MSI Weekly Information Security & Threat Briefing

Apr 16 - 20, 2018

MSI Threat Intelligence Team
info@microsolved.com
614-351-1237

MICROSOLVED,INC.

About the MSI Weekly Information Security & Threat Briefing

What is it? The MicroSolved Weekly Information Security & Threat Briefing contains gists and links to information security (infosec) news items, tools, advisories and more.. To gather this information, MSI employs TigerTrax™; our proprietary platform for gathering and analyzing data from the social media sphere and World Wide Web. This sophisticated platform provides the MSI team with a unique capability to rapidly and effectively monitor the world's data streams for information concerning potential cyber-threats and news items that are of interest to organizations across the globe.

How do I use it? The briefing is split into a number of industry-specific sections that make it easy to find the links that are of highest interest to the individual reader. Simply check the Table of Contents above to find the section of most interest to you (i.e. Financial, Health, High Tech, Government, Utility, SCADA, etc.). And don't miss the featured infosec news of the week and general infosec news sections. These contain infosec news and concerns that are of interest to everyone.

What else is there? MSI has also included a glossary of business impacts in the Weekly Information Security & Threat Briefing. This glossary explains what the threats are and how they work. But what is more important, it explains what their impact can be from the business point of view. This gives Management and Board personnel the perspective they need to make informed decisions when treating the business risks that these cyber-threats represent.

Featured Infosec News Items of the Week

Instagram bends to GDPR – a “download everything” tool is coming: Following criticism about lack of data portability – unlike parent Facebook, it doesn’t have a Download Your Data tool – Instagram now says it’s building a tool to let users download everything they’ve ever shared. What’s not clear yet is if the tool will also enable users to export following and follower lists, Likes, comments, Stories, and the captions they put onto posts.

- https://nakedsecurity.sophos.com/2018/04/13/instagram-bends-to-gdpr-a-download-everything-tool-is-coming/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29

Facebook moving 1.5 billion users away from GDPR protection: If a new European law restricting what companies can do with people's online data went into effect tomorrow, almost 1.9 billion Facebook users around the world would be protected by it. But the online social network is making changes that ensure the number will be much smaller. Next month, Facebook is planning to make that the case for only European users, meaning 1.5 billion members in Africa, Asia, Australia, and Latin America will not fall under the European Union's General Data Protection Regulation (GDPR), which takes effect on May 25.

- https://www.zdnet.com/article/facebook-moving-1-5-billion-users-away-from-gdpr-protection/#%3Ca%20href='https://twitter.com/search?q=ftag'%20target='_blank'%3Eftag%3C/a%3E=RSSbaffb68

Infosec News of General Interest

April 2018 – Microsoft Patch Tuesday: April showers might bring May flowers, but the second Tuesday in April brings a deluge of security updates from Microsoft. As usual, we have updates for all of the currently supported versions of the Windows operating system, both client and server, as well as both of Microsoft's web browsers, Internet Explorer and Edge.

- https://techtalk.gfi.com/april-2018-microsoft-patch-tuesday/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TalkTechToMe-All+%28GFI+Blog%29

25 Million U.S. Individuals Impacted by 2016 Uber Hack: The 2016 data breach that Uber made public in November 2017 impacted over 25 million riders and drivers in the United States, the Federal Trade Commission (FTC) reveals. The hack, which the ride-sharing company kept silent about for a year, impacted more than 57 million users globally. Hackers managed to access data stored on an Amazon Web Services (AWS) account and steal names, email addresses and mobile phone numbers of customers around the world.

- https://www.securityweek.com/25-million-us-individuals-impacted-2016-uber-hack?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29

Cyber security: Don't leave it to your tech team or you'll get breached, warns data protection chief: A company can have the best technology team but if management don't take security seriously too then data will inevitably get lost or stolen, the Information Commissioner has warned.…

- https://www.zdnet.com/article/cyber-security-dont-leave-it-to-your-tech-team-or-youll-get-breached-warns-data-protection-chief/#%3Ca%20href='https://twitter.com/search?q=ftag'%20target='_blank'%3Eftag%3C/a%3E=RSSbaffb6

Actually, Myspace Sold Your Data Too. In the wake of Facebook's privacy debacle, Myspace Tom has emerged as an unlikely hero. But the platform he built and the data you put on Myspace continues to help advertisers target its old users.

