses that may as of now exist on the system, need not be infiltrated, and may not be suspected. These intense tools require similarly solid controls.

In the present day environment, since most data processing relies on upon the use of information technology, the control, prevention and examination of cyber activities is the key to the success of the Organizations, Government's agencies and individuals. The procurement and maintenance of exceptionally skill cybercrime expert by Government and Business Endeavors can't be exaggerated.

Cybercrime essentially characterized as any criminal action that happens over the Internet. There are numerous illustrations, for example, misrepresentation, malware such as viruses, data fraud and cyber stalking.

III. Cybercrime Types

Let us access few of the most common forms of cyber-attacks that we should be alert against & protect our business from in the coming future.

A. *Ransomware:*

Ransomware is a relatively new sort of malware which prevents or limits users from utilizing their system. Ransomware assaults are principally done for money – it's called Ransomware in light of the fact that it viably holds your PC hostage until you pay the assailant a specific measure of money. You usually have to make the payment through a specific online platform and within a certain period of time. When you make the payment, you are again allowed to utilize your own system or to recover your data.

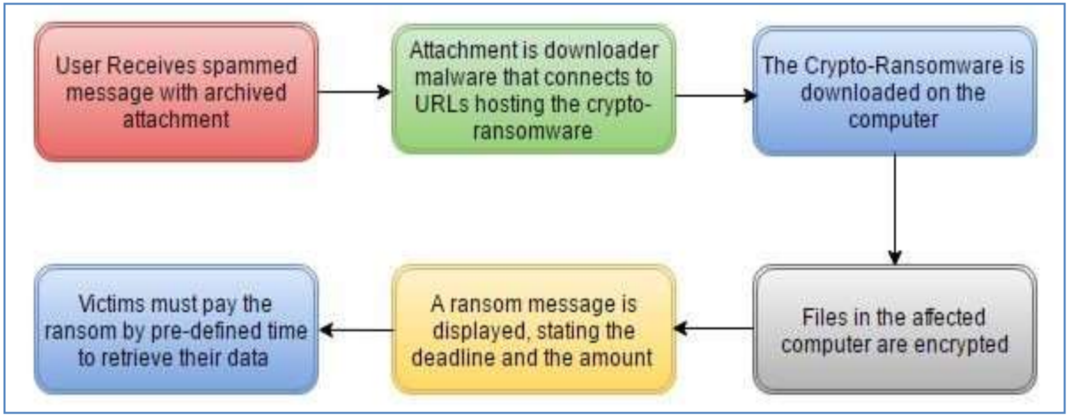
User Receives spammed message with archived attachment
Attachment is downloader malware that connects to URLs hosting the crypto-ransomware
The Crypto-Ransomware is downloaded on the computer
Files in the affected computer are encrypted
A ransom message is displayed, stating the deadline and the amount
Victims must pay the ransom by pre-defined time to retrieve their data

Fig 3.1: How Ransomware takes place

SMEs (as well as big enterprises) are increasingly frequently getting specifically targeted by Ransomware sort malware, including as Cryptolocker, CoinVault or CTB-Locker. There are a few ways it can contaminate your system. Most commonly it can be downloaded by users, ordinarily through visiting a compromised site. Ransomware can likewise be downloaded in conjunction with another file – either dropped into your system by another malware or sent as an attachment in a spam email for example.

B. *Denial-of-Service Attacks:*

Denial-of-service attacks give criminals another way to target individual organizations. By overloading critical systems, such as websites or email, with Internet traffic as a method for blocking access, denial-of-service attacks can wreak financial havoc and disturb typical operations.

