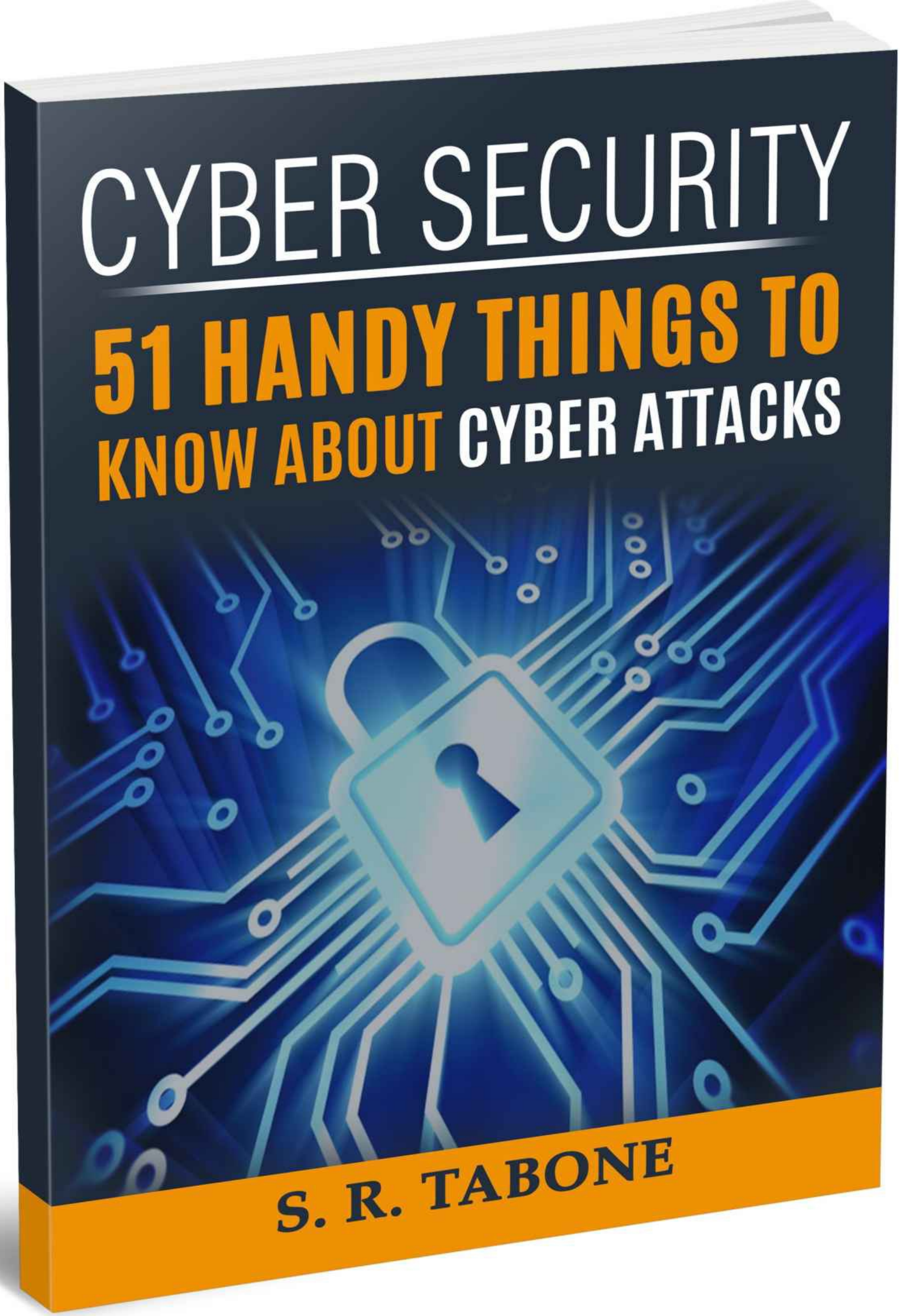

CYBER SECURITY

51 HANDY THINGS TO KNOW ABOUT CYBER ATTACKS

S. R. TABONE

Cyber Security
51 Handy Things
To Know About
Cyber Attacks

First published in Great Britain by R.J.T. Lion Publishing, 2017
This First Edition is published in 2017

ISBN-13: 978-1546841166

ISBN-10: 1546841164

Cyber Security 51 Handy Things To Know About Cyber Attacks

There are handy tips on how to protect your computer/s and what signs to look out for that your information might be under attack. This is the must have book for individuals and businesses.

