Journal of Mines, Metals and Fuels, 71(2): 127-131; 2023. DOI: 10.18311/jmmf/2023/.......

Print ISSN : 0022-2755

Journal of Mines, Metals and Fuels

Contents available at: www.informaticsjournals.com/index.php/jmmf

Jayanta Bhattacharya
Hony. Chief Editor

Security™

How to Prepare for Information Security Threats for Systems Connected with Internet in MOGI Companies

Part I discusses a security event and the threat types

The Threats

The technology progress is often accompanied by unintended consequences. In the case of automation, the computers that make production smarter also make it more vulnerable to external interference. The possibility of infection by the malicious code that infests the internet is one thing: the Stuxnet worm was one memorable example of a virus that targeted industrial control systems; since then there has been a sophisticated attack on a German steel mill that crippled a blast furnace, as well as many day-to-day attacks that do not make it to the headlines, but which also cause damage and delay.

Cyber-attacks are becoming more common by the day. In the modern world, data has become a new asset. It runs companies, state and nations. Data is now known as the new oil. The mining-oil-gas-integrated (MOGI) companies are particularly vulnerable because such attacks can expose the systems to corrupt, deform and deface all the systems connected.

On 23rd November, India’s top public health institute – AIIMS Delhi – came under attack by cybercriminals, crippling routine health services which the institute provides of tens of thousands of patients. The cyberattack froze AIIMS’ e-hospital system – including appointments and registration at outpatient departments (OPD), billing at inpatient departments (IPD), laboratory report generation, and smart lab, among others.

The outages have resulted in long queues and errors in handling emergency cases. According to the institute, a ransomware attack has corrupted all the files stored on the main and backup servers of the hospital.The perpetrators held around 4 crore patient profiles at ransom – including sensitive data and medical records of VIPs. The exploited databases contain Personally Identifiable Information (PII) of patients and healthcare workers, and administrative records kept on blood donors, ambulances, vaccination, caregivers and employee login credentials.

The extent and threat of the attack is so much that multiple agencies like Delhi Police, the Centre’s Computer Emergency Response Team (CERT), the Ministry of Home Affairs, and even the National Investigation Agency have joined the probe. However, they haven’t been able to fully crack the case.

The attack, believed to be a major one, comes within a month after AIIMS announced that it would go paperless from January 1, 2023, and be fully digitized by April 2023.

However, AIIMS is no stand-alone case. Cyber threat watchdog CloudSEK said the Indian healthcare sector was the second most targeted by cybercriminals worldwide. Research by the company showed that health organisations witnessed a massive spike in cyber attacks during the pandemic. "In the first four months of 2022, the number of cyber attacks on the sector rose by 95.34 per cent compared to the same period in 2021," its study said. According to Indusface, a software security company, there were more than 1 million cyber attacks of various types across Indusface's global healthcare clientele. Of these, 278,000 attacks were reported in India alone.

Cyber attack

For those new, a cyber-attack is any attempt to gain unauthorised access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems-using the public data network. Any individual or group can launch a cyber attack from anywhere by using one or more various attack strategies. In AIIMS, cybercriminals have unleashed Ransomware, malware designed to deny a user or organisation access to files. A user or organisation's critical data is encrypted so that they cannot access files, databases, or applications. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Those behind the cyber attack in AIIMS have warned the institute to prepare for a negotiation. "A protonmail address has been left for the institute for communication. An undisclosed demand has been sought in cryptocurrency in exchange for a key that would decrypt the data," sources informed.

Experts suggest that with everything going online, the extent of cyberattacks and their strategies would evolve, however, to neutralise that threat, entities would also have to progress in cyber safety. "Sectors which are critical to a nation will remain on target. Sooner or later, things will go online and whatever service is online is becoming a target. We saw something happening in the power and IT sectors. Now the health sector is at the fore," said Dr. Muktesh Chander IPS, former DGP Goa and Chevening Cyber Security Fellow, UK.

Security Threat

A security threat is a malicious act that aims to corrupt or steal data or disrupt an organization's systems or the entire organization. As cybersecurity threats continue to evolve and become more sophisticated, enterprise IT must remain vigilant when it comes to protecting their data and networks. To do that, they first have to understand the types of security threats they're up against.