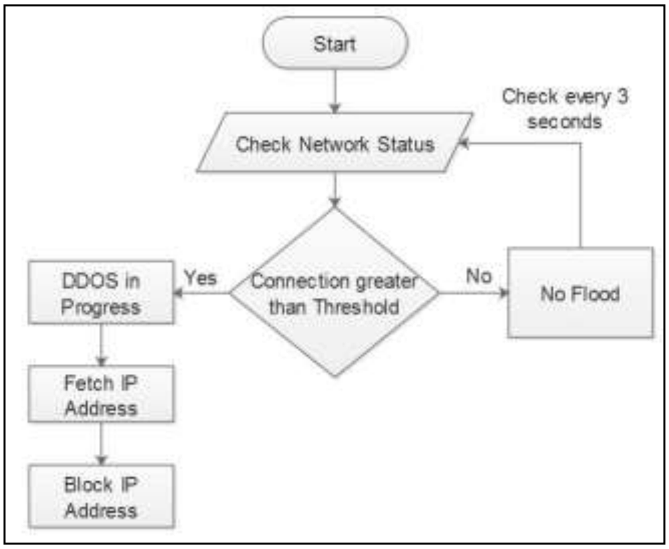

Fig. 3.2: How DDoS Attacker Works

In 2017, we will see an expansion in the utilization of DDoS assaults being utilized as a smokescreen to distract IT groups while different attacks penetrate systems to take sensitive information (otherwise known as Ransomware). My prediction is that ransom demands associated with DDoS attacks will increase exponentially in 2017, fuelled by the increased automation of DDoS attacks and the ability to buy them off the shelf. The ‘Lizard Squad’ is one example of a group of hackers who sell DDoS attacks-as-a-service for as little as $6 a month.

To protect themselves, organizations ought to convey a blend of on-premises and cloud-based solutions to handle assaults of differing sorts and sizes – adequately a multi-layered network security approach.

C. *Mobile Malware:*

One of the key contributors of the risk from mobile malware is the proliferation of applications that conduct real business utilizing access-sensitive and secret information. Commonplace users may have managing an account, Visa, hotel, carrier and corporate applications installed on their cell phones. These get to is secured, at any rate, with username and password controls.

Cybercriminals are reasonable actors; they follow the money. They are turning their concentration and consideration regarding the mobile stage because of the growth in mobile devices coupled with the opportunity to collect an abundance of data from every device. Not at all like work desktops and laptops, which typically contain simply work related data, mobile phones frequently consolidate work and individual information and applications.

D. *Computer Vandalism:*

It is a type of cybercrime that Damages or destroys data rather than stealing. It transmits virus.

1) *Cyber Terrorism:*

It is a utilization of Internet based assaults in terrorist activities. Technology astute terrorists are using 512-bit encryption, which is difficult to decrypt.

2) *Software Piracy:*

It is a burglary of software through the unlawful duplicating of genuine programs. Distribution of products intended to pass for the original. On the off chance that a person with a single user permit loads the product onto a companion's machine, or if an organization loads a software package onto every representative's machine without purchasing a site license, then both the single user and the organization have broken the terms of the software license agreement and are in this way blameworthy of software piracy. Software piracy includes the unauthorized use, duplication, distribution, or offer of economically accessible software. Software piracy is frequently marked as soft lifting, duplicating, unauthorized renting, Internet piracy, hard-disk loading and OEM unbundling.

IV. CYBERCRIME PREVENTION

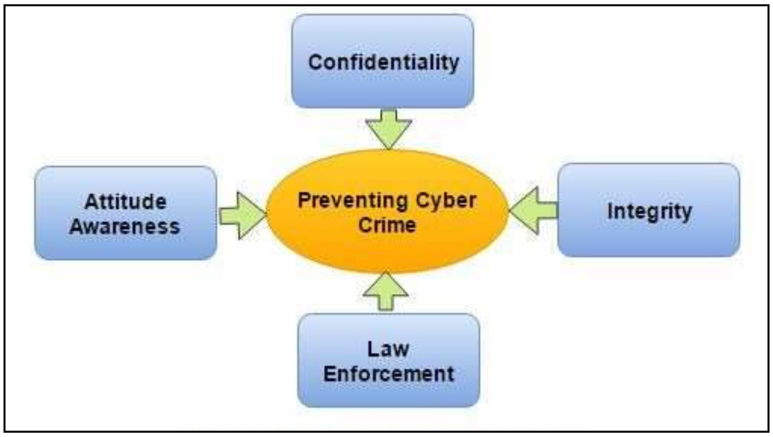

Fig. 4.1: Elements to protect from cyber crime

There are various methods through which a user can prevent oneself from being a victim of cybercrime. Let’s take into consideration few of the vastly recognized methods.