The Cyber threat landscape is continuously evolving and the motivations behind cyber attacks are changing day by day. Youths are increasingly getting themselves involved in cyber-crimes. All sorts of businesses are under threats from cyber attacks and are unprepared from protecting themselves against such crimes that lead to great stress and financial loses. The process of hacking (that used to be regarded as a coding crime) has drastically changed over the years. In addition to utilizing malware, hackers are increasingly adopting social engineering as a mean of exploiting vulnerabilities. Therefore, it is imperative to learn more about the factors, modes, consequences, and lessons reading cyber attacks. The following 51 brief paragraphs will provide a useful overview regarding the major issues about cyber attacks.

Characteristics of cyber attacks and the history of
The relationship between cyber security and the responsible cyber citizens
Reason for utilizing internet as a mode of launching attacks
Easy availability of hacking tools encouraging cyber-crimes
Infinite scope for initiating cyber attacks: Nothing is safe
The most hacker-active countries in the world
The most well known hacking groups of all time
Important things to know about cyber vulnerability
Common forms of cyber-crimes with brief descriptions
Categorizing cyber-attackers from multiple perspectives
Varieties of cyber attacks and ways to initiate these
Cyber crime scenarios to avoid so as to remain safe
Early symptoms of imminent cyber attacks
Sure signs a system has been compromised
Relatively easy ways utilized by hackers to get access to your data
Relatively less cumbersome ways to prevent most attacks

Ways to reduce risk to websites
Inadequate protection offered by traditional antivirus programs
Ways to remain vigilant and avoid cyber attacks
Malware: Cyber-criminal's ultimate choice
Encryption: Proven way to remain secured
Ransomware: A brief history and timeline
Ransomware classification considering severity and complexity
How to protect yourself from ransomware attacks
Recommended undertakings amidst ransomware attacks
How and why companies pay the ransom
Rationale behind ransomware attacks on public institutions
Ransomware: A weapon of mass economic destruction
Exponential rise in cyber attacks targeting small business enterprises
Proactive defense: Understanding the threat landscape
Tools employed by hacktivists and means of defending against these
Common techniques used by cyber criminals and ways to avoid these
How to deal with insider threat to limit cyber-crime
How to limit sate and corporate sponsored attacks
Use of social engineering as a mode of initiating cyber attacks
Types of threats where human behavior is a cause
Ways of neutralizing the human factor in cyber attacks
Components of contemporary hacking operations
Best operating system for cyber criminals
Methods of tracing the hackers behind cyber attacks
Security measures before cyber attacks: Prevention
Security measures during cyber attacks: Incident management
Security measure after cyber attacks: Consequence management
Online freedom versus fear when cyber security is in question
Likelihood of a widespread smart grid attack and potential catastrophe associated with this
International efforts to contain cyber attacks
Role of punishment in reducing cyber-crime
Law enforcement proved insufficient in tackling cyber-crimes
Prerequisites of a top-notch threat intelligence
Future of cyber-crime and cyber security
National capacity building to combat cyber crime

Cyber Security 51 Handy Things To Know About Cyber Attacks

1. **Characteristics of cyber attacks and the history of**

   Cyber attacks are socially or politically motivated attacks carried out though the spreading of malicious programs, obtaining unauthorized web access, and utilizing various means of misappropriating valuable information. Identity theft, extortion, intellectual property theft, loss of access to devices and information, website defacement are likely consequences of a cyber attack. The first occurrence of a deliberate cyber attack took place in 1988 caused by an internet worm. It temporarily shut down around 10% of the world's internet servers. The latest cyber attack, caused by WannaCry ransomware, has already infected around 200,000 computers in 150 countries.

2. **The relationship between cyber security and the responsible cyber citizen**

A cyber citizen utilizes technology in an appropriate manner in order to protect cyberspace security and upholding the cyberspace etiquette. Everyone should play his or her role for improving the current chaotic state of cyberspace. Through sharing knowledge, knowing relevant rules and regulations, maintaining online privacy, respecting copyright policies, remaining vigilant about malicious activity, and acting intelligently, people can make the internet a better place. Moreover, cyber citizens should not take advantage of online anonymity.

3. Reason for utilizing internet as a mode of launching attacks

At present, the internet environment is dynamic and incorporates new technology on a consistent basis. The breadth of internet networks has experienced an exponential rise over the last decade and the integration of Local Area Network (LAN) and Wide Area Network (WAN) has created a single seamless network. Moreover, this massive interconnectivity lacks central administrative control. Around 50% of the world's population has internet access and 42% of the internet users shop online. Amidst such connectivity, any problem occurred in one part of the world can spread to any part of the world instantly. Besides, the sheer complexity of administering computer network along with the presence of ad hoc collection of Transmission Control Protocol (TCP) or Internet Protocol (IP) makes the internet vulnerable to cyber attacks.