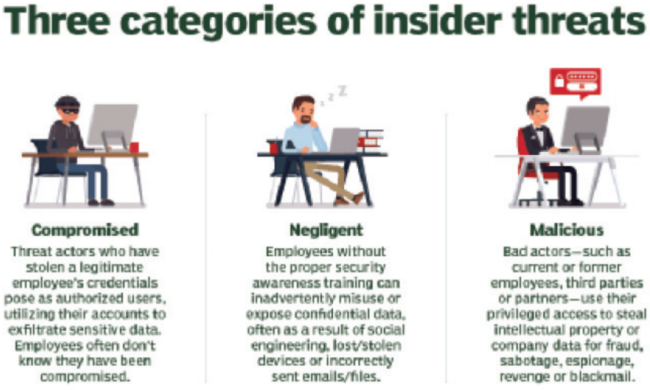
Below are the top 10 types of information security threats that IT teams need to know about.

1. Insider threats

An insider threat occurs when individuals close to an organization who have authorized access to its network intentionally or unintentionally misuse that access to negatively affect the organization's critical data or systems.

Careless employees who don't comply with their organizations' business rules and policies cause insider threats. For example, they may inadvertently email customer data to external parties, click on phishing links in emails or share their login information with others. Contractors, business partners and third-party vendors are the source of other insider threats.

Some insiders intentionally bypass security measures out of convenience or ill-considered attempts to become more productive. Malicious insiders intentionally elude cybersecurity protocols to delete data, steal data to sell or exploit later, disrupt operations or otherwise harm the business.



Three categories of insider threats

Compromised
Threat actors who have stolen a legitimate employee's credentials pose as authorized users, utilizing their accounts to exfiltrate sensitive data. Employees often don't know they have been compromised.

Negligent
Employees without the proper security awareness training can inadvertently misuse or expose confidential data, often as a result of social engineering, lost/stolen devices or incorrectly sent emails/files.

Malicious
Bad actors—such as current or former employees, third parties or partners—use their privileged access to steal intellectual property or company data for fraud, sabotage, espionage, revenge or blackmail.

1.1. Preventing insider threats

The list of things organizations can do to minimize the risks associated with insider threats include the following:

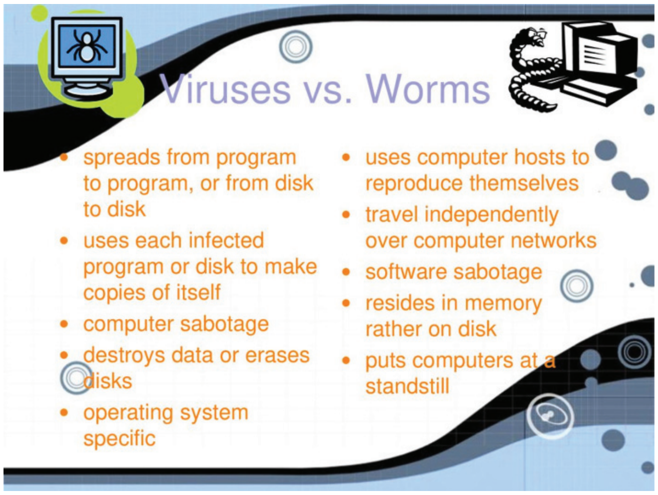
1. limit employees' access to only the specific resources they need to do their jobs;
2. train new employees and contractors on security awareness before allowing them to access the network. Incorporate information about unintentional and malicious insider threat awareness into regular security training;
3. set up contractors and other freelancers with temporary accounts that expire on specific dates, such as the dates their contracts end;
4. implement two-factor authentication, which requires each user to provide a second piece of identifying information in addition to a password; and install employee

monitoring software to help reduce the risk of data breaches and the theft of intellectual property by identifying careless, disgruntled or malicious insiders.

2. Viruses and Worms

Viruses and worms are malicious software programs (malware) aimed at destroying an organization's systems, data and network. A computer virus is a malicious code that replicates by copying itself to another programme, system or host file. It remains dormant until someone knowingly or inadvertently activates it, spreading the infection without the knowledge or permission of a user or system administration.

A computer worm is a self-replicating programme that doesn't have to copy itself to a host programme or require human interaction to spread. Its main function is to infect other computers while remaining active on the infected system. Worms often spread using parts of an operating system that are automatic and invisible to the user. Once a worm enters a system, it immediately starts replicating itself, infecting computers and networks that aren't adequately protected.



