THE CYBERCRIME

DIFFERENT TYPES OF INTERNET FRAUDS AND CASES

Identity theft

Identity theft and fraud is one of the most common types of cybercrime. The term Identity Theft is used, when a person purports to be some other person, with a view to creating a fraud for financial gains. When this is done online on the Internet, its is called Online Identity Theft. The most common source to steal identity information of others, are data breaches affecting government or federal websites. It can be data breaches of private websites too, that contain important information such as – credit card information, address, email ID's, etc.

In one notorious case of identity theft, the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt him -- saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time -- before filing for bankruptcy, also in the victim's name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused. This case, and others like it, prompted Congress in 1998 to create a new federal offense of identity theft.

Ransomware

This is one of the detestable malware-based attacks. Ransomware enters your computer network and encrypts your files using public-key encryption, and unlike other malware this encryption key remains on the hacker's server. Attacked users are then asked to pay huge ransoms to receive this privzate key.

Hollywood Presbyterian Medical Center, a hospital that was hit by a ransomware attack earlier this 2016. The hospital initially tried to thwart its attacker's demand of 9,000 bitcoins by abandoning their encrypted computers, resorting to the use of paper medical records and registration forms, and communicating with other hospitals via fax. Those pre-digital operations proved unsustainable, and the hospital negotiated with the ransomers, ultimately making a payment of 40 bitcoins (then worth about $17,000) to restore their systems.

DDoS attacks

DDoS attacks are used to make an online service unavailable and bring it down, by bombarding or overwhelming it with traffic from multiple locations and sources. Large networks of infected computers, called Botnets are developed by planting malware on the victim computers. The idea is normally to draw attention to the DDOS attack, and allow the hacker to hack into a system. Extortion and blackmail could be the other motivations.

A gang using distributed denial of service (DDoS) attacks to extort bitcoins since July 2014 ramped up operations despite a bounty of $26,000, according to Arbor Networks.

The gang, calling itself DD4BC (DDoS for Bitcoin), has been rapidly increasing the frequency and scope of its DDoS extortion attempts, shifting from targeting Bitcoin exchanges to online casinos and betting shops and, most recently, prominent financial institutions in the US, Europe, Asia, Australia and New Zealand.

Botnets

Botnets are networks of compromised computers, controlled by remote attackers in order to perform such illicit tasks as sending spam or attacking other computers. Computer Bots can also be used act like malware and carry out malicious tasks. Then can be used to assemble a network of computers and then compromise them.

In December 2015, an international operation involving law enforcement organisations, government cyber security teams and private organisations targeted the Dorkbot botnet. In February, the National Crime Agency (NCA) and other European crime agencies shut down servers used by a botnet targeting personal banking information, while in June, police arrested 130 suspects in connection with cyber fraud at 140 airports around the world in an international law enforcement operation, and in December, EU police agency Europol announced it is to get new powers to step up efforts to fight terrorism, cyber crime and other crime.

Spamming

Spam is basically unwanted emails and messages. They use Spambots. Phishing is a method where cyber criminals offer a bait so that you take it and give out the information they want. The bait can be in form of a business proposal, announcement of a lottery to which you never subscribed, and anything that promises you money for nothing or a small favor. There are online loans companies too, making claims that you can get insecure loans irrespective of your location. Doing business with such claims, you are sure to suffer both financially and mentally. Phishing has its variants too – notably among them are Tabnabbing, Tabjacking. and Vishing and Smishing.

This is the famous Nigerian 419 scam, so-called because it reflects the relevant section of the Criminal Code of Nigeria, and victims of this fraud of been defrauded millions. Only recently a victim of the Nigerian 419 scam was defrauded $2.1 million. You may argue that the person was greedy and knew they were likely breaking the law themselves, and you would have a point. However, the unsolicited spam e-mail was sent with one intent and one intent only, to defraud the recipient of the email out of their savings. Thus it is a criminal act and there should be criminal law to reflect this.

Phishing

Phishing attempts are mostly emails sent by random people whom you did not ever hear of. You should stay away from any such offers especially when you feel that the offer is too good. The US Cybercrime Center says – do not get into any kind of agreements that promise something too good to be true. In most cases, they are fake offers aiming to get your information and to get your money directly or indirectly.

In 2009, Microsoft warned that "several thousand Windows Live Hotmail customers' credentials were exposed on a third-party site due to a likely phishing scheme." The online attack also appears to have affected users of other online e-mail services, including Google Gmail, and Yahoo Mail.