4. Easy availability of hacking tools encouraging cyber-crimes

The amount of technical knowledge required to become a successful cyber-criminal has significantly dropped over the years. Many illegal hacking materials and accessories are readily available on various hacking or gaming forums. The easy availability of off-the-shelf hacking tools (e.g., DDoS and Ransomware) at an affordable cost with step-by-step tutorials can literally enable anyone to compromise a legit website. The aforementioned scenarios have created an enabling environment in which more and more young people are getting involved in cyber-crime.

5. **Infinite scope for initiating cyber attacks: Nothing is safe**

An abrupt blackout, nuclear station malfunction, pipeline explosion, random changes in airline and railway reservation, identity theft, false online transaction and website compromise are the likely outcomes of cyber attacks. Gaming companies, financial corporations, e-business platforms, social media sites and data centers are lucrative targets for hackers. Moreover, cyberspace is widely regarded as the fifth domain of warfare and countries around the world are busy preparing to tackle the problem of information warfare.

6. **The most hacker-active countries in the world**

According to the 2016 Global Threat Intelligence Report published by Internet Solution, 65% of attacks originated from IP addresses within the US and hackers predominately host such attacks locally to circumvent potential geo-location blocking. However, China continues to top the list of hacking active countries and accounts for around 41% of the world's hacking activities. China's leadership in hacking can partly be attributed to the Chinese government's explicit support for cyber security and the hacking competitions organized by Chinese universities. China, the US, Turkey and Russia altogether are responsible for 60% of all attacks.

7. **The most well-known hacking groups of all time**

- Lizard Squad: This group was responsible for hacking Facebook, Malaysian Airline's website, Microsoft Xbox Live and Sony's Playstation Network.
- Anonymous: This group is made up of thousands of hacktivists. Its hacking victims include MasterCard, Visa, PayPal, and New York Stock Exchange website.
- Chaos Computer Club (CCC): This German hacking club, founded in 1981, is one of the oldest and most respected ethical hacking groups. The main objective of this group is to uncover security flaws in major

systems.

- OurMine: This group was accused of hacking social accounts of Mark Zuckerberg and Sundar Pichai. Moreover, it attacked LinkedIn also. Besides conducting cyber attack, this group provides professional security audit service.
- Other notable groups: LulzSec, Syrian Electronic Army, The Level Seven Crew, globalHell, and TeaMp0isoN

8. Important things to know about cyber vulnerability

- Java based programs like Adobe Reader, flash player are available on almost any computer, and these programs are extremely vulnerable to syntactic attacks. Thus, most of the computers are exposed to software vulnerabilities.
- Most of the government agencies around the world are implicitly involved in the development and deployment of malware programs for their espionage operations. Stuxnet is an example of such malware, jointly developed by the US and Israel. Hackers conduct reverse engineering on government malware for creating more advanced malware of their own.

9. Common forms of cyber-crime with brief description

Cyber criminals use different ways to commit attacks. The most common ones are explained below:

- Hacking: Hackers use different tools to get unauthorized access to their victim's computers and networks. Their main purpose is to shut down or misuse the hacked devices.
- Cyber stalking: This is a type of online harassment where the victim is subject to a barrage of offensive online messages.
- Identity theft: In this case, a criminal gets access to victim's bank account, credit card and other financial information. Criminals use this information to steal money and buy things online.
- Child soliciting and abuse: Here, criminals solicit youths via chat rooms for the purpose of child pornography.

10. Categorizing cyber-attackers from multiple perspectives

Cyber attackers can broadly be categorized into insiders and outsiders. Discontented employees, financially motivated insiders and unintentional insiders constitute the former group. Discontented employees can threaten the safety of internal systems for retaliatory purpose whereas financially motivated insiders misuse company assets for personal gain. Unintentional insiders involuntarily divulge proprietary information. Outsiders are also known as organized attackers consisting of terrorists, hacktivists, nation states, and criminal actors.

11. Varieties of cyber attacks and ways to initiate these

Cyber attacks can broadly be categorized into syntactic attacks and semantic attacks. Malicious software, e.g., viruses, worms, and Trojan Horses are used for launching syntactic attacks. Viruses are self-replicating programs and can attach themselves to any file for executing their codes. Worms are self-sustaining programs and capable of replicating themselves over a network using protocols. Moreover, such software exploits known vulnerabilities in the system to perform its operation. In addition to performing its legitimate tasks, Trojan horse carriers out unwanted and unwanted activity to gather additional information about the target anonymously.