- https://motherboard.vice.com/en_us/article/43bbbn/myspace-tom-viant-time-inc-facebook-cambridge-analytica

Cyber Infosec News & Security Advisories

"Early Bird" Code Injection Technique Helps Malware Stay Undetected: Security researchers have discovered at least three malware strains using a new code injection technique that allowed them to avoid antivirus detection. They named the technique "Early Bird" because its mode of operation relies on using legitimate Windows OS functions to inject malicious code inside application processes before the actual app process starts and anti-malware products hook into the process to scan for malicious behavior.

- https://www.bleepingcomputer.com/news/security/early-bird-code-injection-technique-helps-malware-stay-undetected/

Google Chrome to Boost User Privacy by Improving Cookies Handling Procedure: Google engineers plan to improve user privacy and security by putting a short lifespan on cookies delivered via HTTP connections. Google hopes that the move will force website developers and advertisers to send cookies via HTTPS, which "provides significant confidentiality protections against [pervasive monitoring] attacks."

- https://www.bleepingcomputer.com/news/security/google-chrome-to-boost-user-privacy-by-improving-cookies-handling-procedure/

Hackers Have Started Exploiting Drupal RCE Exploit Released Yesterday: Hackers have started exploiting a recently disclosed critical vulnerability in Drupal shortly after the public release of working exploit code.

- https://thehackernews.com/2018/04/drupal-rce-exploit-code.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29

A Facebook malware has compromised thousands of accounts. The IT security researchers at Radware have discovered a sophisticated malware campaign targeting unsuspecting Facebook users in the name of a painting application called ‘Relieve Stress Paint.’ As a result, tens of thousands Facebook accounts have been compromised in the last couple of days.

- https://www.hackread.com/facebook-malware-hacks-thousands-of-accounts/

Financial Industry Infosec News

Inside Job Behind Theft of $3M from Bitcoin Exchange, Says CEO: The chief executive officer of a Bitcoin exchange believes the theft of more than $3 billion from the platform was an inside job.

- https://www.tripwire.com/state-of-security/latest-security-news/inside-job-behind-theft-3b-bitcoin-exchange-says-ceo/

Scammers Bank on Cryptocurrency with Fake Apps: Fake cryptocurrency apps in the mobile app ecosystem. In the mobile app ecosystem, Risk IQ has detected and blacklisted dozens of fake cryptocurrency apps that exploit the names of well-known exchanges and mixers, as well as hundreds of sites that falsely promise to make users money in other ways.…

- https://www.infosecurity-magazine.com:443/news/scammers-bank-on-cryptocurrency/

Open Banking: Tremendous Opportunity for Consumers, New Security Challenges for Financial Institutions. The concept of open banking, as structured by the U.K.'s Open Banking and PSD2 regulations, is designed to enable third-party payment service providers (TTPs) to access account information and perform payments under the authorization of the account owner. This represents both a challenge and a tremendous opportunity for financial institutions and TPPs.…

- https://securityintelligence.com/open-banking-tremendous-opportunity-for-consumers-new-security-challenges-for-financial-institutions/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SecurityIntelligence+%28Security+Intelligence%2

Business, Retail & Commercial Infosec News

Chris Vickery Discusses Data Leak of 48 Million Users by Private Intelligence Firm (Localblox): SAN FRANCISCO – Profile data of 48 million users that was scraped from social networks and websites ranging from Facebook, LinkedIn, Zillow and Twitter was leaked by a private intelligence agency. The data was left on an Amazon S3 storage bucket accessible without a password by Localblox, the company that harvested the data.

- https://threatpost.com/chris-vickery-discusses-data-leak-of-48-million-users-by-private-intelligence-firm/131295/

LinkedIn bug allowed data to be stolen from user profiles. A bug in how LinkedIn autofills data on other websites could have allowed an attacker to silently steal user profile data. The flaw was found in LinkedIn's widely used AutoFill plugin, which allows approved third-party websites to let LinkedIn members automatically fill in basic information from their profile -- such as their name, email address, location, and where they work -- as a quick way to sign up to the site or to receive email newsletters.