1) Computer users must utilize a FIREWALL to shield their PC from hackers. Most security software has firewall included as default. Enable firewall that comes with the router as well.
2) Computer users are recommended to use anti-virus software in their systems. There are wide range of anti-virus software available in the market from low-to-high price range as well as free anti-virus protection is also offered by software such as AVG for those who don’t want to purchase.
3) It is suggested by digital/cyber experts that users must shop only at secure and trusted web portals. Users must avoid providing bank/card details to the websites that raise suspicions or look strange.

4) Users must use strong password combinations which may include combining the numbers, letters (combination of Uppercase & Lowercase), and special symbols (ex. ! @, #, etc), to protect their accounts. In addition to that, users should keep changing their login credentials on regular intervals.
5) It is recommended to monitor children and how they utilize the Internet. Install parental control software to limit where they can browse the internet.
6) Make sure that social networking profiles are set as private and check their security settings. Be careful what users post on the internet, because once it is uploaded, it is very difficult to remove it from the internet.
7) Secure mobile devices. Most of the time, individuals leave their mobile devices unattended. By activating the in-built security features, they can avoid any access to personal details. Never store passwords, pin numbers and even own addresses on any mobile device.
8) Protect important data from being hacked by cyber criminals. Use encryption for the sensitive files such as financial records and make back-up files regularly to avoid any loss.
9) Do not use public networks (ex. Public Wi-Fi Hotspots) for financial or corporate transactions.

V. Conclusion

To sum things up, Cyber-crime is advancing as a serious threat. A cyber-attack is an attack started from a computer against a site, computer framework or individual computer that jeopardizes the secrecy, integrity or accessibility of the computer or data stored on it. It is major and maybe the most entangled problem in the cyber space. Worldwide governments, police departments and intelligence bureaus have started to respond against cybercrime. Numerous efforts are being made at global level to check cross border cyber threats. Indian police has started special cyber cells across the nation and have begun training groups of people with the goal that they gain knowledge and protect themselves from such crime.

References

[1] Chwan-Hwa (John) Wu and J. David Irwin, Introduction to Computer Networks and Cybersecurity 1st Edition, Taylor & Francis, 04-Feb-2013 Computers - 1336 pages
[2] Cybersecurity for Beginners by Raef Meeuwisse, First printing: 2015, first published by: lcutrain Ltd
[3] Peter W. Singer and Allan Friedman, Cyber security and Cyber War: What Everyone Needs to Know, OUP USA, 2014 - Computers - 224 pages
[4] "The Electronic Attack Threat to Supervisory Control and Data Acquisition (SCADA) Control & Automation Systems", National Infrastructure Security Co-ordination Centre (NISCC), UK, July 12, 2003
[5] Cyber security current and emerging trends for 2017, http://www.oakconsulting.biz/?p=3174
[6] Types and prevention of cyber-crime, Civil service India, Published- May 9, 2016
[7] Sean B. Hoar, Trends in Cybercrime: The Dark Side of the Internet, 20 Crim. Just. 4 (2005-2006)
[8] Roderic Broadhurst and Lennon Y. C. Chang, Cybercrime in Asia: Trends and Challenges, Handbook of Asian Criminology, pp 49-63, Date: 02 November 2012
[9] Chichao Lu, Wenyuan Jen and Weiping Chang, Trends in Computer Crime and Cybercrime Research During the Period 1974-2006: A biometric, Approach Pacific-Asia Workshop on Intelligence and Security Informatics, PAISI 2007: Intelligence and Security Informatics pp 244-250