A semantic attack is an attack in which the attacker uses the device or network in a way that provides misleading information to the victim and allows the attacker to hide his trace. Semantic attacks are arguably the most vicious attacks and deceive users into divulging information. “Pump and Dump” schemes and phishing are notable examples of semantic attacks. “Pump and Dump” strategies are used for exploiting stock market trading and phishing deceives users to obtain useful information.

12. Cyber crime scenarios to avoid so as to remain safe

- Fall victim to premium service abuser: Getting unrealistic mobile phone bill without any valid reason can be caused by some malicious smartphone apps. Such apps automatically send premium subscription request or covertly make calls and send messages. To avoid this sort of experience, it is recommended to go through the review section of the app download page carefully before downloading.
- Forced to answer surveys to download something: This is an example of a deliberate survey scam, aimed at collecting information such as credit card information, first name, last name etc. To avoid such scams, one should go directly to reliable websites for downloading instead of doing a Google search.
- Too short battery backup: If a smartphone user is experiencing an unusually short battery backup, s/he should uninstall a battery consuming apps to check whether the situation has changed or not. If battery backup is improved, the likelihood of malware attack on that phone becomes apparent.

13. Early symptoms of an imminent cyber attack

Most of the symptoms of a cyber attack seem harmless at first and can easily be attributed to the usage of outdated hardware or infrastructure components. However, correctly recognizing the following trivial signs can allow a user to stop the attack in its track:

- Slow internet connection: Sluggish internet connection can be the first sign of a cyber attack. Denial of Service (DoS) and Distributed Denial of Service (DDoS) often cause such internet connection problem.
- Fake antivirus message: it is usual to get a fake antivirus message on an unprotected PC and such message frequently prompts the user to install an infected yet legitimate looking antivirus.
- Unwanted browser toolbar: If the user notices an unfamiliar browser tool bar that had not been installed by him/her, the respective person should notice whether he automatically is directed to a different site while searching. If so, it may indicate a likely cyber attack.

14. Sure signs of system compromise

- Unusual webcam activity: if the user’s PC webcam light is automatically turned on or off, it is highly likely that Remote Administration Tools (RAT), a popular malware program, has infected the PC.
- Sudden appearance of new programs: if an unknown program frequently gets loaded onto the user’s computer, it is a clear indication of cyber attack.
- Malfunction of utility software: if antivirus program, task manager and/or registry editor are disabled and cannot be restarted, the system is compromised.

15. Relatively easy ways utilized by hackers to get access to user’s data

- Free software download: Downloading what should be paid software for free is illegal and harmful for system security. Such activity opens the gateway for introducing malicious programs into the system. Therefore, unless the intended software is completely free anyway, it is best to purchase it to avoid potential intrusion.
- Cookie theft: Cookies are used for remembering browsing history and login information. Both general and encrypted cookies can easily be stolen by using simple browser add-on. One possible solution to this problem is to browse well-built and secured sites only.
- Use of free Wi-Fi: Using free Wi-Fi connection for banking, online transaction, and social media communication is severely dangerous because most free Wi-Fi connections are unprotected. Anyone with a packet sniffer program can intercept unencrypted data. So, it is recommended to use Virtual Private Network (VPN) connection while using a public Wi-Fi hotspot.

16. Relatively less cumbersome ways to prevent most attacks

- Use different passwords on different sites: The habit of using different passwords for different sites can largely reduce the magnitude of information theft even if one account is compromised. Moreover, it is wise not to use the primary account's password on any other site.

- Ignore pop-ups: Allowing pop-ups often results in downloading malicious programs. Therefore, it is always advisable to avoid pop-up offering like site-survey on e-commerce site.
- Avoid storing account details on websites: Most websites offering storing passwords and other credentials for future use. Following such practice often leads to serious economic loss.

17. Ways to reduce risk to websites

- Use updated version of integrated software: Since older version of an app/widget/plugin may not work properly and can provide quick access points for hackers, website developer should always use current version of integrated software.
- Choose secured hosting companies: To reduce the risk to the website, website owner should only select such web-hosting company that adopts exceptional safety measures and provide latest database and programming language support.
- Use ".htaccess" to deny access: Though using ".htaccess" file, one can easily reduce the likelihood of accessing his login page from unknown IP address. This process is ideal for WordPress or Content Management System (CMS) based websites.

18. Inadequate protection offered by traditional antivirus programs

Since most of the cyber, attacks are well crafted and considerably different from typical threats encountered by web surfers, traditional antivirus programs prove inefficient in providing complete protection. In reality, without adopting an integrated online-offline risk management program, nobody can ensure complete security. Commercially available solutions are available to anyone and hackers can easily crack the security system by deploying ingenious ways. Moreover, modern hackers tend to exploit human psychology rather than program inefficiency by utilizing social engineering. Traditional antivirus solutions can rarely prevent this sort of attack.