- https://www.zdnet.com/article/linkedin-bug-allowed-data-to-be-stolen-from-user-profiles/#%3Ca%20hr

LinkedIn Fixes AutoFill Button That Allowed Rogue Harvesting of User Data:

- https://www.bleepingcomputer.com/news/security/linkedin-fixes-autofill-button-that-allowed-rogue-harvesting-of-user-data/

Heavy Industry, Utility & SCADA Infosec News

Great Western Railway accounts breached: Great Western Railway (GWR) is urging their customers to reset their passwords immediately after confirming that it was a target of a cyber-attack. The train operator confirmed this by saying that they have identified a series of automated attempts to access 1,000 customer accounts on their website, out of which more than one million people who have GWR accounts have already been notified before broader email was distributed

- http://www.ehackingnews.com/2018/04/great-western-railway-accounts-breached.html

70% of energy firms worried about "catastrophic failure" due to cyber attacks. Operational outages and shutdowns and physical injury to employees due to cyberattacks are among the main worries of more than 95% energy and oil & gas firms, a new survey shows. Some 70% worry that cyberattacks could yield catastrophic results, such as explosions, according to the Dimensional Research study conducted on behalf of Tripwire. The report surveyed 151 IT and technology (OT) security professionals at energy and oil and gas companies. Some 65% say their organizations properly invest in ICS security, while 56% of those without sufficient security budgets say it would take a major cyberattack to pressure thier firm to properly invest in security.

- https://www.darkreading.com/attacks-breaches/70--of-energy-firms-worry-about-physical-damage-from-cyberattacks/d/d-id/1331589

Health Care Industry Infosec News

FDA moves to require patching in connected medical devices: The Food and Drug Administration is looking to mitigate serious cybersecurity threats to connected medical devices, especially attacks that could disrupt the operation of critical monitors and drug delivery equipment. As part of a plan announced on April 17, the FDA wants software and firmware in devices directly linked to patient safety like insulin pumps and cardiac pacemakers to be able to be patched on an ongoing basis. The FDA is also considering new requirements covering the disclosure of vulnerabilities and updated guidance to guard against ransomware attacks as well as major risks to patient safety.

- https://fcw.com/articles/2018/04/19/fda-cyber-device.aspx

Beware! Medical AI systems are easy targets for fraud and error. Medical AI systems are particularly vulnerable to attacks and have been overlooked in security research, a new study suggests. Researchers from Harvard University believe they have demonstrated the first examples of how medical systems can be manipulated in a paper published on arXiv. Sam Finlayson, lead author of the study, and his colleagues Andrew Beam and Isaac Kohane, used the projected gradient descent (PGD) attack on image recognition models to try and get them to see things that aren't there.

- https://www.theregister.co.uk/2018/04/19/beware_medical_ai_systems_are_easy_targets_for_fraud_and_error/

Government & Military Infosec News

FBI Refuses To Say Whether It Bought iPhone Unlocking Tech GrayKey: Motherboard found that federal and more local law enforcement agencies have bought tech to unlock up to date iPhones. But the FBI, which is pushing for backdoors, refuses to say whether it has also purchased the equipment.…

- https://motherboard.vice.com/en_us/article/ne99mg/fbi-refuses-graykey-grayshift-iphone-unlock

Zuckerberg Unveils the Cyber-Naivete of Congress: The 10-plus hours of Q&A between Facebook CEO Mark Zuckerberg and members of both houses of congress on April 10 and 11 was, in a word, painful. Agonizingly painful, as we watched one senator and congressman/congresswoman after the other demonstrate their lack of basic knowledge of how the internet and Facebook worked.…

- https://securityboulevard.com/2018/04/zuckerberg-unveils-the-cyber-naivete-of-congress/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SecurityBloggersNetwork+%28Security+Bloggers+Network%29

Schneier talks cyber regulations, slams U.S. lawmakers. Schneier, security expert and CTO of IBM Resilient, spoke twice this week at RSAC about the coming wave of cyber regulations, and the dangers those laws and policies will bring if the lack input from technologists.

