MOORE Singhi

Increasing Cyber Attacks due to Work From Home

FOREWARD

As the period of pandemic has increased the Lockdown period, the Cyber Attacks have also increased many-fold majorly in Tier-I and Tier-II companies. These attacks aimed to compromise computers and mobile devices to gain access to users' confidential data, banking details and crypto-currency accounts.

The key threats seen during this period ranged from phishing attacks to rogue apps disguised as COVID-19 information apps that targeted users' sensitive data.

According to cyber security experts, hacking activities and cybercrimes are rising at an alarming rate as miscreants take advantage of the globe's new-found dependence on the virtual world. From Tier-I companies to MSMEs and individuals, nobody is safe as the cyber criminals are not sparing anyone.

Cyber attacks can take many forms: from malware injection and phishing, to hacking and ransomware. Some types of attacks are more effective than others, but all present a significant - and increasingly unavoidable - business risk.

MAJOR ATTACKS RECENTLY

Major Cyber Attacks faced by Businesses houses recently are:

Ransomware

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Ransomware attack has spiked recently as one of the most noticeable attack. The serious risk about this ransomware is its ability to encrypt or lock the data in servers/ individual systems. The data is unlocked, only after the owner pays a ransom amount to the attacker. This system hi-jacking component makes ransomware very disruptive.

Phishing Attacks

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email.

Phishing accounts for 80% of all breaches that organizations face, they've grown 60% over the last year, and they account for over $11 billion in business losses.

Some degree of data breaches happens because of human error and the form of human error which leads to a breach happens when an employee clicks on a phishing email. A phishing email often carries a payload like ransomware or a trojan horse virus which wreaks havoc on the system right after its opened.

Attackers gather information about their victim organizations to ensure they can inflict maximum disruption to them.

Advanced Persistent Threats (APTs)

An advanced persistent threat is an attack in which an unauthorized user gains access to a system or network and remains there for an extended period of time without being detected.

Organizations should be careful of advanced persistent threats. Cybercriminals who are into APTs, give lot of effort and time in mapping their target after they've successfully infiltrated the system. Once they've gathered information, they'll start capturing and transmitting data back to their own servers.

This particular type of attack is persistent in the sense that it can go on for years with the victim remaining unaware. Hackers who participate in APTs are dedicated professionals and often work in groups to penetrate their target organizations

Mirai Malware

Mirai is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnets in large-scale network attacks. It primarily targets online consumer devices such as IP Cameras and home Routers. It has been used in some of the largest and most disruptive Distributed Denial of Service (DDOS)

Stagewares

Stegware seems to be the newest gimmick for cyber-criminals. Using Steganography - the practice of hiding malicious code within an image, video, or otherwise innocuous file - hackers have found yet another way to get malware past security tools.

By hiding malicious code in different file formats that aren't analyzed by standard data security tools, the attacks can fly below the radar of a traditional anti-malware and gateway analysis system. This very method of concealment is invisible to the human eye but can be read through a few certain softwares. This allows an attacker to insert a benign file in the form of a picture or a sound file, into the victim's system and activate once they are past the system's defenses.

Attacks through steganography have reached its peak in recent times. Social media has also been exploited as a platform for the propagation and control of Stegware, with images and tweets sending commands which activate the malware on an infected device.

IOT Malwares

IoT malware is used to perform DDoS attacks; IoT malware scans the open port of IoT services such as FTP, SSH or Telnet; IoT malware performs a brute-force attack to gain access to IoT devices.

There are a number of ways manufacturers can leave IoT devices vulnerable to hackers, but the most common involves assigning weak default login credentials. Sometimes, those credentials often can't be changed, and even if they can, users are rarely prompted to do so.

TYPE OF CYBER SECURITY ASSESSMENTS EACH BUSINESS SHOULD CONDUCT

Sl No.	Assessment	Nature
1	**Risk Assessment**	It helps identify, estimate and prioritize risk for organizations
2	**Vulnerability Assessment**	It uncovers flaws in your security procedures, design, implementation or internal controls
3	**Penetration Testing**	It is unique because it involves an expert acting as a “hacker” in an attempt to breach your security systems. This type of security audit leads to insight about potential loopholes in your infrastructure.
4	**Compliance Audit**	This type of cyber security audit usually examines company policies, access controls and whether regulations are being followed. An organization that does business in the European Union, for example, should run a compliance audit to make sure that they adhere to the General Data Protection Regulation (GDPR)

SUMMARY

Cyber Criminals are increasing now a days and the approach adopted by them are becoming more and more sophisticated. New and latest technologies are being adopted by attackers to attack the organizations.To combat such attacks, it is becoming critical for organizations to adopt latest security measures and get their systems and network audited on a regular basis.

One of the important testing that can be conducted by organization on an annual basis is Vulnerability and Penetration Testing (VAPT) to identify any vulnerability in the organization.

Authored By:

Raj Poddar, *CA, CISA, MBA, CEH, CHFI*
Partner – IT Consulting
Moore Singhi Advisors LLP

TOUCH POINTS

Kolkata
161, Sarat Bose Road
Kolkata 700 026
Tel: +91 (33) 2419 6000/1/2
Email- Services@singhico.com

Hyderabad
5-4-187/3 & 4 Soham Mansion
M. G. Road, Secunderabad - 500
003
Tel: +91 (0)40 2754 2635 / 1015

Ahmedabad
705 P B Parekh Tower,
Near Diwan Ballubhai School,
Kankaria
Ahmedabad – 380022
Tel: +91 (0) 79 - 2547 1562
Email: ahmedabad@singhico.com

Mumbai
B2 402B, Marathon Innova, 4th
Floor, Off Ganpatrao Kadam Marg
Lower Parel, Mumbai - 400 013
Tel: +91 (0) 22 2495 2881
Email: mumbai@singhico.com

Chennai
Unit-11-D, 11th Floor, Ega Trade
Centre,
809, Poonamallee High Road, Kilpauk,
Chennai - 600 010
Tel: +91 (44) 4291 8459
Email: chennai@singhico.com

Bengaluru
No.28, R V Layout, V S Raju road,
Kumara Park West
Bangalore- 560 020
Ph. No.: +91 80 23463462/65
Email: bangalore@singhico.com

Delhi NCR
Unit No.1704, 17th Floor,
World Trade Tower (Tower-B)
DND Fly Way, C-01, Sector 16,
Noida-201301
Tel. No - 0120-2970005, 9205575996
Email- newdelhi@singhico.com

Nagpur
1st Floor, VCA Complex, Civil Lines
Nagpur - 440001
Tel: +91 (0)71 2664 1111
Fax No.: +91 (0)71 2664 1122

DISCLAIMER

This publication contains information in summary form and is therefore intended for general guidance of clients / associates and is meant for private circulation only. We shall not accept anyresponsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriateadvisor.

This document has been compiled based upon information / documents available in public domain and sources believed to be true and reliable. However, no representation is made that it is accurate and complete.