19. Ways to remain vigilant and avoid cyber attacks

- Scrutinize question links/forms shared on social media: If someone shares a link that seems questionable, it is better not to click on it. Hackers use such links to spread malware on a large scale.
- Closely monitor credit reports: By monitoring credit reports on a regular basis, a user can easily discern any abnormal activities that, in turn, will enable him to stop identity theft before it gets out of control.
- Just keep relevant customer information: Keeping only relevant information about customers will reduce the magnitude of loss and information theft in worst-case scenario.
- Be wary of wearable technology: A wearable device like smart watch uses master application to synchronize and streamline activities among peripheral devices. Merely compromising the app will enable the hacker to get access to all the devices and information. Therefore, it is imperative to avoid poorly coded devices.

20. Malware: Cyber-criminal's ultimate choice

Malware is the term commonly used for identifying a group of intrusive software including scareware, spyware, ransomware, worms, computer virus etc. Less severe nuisance software like adware also falls under this category. Advanced malware targets endpoints either by exploiting vulnerabilities in computer applications or by deploying social engineering methods. Gozi, Vawtrak, Dridex are some high profile malware used for committing banking fraud. Modified or missing files, increased CPU usage, frequent freezing are some common symptoms of malware attack.

21. Encryption: Proven way to remain secured

Encryption is a relatively easy way to protect data and secure communication. Link encryption enables a user to encrypt and decrypt all traffic at each endpoint of a communication network. Even if the user's computer is hacked, encryption will make the data unusable. Encryption works for both physical data storage and cloud service. Now-a-days, popular cloud storage service providers such as Dropbox and OneDrive offer encryption service. However, encryption provides a little leeway in case of a severe intrusion attempt by quantum computers.

22. Ransomware: A brief history and timeline

Ransomware is a special variant of malware that blocks access to data by using encryption and demands a ransom for decryption. The first incidence of a ransomware attack took place in 1989 and the AIDS Trojan was responsible for it. With the introduction of Bitcoin and the advancement in encryption algorithms, ransomware has become a major threat in cyber space. During 1989-2017 periods, the US has encountered 27 massive ransomware attacks. The use of ransomware is also prevalent in mobile operating systems. As apps can be installed from third-party websites, android operating system is critically vulnerable to ransomware.

23. Ransomware classification considering severity and complexity

Lock screen ransomware and encrypting ransomware are the likely variants of ransomware program. Lock screen ransomware prevents the user from accessing the PC and displays a full-screen message for ransom payment. WinLock is an example of lock screen ransomware. Encrypting ransomware adopts crypto-viral extortion mechanism. Here, it encrypts the victim's file and demands ransom for decryption. Master Boot Record (MBR) ransomware is a special variant of encrypting ransomware, which can make the operating system unbootable by overwriting the master boot record or master file table. CryptoLocker, CryptoDefense, and CryptoWall are other variants of encrypting ransomware. MarsJoke ransomware especially targets public institutions whereas Virlock is proficient in targeting cloud storage and collaboration apps.

24. How to protect yourself from ransomware attacks

- Watch for strange spelling: After receiving an email or notification, it is advisable to check whether the subject line contains any typo or not.

Phishing frauds are widely known for having typos. Additionally, a user should pay close attention while typing a URL. Writing a misspelled URL can lead the user to a malicious site.

- Use deception technology for security program: Deception technology-based products are capable of identifying ransomware without using signature-based method. Moreover, these products can provide dynamic protection against malicious activities within the internal network, an attribute missing in conventional security programs.

25. Recommended undertakings amidst ransomware attacks

- Adopt security measures early: Anti-virus program often fails to detect a ransomware payload at the onset of the attack. However, carefully monitoring the programs running in the background can provide insight into malicious activity. If a suspected program is detected, immediately removal of it can limit further damage to data.
- Use decryption software: Decryption software can recover data if the same encryption key is used for all encrypted files. However, decryption mechanism is time consuming and cannot guarantee successful recovery all the times.

26. How and why companies pay the ransom

Information regarding customer and competitor profile, pending work order, company budget etc. are vital to business operation. Therefore, most of the businesses choose to pay the ransom and recover their files. Meeting the decline of the ransom payment for avoiding ransom hike is also a probable reason. Besides, business enterprises seldom report security breach to authorities considering the likely legal penalties for inadequate protection and loss of brand image. Criminals use Bitcoin, a crypto currency, for receiving payments. Transactions in Bitcoins cannot be traced by law enforcement agencies.