- https://searchsecurity.techtarget.com/news/252439555/Schneier-talks-cyber-regulations-slams-US-lawmakers

Senate passes DHS bug bounty bill: The Senate passed legislation April 17 that compels DHS to establish a bug bounty program. Sponsored by Sens. Maggie Hassan (D-N.H.), Rob Portman (R-Ohio), Claire McCaskill (D-Mo.) and Kamala Harris (D-Calif.), the bill was introduced last year and authorizes $250,000 for DHS to contract with an outside organization to run the program, which would pay security researchers for finding undiscovered flaws and vulnerabilities in DHS systems and software.

- https://fcw.com/articles/2018/04/19/dhs-bug-bounty-senate.aspx

Cyber-Security Tools, Techniques & Advice

Net Creds-Sniff out Username and Password of Users in your Network: In this Kali Linux Tutorial, we show you how to use Net Creds to launch a MITM attack.Net creds is a python based script to sniff login credentials of victim who visited the website.

- https://gbhackers.com/net-creds-mitm-attack/

SnoopSnitch shows Android users what security patches are missing from their phone: Google provides Android security patches to AOSP once a month, which manufacturers pull from to integrate into the Android distributions on their devices.

- https://www.techrepublic.com/article/snoopsnitch-shows-android-users-what-security-patches-are-missing-from-their-phone/#%3Ca%20href='https://twitter.com/search?q=ftag'%20target='_blank'%3Eftag%3C/a%3E=RSS56d97e7

Pymeta - Search The Web For Files On A Domain To Download And Extract Metadata. Pymeta is a Python3 rewrite of the tool PowerMeta, created by dafthack in PowerShell. It uses specially crafted search queries to identify and download the following file types (pdf, xls, xlsx, doc, docx, ppt, pptx) from a given domain using Google and Bing

- https://goo.gl/rmUvLv #CommandLine… https://twitter.com/i/web/status/984935996092534785

How attackers can exploit iTunes Wi-Fi sync to gain lasting control of target devices. Apple has implemented a mechanism that should prevent easy exploitation of the feature, but the researchers say that it doesn't address the "Trustjacking" problem in an holistic manner.

- https://www.helpnetsecurity.com/2018/04/19/itunes-wi-fi-sync-ios-compromise/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

First Public Demo of Data Breach via IoT Hack Comes to RSAC: The vice president of research, M. Carlton, and chief technology officer, Stephen Ridley, of IoT security company Senrio will present "Lateral Attacks between Connected Devices in Action" on the RSA Sandbox's IoT stage Thursday.

- https://www.darkreading.com/vulnerabilities---threats/first-public-demo-of-data-breach-via-iot-hack-comes-to-rsac/d/d-id/1331588?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple

Appendix A: Glossary of Business Risks and Threats

The glossary below contains explanations of information security terms you may see in our reports. This glossary is written in non-technical terms and gives the readers some idea of the threats and risks each term presents to businesses.

1. **Advanced Persistent Threat (APT):** Advanced persistent threats are stealthy, multi-phase, long term network attacks perpetrated by individuals or groups. The purpose of these attacks is generally to linger on the network undetected and intercept private information and intellectual property. These attacks are also perpetrated by groups and nation states for political purposes.
2. **Botnets:** Botnets are groups of compromised computers that have been infected by malware which allows them to be controlled by the attacker(s). It can be very difficult for organizations to detect the fact that they have been infected. Botnets are used by their controllers to mount DDoS attacks, steal information, send spam, etc. Egress filtering is a good way to detect Botnet activity.
3. **Brute-Forcing:** Brute forcing attacks entail trying every possible combination (using trial and error) when attempting to decrypt keys and passwords rather than employing intellectual strategies to limit the number of guesses that need to be made. Brute forcing works best when trying to decrypt relatively short passwords.
4. **Code Injection Attacks:** There are a number of code injection attacks including SQL injection, command line injection, LDAP injection, XSS, etc. These attacks generally entail inputting unexpected strings of characters into form fields that allow attackers to corrupt or take command of the application. These attacks are generally made possible by improper application coding methods that do not perform proper input validation (making sure that the characters typed into a form field are of the expected type and length).
5. **Cross-Site Request Forgery (CSRF) Attacks:** To mount CSRF attacks, the attacker must have the ability to place hidden links on web pages in places likely to be clicked by users. If attackers are able to find a reproducible link that executes a specific action on the target web page while the victim is logged in there, they are able to embed the link on a page they control and trick the victim into opening it. Social engineering is often used in conjunction with CSRF to trick the victim into doing what the attacker wants.