Viruses vs. Worms

- spreads from program to program, or from disk to disk
- uses each infected program or disk to make copies of itself
- computer sabotage
- destroys data or erases disks
- operating system specific

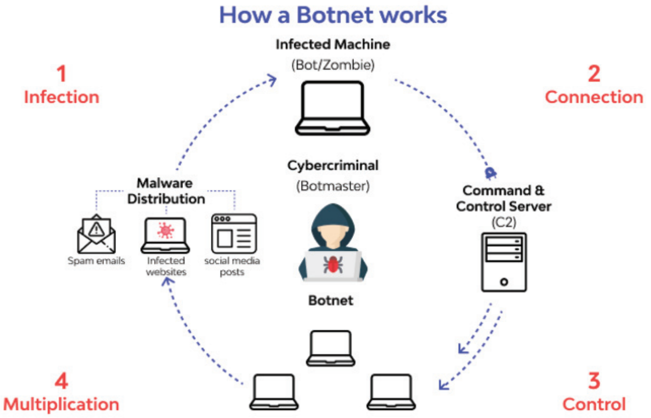
- uses computer hosts to reproduce themselves
- travel independently over computer networks
- software sabotage
- resides in memory rather on disk
- puts computers at a standstill

2.1 Preventing Viruses and Worms

To reduce the risk of these types of information security threats caused by viruses or worms, companies should install antivirus and antimalware software on all their systems and networked devices and keep that software up to date. In addition, organizations must train users not to download attachments or click on links in emails from unknown senders and to avoid downloading free software from untrusted websites. Users should also be very cautious when they use P2P file sharing services and they shouldn't click on ads, particularly ads from unfamiliar brands and websites.

3. Botnets

A botnet is a collection of Internet-connected devices, including PCs, mobile devices, servers and IoT devices that are infected and remotely controlled by a common type of malware. Typically, the botnet malware searches for vulnerable devices across the internet. The goal of the threat actor creating a botnet is to infect as many connected devices as possible, using the computing power and resources of those devices for automated tasks that generally remain hidden to the users of the devices. The threat actors — often cybercriminals — that control these botnets use them to send email spam, engage in click fraud campaigns and generate malicious traffic for distributed denial-of-service attacks.



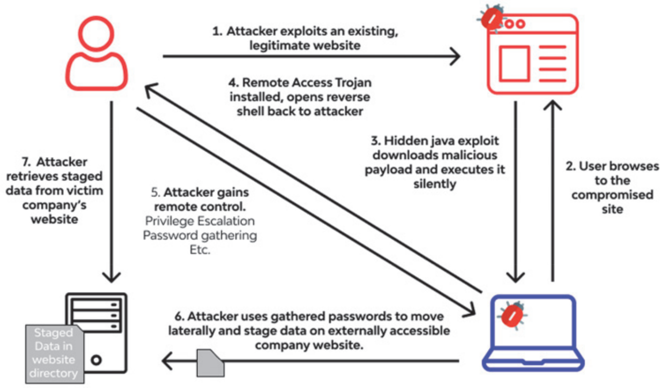
3.1 Preventing Botnets

Organizations have several ways to prevent botnet infections:

a. monitor network performance and activity to detect any irregular network behaviour;
b. keep the operating system up to date;
c. keep all software up-to-date and install any necessary security patches;
d. educate users not to engage in any activity that puts them at risk of bot infections or other malware, including opening emails or messages, downloading attachments or clicking links from unfamiliar sources; and
e. implement antibotnet tools that find and block bot viruses. In addition, most firewalls and antivirus software include basic tools to detect, prevent and remove botnets.

4. Drive-by Download Attacks

In a drive-by download attack, malicious code is downloaded from a website via a browser, application or integrated operating system without a user's permission or knowledge. A user does not have to click on anything to activate the download. Just accessing or browsing a website can start a download. Cybercriminals can use drive-by


1. Attacker exploits an existing, legitimate website
2. User browses to the compromised site
3. Hidden java exploit downloads malicious payload and executes it silently
4. Remote Access Trojan installed, opens reverse shell back to attacker
5. Attacker gains remote control.
Privilege Escalation
Password gathering
Etc.
6. Attacker uses gathered passwords to move laterally and stage data on externally accessible company website.
7. Attacker retrieves staged data from victim company's website
Staged Data in website directory

downloads to inject banking Trojans, steal and collect personal information as well as introduce exploit kits or other malware to endpoints.

4.1 Preventing Drive-by Download Attacks

One of the best ways a company can prevent drive-by download attacks is to regularly update and patch systems with the latest versions of software, applications, browsers, and operating systems. Users should also be warned to stay away from insecure websites. Installing security software that actively scans websites can help protect endpoints from drive-by downloads.