According to the FBI, the U.S.-Egypt phishing operation collected personal information from thousands of victims and used that information to defraud U.S. banks. Hackers based in Egypt allegedly captured banking information and other personal details, then supplied that information to associates in the U.S. who then withdrew funds using the stolen credentials and wired back a portion of the proceeds to Egypt.

Social Engineering

Social engineering is a method where the cyber criminals make a direct contact with you using emails or phones – mostly the latter. They try to gain your confidence and once they succeed at it, they get the information they need. This information can be about you, your money, your company where you work or anything that can be of interest to the cyber criminals.

In 2013, the Twitter account of the Associated Press news wire service reported "Breaking: Two Explosions in the White House and Barack Obama is injured." It was false news. AP's Twitter account had been hijacked by the Syrian Electronic Army, one of a series of attacks on media organizations around that time.

Ferrara puts this on his top five list because of the quick aftermath. "It had an immediate impact," he says. Within moments, the stock market dropped.

The tweet was sent at 1:07 p.m. At 1:08 the Dow started the nosedive. It dropped by 150 points before 1:10, when news began to spread that the tweet was erroneous.

This was yet another attack that started with phishing, and even a security-savvy user might fall for it.

Malvertising

Malvertising is a method whereby users download malicious code by simply clicking at some advertisement on any website that is infected. In most cases, the websites are innocent. It is the cyber criminals who insert malicious advertisements on the websites without the knowledge of the latter. It is the work of advert companies to check out if an advertisement is malicious but given the number of advertisements they have to deal with, the malverts easily pass off as genuine ads.

Malvertising contradicts basic Web safety tips security experts have drilled into our heads – such as “Stay away from ‘sketchy’ Web sites if you don’t want to pick up malware.” This is because mainstream, high-trafficked Web sites today outsource the ad content on their pages to a vast array of third-party ad networks, including household names like Google (DoubleClick) to start-up providers and others well under the radar.

PUPs

PUPs, commonly known as Potentially Unwanted Programs are less harmful but more annoying malware. It installs unwanted software in your system including search agents and toolbars. They include spyware, adware, as well as dialers. Bitcoin miner was one of the most commonly noticed PUPs in 2013.

Drive-By-Downloads

Drive By Downloads too, come close to malvertising. You visit a website and it triggers a download of malicious code to your computer. These computers are then used to aggregate data and to manipulate other computers as well.

The websites may or may not know that they have been compromised. Mostly, the cyber criminals use vulnerable software such as Java and Adobe Flash and Microsoft Silverlight to inject malicious codes as soon as a browser visits the infected website. The user does not even know that there is a download in progress.

Remote Administration Tools

Remote Administration Tools are used to carry out illegal activities. It can be used to control the computer using shell commands, steal files/data, send location of the computer to a remote controlling device and more.

Exploit Kits

A vulnerability means some problem in the coding of a software that enables cyber criminals to gain control of your computer. There are ready to use tools (exploit kits) in the Internet market which people can buy and use it against you. These exploit kits are upgraded just like normal software. Only difference is these are illegal. They are available mostly in hacking forums as well as on the Darknet.

Scams

Notable among Internet scams are, scams which misuse the Microsoft name and other general tech support scams. Scamsters phone computer users randomly and offer to fix their computer for a fee. Every single day, scores of innocent people are trapped by scam artists into Online Tech Support Scams and forced to shell out hundreds of dollars for non-existent computer problems.

Waterhole attacks

If you are a big fan of Discovery or National Geographic channels, you could relate easily with the waterhole attacks. To poison a place, in this case, the hacker hits the most accessible physical point of the victim.

For example, if the source of a river is poisoned, it will hit the entire stretch of animals during summer. In the same way, hackers target the most accessed physical location to attack the victim. That point could be a coffee shop, a cafeteria etc.

Once hackers are aware of your timings, they might create a fake Wi-Fi access point and modify your most visited website to redirect them to you to get your personal information

Fake WAP

Even just for fun, a hacker can use software to fake a wireless access point. This WAP connects to the official public place WAP. Once you get connected the fake WAP, a hacker can access your data, just like in the above case.

Eavesdropping (Passive Attacks)

Unlike other attacks which are active in nature, using a passive attack, a hacker just monitors the computer systems and networks to gain some unwanted information.

The motive behind eavesdropping is not to harm the system but to get some information without being identified.

Rootkit

A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.

Forgery

involves a false document, signature, or other imitation of an object of value used with the intent to deceive another. Those who commit forgery are often charged with the crime of fraud. Documents that can be the object of forgery include contracts, identification cards, and legal certificates.

Vulnerability Scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses.Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented.)

Password Cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.