6. **Cross-Site Scripting (XSS) Attacks:** XSS attacks generally become possible when software applications do not properly encode or validate user input (making sure that form field only accepts certain types and lengths of characters). These attacks are wide spread and dangerous as the malicious code used by the attacker comes from a trusted source and therefore bypass security mechanisms. XSS allows attackers to access session tokens, cookies and other sensitive information retained by the browser.
7. **Data Leaks:** When private information is inadvertently revealed by, or is stolen from, a computer system, a data leak is said to have occurred. Data leaks have many causes including system misconfigurations, employee errors, malware/cyber-attacks, failure to update/patch systems, ineffective information security mechanisms, etc. Data leaks can cause great damage to companies and organizations, and can result in fines/penalties, lawsuits, loss of business, reputational damage, loss of intellectual property, etc.
8. **Denial of Service (DoS) Attacks:** To perform denial of service, attackers flood networks or systems with so much input that they cannot carry out their normal functions. Although there are a number of fixes that can be installed to limit the damage caused by DoS attacks, attackers are constantly formulating new kinds of attacks. Attackers often employ or threaten denial of service in order to extort target businesses and organizations.
9. **Dictionary Attacks:** Dictionary attacks entail using all the words in various dictionaries when attempting to decrypt keys or passwords. This limits the number of guesses that need to be made and speeds up the decryption process (as opposed to brute forcing). Dictionary attacks are the reason why security professionals recommend that passwords should be obfuscated using numbers and special characters.
10. **Directory Traversal Attacks:** Directory traversal attacks typically use web browsers to input data into flawed web servers that do not properly validate that data (make sure the data is of the expected type and length). This allows attackers to “traverse” from the intended directory to other directories. These attacks can allow attackers to view private information or even to take control of the system.
11. **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks are similar to DoS attacks, but are more dangerous. In DDoS attacks, Botnets of thousands or even millions of computers are typically used to flood networks or systems with input and render them unusable for regular business purposes. These attacks are more difficult to stop than standard DoS attacks, and often require the assistance of the

users' Internet Service Provider (ISP). DDoS attacks are increasing in scale and sophistication as time passes.

12. **Executables:** An executable is a particular type of file that is capable of being run as a program on a computer. Running an executable causes a computer to perform a task(s). Malware and injected code often contain executables that allow attackers to corrupt or control target systems. There are a number of file extensions associated with executable including .exe, .jar, .com, etc.
13. **Exploits:** Exploits are methodologies or mechanisms that are used by attackers to take advantage of vulnerabilities in operating systems, software applications, etc. There are many websites on the Internet that detail exploits that can be used to compromise vulnerable systems. These exploits are often available free of charge.
14. **Exposures:** Exposures occur when private information, systems, services or control mechanisms are made available to unauthorized viewers or users. Exposures can occur accidentally through personnel error, because of system misconfigurations or because of malicious actions by outside parties or disgruntled insiders. One of the primary reasons for conducting network vulnerability assessments is to detect unwanted exposures.
15. **Hacktivism:** Hacktivism entails subverting or exploiting vulnerable networks or computer systems for some political or socially motivated reason. Hacktivists can be groups or individuals. The best known hacktivist group currently operating is known as "Anonymous".
16. **Indicators of Compromise and/or Attack:** Indicators of compromise or attack on networks and computer systems include suspicious ports being active, slow or strange system performance, changes is services and drivers, anomalous system permission changes, changes in DNS or IP routing, etc. System compromises or attacks are often very difficult to detect. That is the reason why security professionals recommend that organizations monitor for and address these indicators diligently.
17. **Indirect Attacks:** It is usually very difficult to successfully attack computer networks and systems directly because of network perimeter defenses and other security measures. Because of this, attackers often begin their network attacks indirectly. Common indirect attacks include compromising vendor/third party systems that are trusted by the target network, social engineering attacks and watering hole attacks. Indirect attacks are one of the reasons organizations should employ controls such as layered security defenses, monitoring and internal network vulnerability assessment.