27. Rationale behind ransomware attacks on public institutions

- Public institutions like hospitals, educational institutions, and government agencies are one of the major sources of personal and confidential information. Getting access to their database will enable hackers to launch attack on a large scale. This sort of attack can cause huge disruptions.

- Inadequate funds along with mismanagement impede the growth and development of cyber security departments. Moreover, most institutions tend to use outdated software and the use of such software make them extremely vulnerable to cyber threat
- Most of the staffs are not trained enough to identify and avoid socially engineered forms of cyber attacks

28. Ransomware: A weapon of mass economic destruction

The use of ransomware for making quick money is rapidly increasing day by day. It is estimated that the total market size of ransomware business is close to USD 1 billion. This figure alone is sufficient to gauge the viciousness of ransomware attack. Anyone connected to the internet is a potential target. Both small and large enterprises are severely affected. A study, conducted by IBM, found that around 40% of all spam messages sent in 2016 contained ransomware. Another similar study, carried out in 2017, revealed the fact that 85% of all malicious email attachments sent in 2016 were loaded with ransomware.

29. Exponential rise in cyber attacks targeting small business enterprises

Hackers are increasingly shifting their attention to Small and Medium Business (SMB) enterprises. Most of the attacks against SMBs are spear phishing attacks. These enterprises are less prepared to tackle any sort of attack and the magnitude of loss is quite overwhelming. In 2015, 74% of the small organizations in the UK reported the incidence of security breach. The same goes for the US. Around 33% of the US SMBs do not have any security mechanism to protect themselves against cyber attack. Most of the business owners do not even think that they are at risk and hackers are taking advantage of such perception.

30. Proactive defense: Understanding the threat landscape

Cyber threat landscape has drastically expanded over the past few years. To remain safe and protect establishments from falling victim to cyber attack, it is imperative for organizations to understand the motivations and objectives of threat actors. It will enable organizations to defend their networks adequately and effectively. Hacktivism, cyber-crime, and cyber-espionage predominantly constitute the threat landscape.

- Hacktivism: Hacktivists want to undermine the reputation of the organization or to destabilize the organization’s operation.
- Cyber-crime: Cyber criminals are largely motivated by money. They frequently attack financial institutions and their clients. Payment card and online banking fraud is the mainstay of such attack.
- Cyber-espionage: Attaining and maintaining access to target networks for gathering strategically valuable information from governments, corporations, and individuals are main objectives of conducting cyber-espionage.

31. Tools employed by hacktivists and means of defending against these

Hacktivists mostly favor attacking websites using Distributed Denial of Service (DDoS) attacks. To initiate a DDoS attack, a hacktivist takes over a large number of computers using malware spam campaigns and subsequently uses botnet to send simple requests (e.g., logging into your account) to a website over and over again. The amount of traffic generated by a DDoS attack can be overwhelming and such traffic often causes site crashes. Anticipating and preventing DDoS attack is difficult task. Setting up a top-notch risk management system along with using DDoS mitigation software (e.g., Cloudflare, Wanguard etc.) can be useful in this regard.

32. Common techniques used by cyber criminals and ways to avoid these

Cyber criminals use mass phishing (socially engineered electronic content), key logging (using a program to record keystrokes), ATM and Point of Sale (PoS) skimming (stealing bank and card information when cards are interested into card readers), and code injection to computer programs for launching their attacks. By scanning all incoming and outgoing emails for suspicious contents, blocking domains and IPs from where phishing emails come and using Domain Message Authentication Reporting and Conformance (DMARC) system can lessen security threat to some extent.

33. How to deal with insider threat to limit cyber-crime

Firstly, selection and management of employees are of most importance. Besides, security awareness program is an absolute must here. For compromised insiders, honey pots along with user behavior analytics should be used to identify users who are actively looking for strategically vital information. Once malicious employees are identified, their behavior should be monitored closely and corrective measures should be quickly adopted if required. In every instance, taking action proactively is of immense importance.

34. How to limit sate and corporate sponsored attacks

As corporate and cyber espionage require prolonged access to target IT infrastructure, attackers use Advanced Persistent Threat (APT) technique. Here, attackers utilize multiple attack vectors simultaneously to increase their likely payoff. The sole purpose of APT attack is to steal data rather than cause harm to the organization or network. Since APT, users utilize multiple attack vectors, no single security measure can keep the organization secured. A well-conceived, consistent, and ongoing security program is necessary in this regard.