5. Phishing Attacks

Phishing attacks are a type of information security threat that employs social engineering to trick users into breaking normal security practices and giving up confidential information, including names, addresses, login credentials, Social Security numbers, credit card information and other financial information. In most cases, hackers send out fake emails that look as if they're coming from legitimate sources, such as financial institutions, eBay, PayPal – and even friends and colleagues.

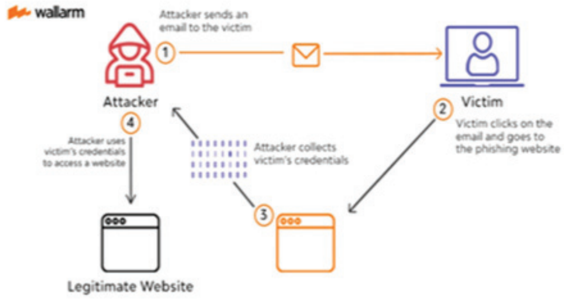
In phishing attacks, hackers attempt to get users to take some recommended action, such as clicking on links in emails that take them to fraudulent websites that ask for personal information or install malware on their devices. Opening attachments in emails can also install malware on users' devices that are designed to harvest sensitive information, send out emails to their contacts or provide remote access to their devices.

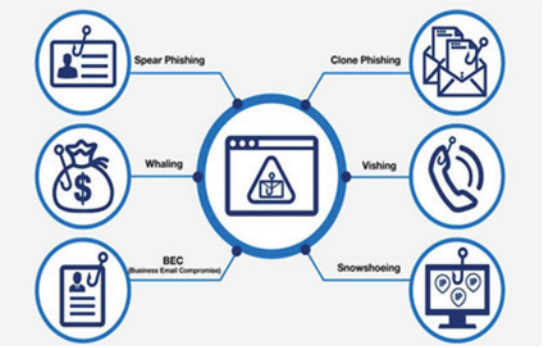
5.1 Preventing Phishing Attacks

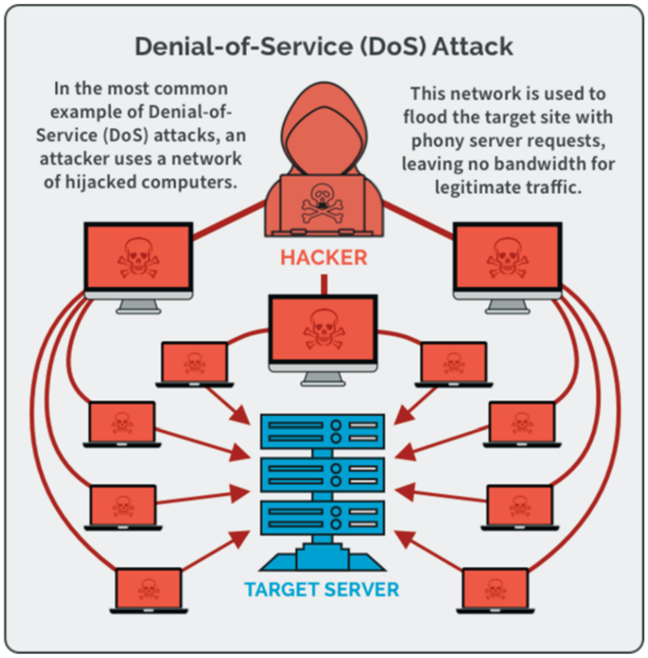
Enterprises should train users not to download attachments or click on links in emails from unknown senders and avoid downloading free software from untrusted websites.

6. Distributed Denial-of-Service (DDoS) Attacks

In a distributed denial-of-service (DDoS) attack, multiple compromised machines attack a target, such as a server, website or other network resource, making the target totally inoperable. The flood of connection requests, incoming messages or malformed packets forces the target system to slow down or to crash and shut down, denying service to legitimate users or systems.


wallarm
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
4
Attacker uses victim's credentials to access a website
Legitimate Website




Denial-of-Service (DoS) Attack
In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.
This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.
HACKER
TARGET SERVER