35. Use of social engineering as a mode of initiating cyber attacks

The vast majority of the companies are more exposed to cyber attacks than they have to be. Human error alone is responsible for 52% of data and security breaches. In 2015, phishing technique is used in 95% of all espionage attacks and around 80% of all malware attacks are due to phishing frauds. While technical updates are important, minimizing human error demands more attention. Social engineering seeks to exploit irregularities in human behavior to get access to intellectual and financial information. Violation of standard procedures, failure to patch system vulnerabilities and application of misconfigured settings create many opportunities for utilizing social engineering as a way of initiating mass attack.

36. Types of threats where human behavior is a cause

Phishing techniques are commonly used to trick users. However, different variants of phishing seek to exploit users differently. Typical phishing is an email spoofing attack initiated by a known contact or organization. Once the recipient clicks on the link or malicious attachment, phishing process gets started. Spear phishing accomplishes the same task in a more sophisticated way. Instead of sending the phishing emails to a large group of people, the attacker targets a selected group of individuals. Moreover, the source of the email is likely to be a high profile individual within the recipient's own organization. By limiting the target, it becomes easier to make the malicious emails seem even more trustworthy. The success of a spear phishing attack depends on the trustworthiness of the source as well as the validity of the request and message. A highly lucrative variant of spear phishing is business email compromise or whaling. A whaling attack is specifically directed towards the high profile targets like politicians, celebrities, and top-level executives. In each case, email sender asks for transferring money or sharing important documents such as tax file or credit card history immediately.

37. Ways of neutralizing the human factor in cyber attacks

- Second Factor Authentication (2FA): It is almost impossible to prevent every user from clicking on a malicious link. However, 2FA can significantly reduce the likelihood of identity and information theft as it requires a second layer of authentication to access the login credentials after a password has been given.
- Risk based authentication: Risk based authentication applies varying levels of parameters (e.g., login by IP address or specific device) to authentication process. Different levels of authentication may be required for a given user depending on the risk potential of the transaction.

38. Components of contemporary hacking operations

Team diversity is instrumental in modern hacking operation. Having members with expertise on the business operation of target organization provide new ways of approaching the hacking. Contemporary hackers are detail-oriented and select their targets based on available intelligence. They are relentless and will do anything to infiltrate their target. Survivability and resilience are the key attributes of a hacker. In addition to coding, hackers are widely utilizing social media for collecting more information regarding behavioral pattern and exploitable human error. It is also surprising that penetrating a network is the simplest part of an operation and is occasionally outsourced to skilled people to ensure successful completion.

39. Best operating system for cyber criminals

Despite the fact that most of the general users prefer Windows as their primary operating system, nearly all hackers and crackers favor Linux based operating system. Backtrack is a well-known operating system for network cracking and penetration testing. It is arguably the most comprehensive Linux based distribution for security tools. Backtrack provides tools for information gathering, network mapping, digital forensics and reverse engineering. Other well-known operating systems include Kali Linux, Matriux, BackBox, GnackTrack, BalckBuntu and Cyborg Hawk.

40. Methods of tracing the hackers behind cyber attacks

Software developers are working closely with law enforcement agencies for providing training to cyber-crime units and developing forensic tools to collect evidence. COFEE (Computer Online Forensic Evidence Extractor), a USB device developed by Microsoft, enables investigators to extract data promptly from a suspect's device. In most cases, investigators use various tools such as NetStat and Google Analytics for identifying the IP address of the invader. After tracing the IP address, they utilize Geo IP tool to get an idea of the hacker's location. The next step is to contact local Internet Service provider (ISP) to trace the exact location. However, most of the criminals use proxy to hide their tracks. In such case, investigators conduct traffic analysis utilizing records from several ISPs to isolate the proxy service provider.

41. Security measures before cyber attacks: Prevention

To prevent a likely cyber attack, the notion of built-in system security should be incorporated into the design of IT systems. Additionally, the following procedures can largely contribute to preventing attacks:

- Frequently review privacy settings of social media accounts
- Refrain from responding to online requests demanding personal information and apply caution while opening attachments or responding to unknown emails
- Use alphanumeric password and change it regularly
- Periodically run penetration system for identifying system vulnerability
- Make schedules for taking system and data backup

42. Security measures during cyber attacks: Incident management

If the system is compromised, the next line of defense is internal compartmentalization and containment. For defending against a cyber attack, the following instructions can be helpful:

- Attempt to conduct partial system shutdown and relocation for isolating the hacked database
- Backup important files from infected drive to facilitate post recovery
- Disable internet access, try to perform a full system restore and change prior passwords
- Reinstall security software prior to any other program and start deep scanning
- Inform the appropriate authority for conducting investigation

43. Security measure after cyber attacks: Consequence management

Consequence management entails response and recovery mechanism. Recovery mechanism involves conducting a damage assessment survey, taking prompt action for relocating the residual unaffected data/infrastructure and facilitating restoration to pre-attack status without destroying evidence. Carefully crafted attacks can make recovery more difficult. On the contrary, response mechanism is largely associated with tracing the culprit and learning lessons from the incidence to make the organization better capable of defending itself in future.

44. Online freedom versus fear when cyber security is in question

Most major nations are contemplating to impose stringent regulation on online activities for ensuring cyber safety. The US has also tried to adopt “kill switch” program (the act of shutting down the entire online traffic in case of a major threat). However, such government actions have raised questions regarding online freedom among mass people. Amidst such cloudy environment, the use of onion routing for anonymous communication is getting increasingly popular day by day for bypassing likely government intervention.

45. Likelihood of a widespread smart grid attack and potential catastrophe associated with this

Increased level of digitization and automation in the electricity industry has amplified the likelihood of cyber attack in power grids. Moreover, smart grids and meters are more exposed to cyber threat and most developed nations are moving towards smart grid mechanism. Such approach has exponentially heightened the risk of cyber threat. According to the most recent US government report, the number of reported cyber incidents in the energy industry is more than the accumulated number of incidents in all other industries. Hackers specialized in social engineering can easily hack the security credentials of Industrial Control System (ICS) by sending malicious email attachments to power company employees. The magnitude of poetical loss from smart grid attack will be profound. As almost all the activities are heavily dependent on electricity, the whole system will collapse in case of widespread cyber attack.

46. International efforts to contain cyber attacks

Although nearly 90% of the global IT infrastructure belongs to the private sector, 60% of the attacks are aimed at government infrastructures. Therefore, different nations are jointly collaborating to thwart persistent cyber attacks. The International Multilateral Partnership Against Cyber Threat (IMPACT), launched in 2008, is currently the largest global security alliance with 152 member countries excluding the US, United Kingdom, China and Russia. Additionally, NATO member countries are also working together to ensure the cyberspace security. The main objective of these multilateral agencies is to share critical technology and expertise among participating nations.

47. Role of punishment in reducing cyber-crime

Despite the presence of severe penalty such as huge monetary fine, lifetime imprisonment, and even death sentence, legislation often fails to contain cyber-crime. Besides, hacking process is changed rapidly and law cannot properly define all contingencies. Moreover, there are subtle differences between a cyber criminal and an ethical hacker. Improperly constructed law may find it difficult to decipher. Moreover, failure of business to comply fully with regulation (e.g., deploying stringent security protocol) can help the criminal go unpunished.

48. Law enforcement proved insufficient in tackling cyber-crimes

Because of fragmented and uncoordinated resources, law enforcers frequently fail to keep pace with the ever-increasing number of computer intrusion. Besides, they need ongoing training on conducting high-tech forensics for promptly completing the investigation and tracing the criminals. Conducting investigation gets more difficult in case of cross-border cyber crime. In most cases, foreign agencies decline to co-operate if the criminal is a citizen of the respective country. Finally, law enforcement alone cannot make any difference if public awareness cannot be raised against cyber criminals.

49. Prerequisites of a top-notch threat intelligence

At first, the organization must have a clear understanding of all the information assets it has and then should choose a security solution that can effectively protect its asset base from cyber threat. Threat intelligence should come from a qualified third party and must provide insights into the likelihood and magnitude of the risk factors. While sorting through threat intelligence, organizations should give priority to information regarding critical assets with greatest business aspect. In addition, completeness, accuracy, relevance, and timeliness are the desirable attributes of qualified threat intelligence.

50. Future of cyber-crime and cyber security

Currently, we are living in a world where everyone is connected and everything is hackable. According to Intel's forecast, the number of internet-connected devices will increase from 15 billion to 200 billion in 2020. It will be close to impossible to maintain cyberspace security amidst the presence of such insane number of devices. Moreover, increased level of digitization gives tech-savvy people access to unimaginable computing power that can cause havoc, if improperly used. Therefore, it is essential for cyber security professionals to device a mechanism that will enable them to control the devices and data on real time basis.

51. National capacity building to combat cyber crime

It is high time the governments around the world stood up against cyber crime. Every government should establish its national cyber crime action plan and strive to raise public awareness regarding cyberspace security and safety. Special focus should be given to educate vulnerable groups like young people. Moreover, increasing technical capability and developing skilled IT professional are vital for combating cyber crime. Devising a coordinated approach to risk management and skill development is crucial.

Thank you for reading

Cyber Security 51 Handy Things To Know About Cyber Attacks

By

S. R. Tabone

Please have a look at my other books:

https://www.amazon.com/author/stephentabone