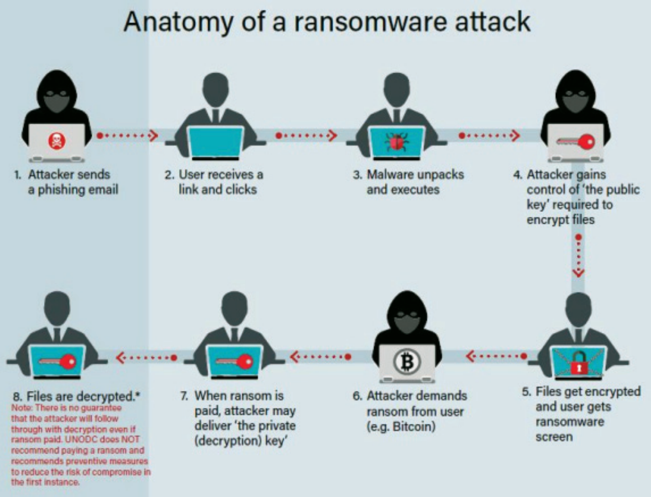
Preventing DDoS Attacks

To help prevent DDoS attacks, companies should take these steps:

1. Implement technology to monitor networks visually and know how much bandwidth a site uses on average. DDoS attacks offer visual clues so administrators who understand the normal behaviours of their networks will be better able to catch these attacks.
2. Ensure servers have the capacity to handle heavy traffic spikes and the necessary mitigation tools necessary to address security problems.
3. Update and patch firewalls and network security programs.
4. Set up protocols outlining the steps to take in the event of a DDoS attack occurring.

7. Ransomware

In a ransomware attack, the victim's computer is locked, typically by encryption, which keeps the victim from using the device or data that's stored on it. To regain access to the device or data, the victim has to pay the hacker a ransom, typically in a virtual currency such as Bitcoin. Ransomware can be spread via malicious email attachments, infected software apps, infected external storage devices and compromised websites.

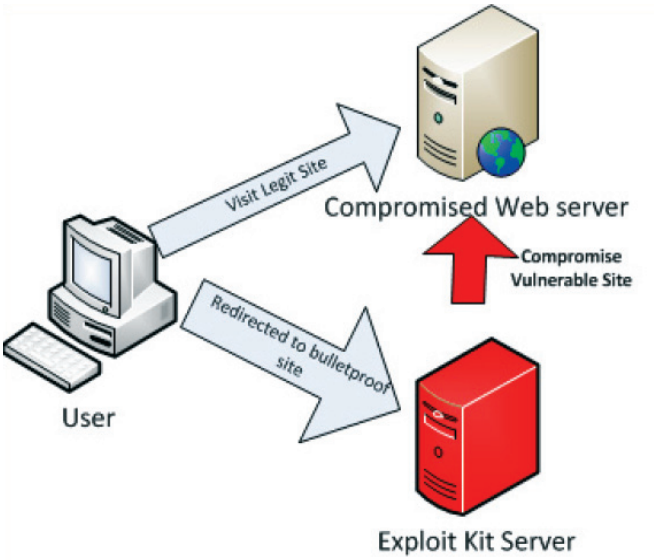

Anatomy of a ransomware attack
1. Attacker sends a phishing email
2. User receives a link and clicks
3. Malware unpacks and executes
4. Attacker gains control of 'the public key' required to encrypt files
5. Files get encrypted and user gets ransomware screen
6. Attacker demands ransom from user (e.g. Bitcoin)
7. When ransom is paid, attacker may deliver 'the private (decryption) key'
8. Files are decrypted.*
Note: There is no guarantee that the attacker will follow through with decryption even if ransom paid. UNODC does NOT recommend paying a ransom and recommends preventive measures to reduce the risk of compromise in the first instance.

7.1 Preventing Ransomware

To protect against ransomware attacks, users should regularly back up their computing devices and update all software, including antivirus software. Users should avoid clicking on links in emails or opening email attachments from unknown sources. Victims should do everything possible to avoid paying ransom. Organizations should also couple a traditional firewall that blocks unauthorized access to computers or networks with a programme that filters web content and focuses on sites that may introduce malware. In addition, limit the data a cybercriminal can access by segregating the network into distinct zones, each of which requires different credentials.

8. Exploit Kits

An exploit kit is a programming tool that enables a person without any experience writing software code to create, customize and distribute malware. Exploit kits are known by a variety of names, including infection kit, crimeware kit, DIY attack kit and malware toolkit. Cybercriminals use these toolkits to attack system vulnerabilities to distribute malware or engage in other malicious activities, such as stealing corporate data, launching denial of service attacks or building botnets.



8.1 Preventing Exploit Kits

To guard against exploit kits, an organization should deploy antimalware software as well as a security programme that continually evaluates if its security controls are effective and provide protection against attacks. Enterprises should also install antiphishing tools because many exploit kits use phishing or compromised websites to penetrate the network.