18. **Malware:** Malware is a broad term used to describe a number of different types of hostile computer code (software) used by cyber-attackers to compromise computer systems and information. Malware is becoming more sophisticated and capable on a constant basis. It can be used by attackers to take over computer systems (or entire networks), to access and exfiltrate private information, to cause systems to fail or be overwhelmed (denial of service), and many other things. Malware can enter computer systems and networks from many vectors including infected software applications, infected hardware appliances, infected user laptops/desktops/smart phones, email messages and attachments, malicious websites, infected documents, etc.

19. **Man-in-the-Middle attacks**: To perform man-in-the-middle (MitM) attacks, attackers secretly intercept messages from one party, change them, then send them on to the intended recipient. These attacks are easier to carry out if the attacker is on the same physical network as the target(s). MitM attacks are often a necessary element of multi-part attacks. For example, attackers might need to set up a MitM attack to exploit a vulnerability identified in an operating system, software application or cryptographic mechanism.

20. **Misconfiguration**: Devices and software applications have many settings that must be set correctly to be secure. Attackers can exploit vulnerabilities in systems that are not configured correctly to compromise them, much the same way they can exploit vulnerabilities in systems that have not been properly patched. In addition, networking equipment such as firewalls and routers must be correctly configured in order to work correctly and securely. Some tools and processes that are useful in maintaining secure configurations include checklists, peer review among system administrators and configuration security assessments.

21. **Patching/Updating/Upgrading:** Many security breaches occur because operating systems, software/firmware applications and computer/networking devices are not patched, updated or upgraded. Patches and updates/upgrades are used to repair vulnerabilities and to replace operating systems/software applications that are no longer supported by the vendor. To meet best practices guidance, organizations should monitor vendor and security websites for vulnerabilities and support discontinuations that affect the devices and software present on their networks. This is a tedious process to perform manually, so tools that aid in the process should be used whenever possible.

22. **Phishing:** Phishing is a type of social engineering mechanism in which attackers masquerade as some sort of trusted entity and lure people into performing an act (such as clicking on links) or revealing private information (such as user names and

passwords). Attackers often use email to mount phishing campaigns against organizations and individuals.

23. **Poodle Attacks:** Poodle attacks are man-in-the-middle attacks that exploit Internet and security software clients' fallback to the use of SSL 3.0. Weaknesses in this cryptographic mechanism allow successful attackers to read private information. SSL 3.0 and TLS 1 should be disabled on systems to prevent possible Poodle attacks.

24. **Ransomware Attacks:** Ransomware attacks take several forms, but basically cyber-attackers take control of an organizations private data (and sometimes whole computer systems) and demand payment from the owner to restore their systems to them. These kinds of attacks usually involve malware of one type or another. This malware is often introduced into the system by means of Phishing attacks.

24. **Remote Exploit:** Remote exploits are simply exploits that are performed from outside the local network used by an organization, such as from the Internet. These types of exploits are particularly dangerous as they can be carried out from foreign countries, making it difficult or impossible to prosecute the perpetrators or to recover intellectual property.

26. **Root Access:** Root access is a superuser account on computer systems that has complete control. Root is also known as admin or administrator access. Attackers that attain root access to the system can disable or change security mechanisms, add or subtract users from the system, change system logs or perform many other malicious activities on the system. System administrators commonly use the same password for simple network access and administrative access to the system. Attackers often gain access to root passwords by hacking into user-level systems, cracking the password hashes they find there and trying those passwords as root. This is why security professionals recommend that root / admin users should use different passwords for network and admin access and that root access to the system should be strictly monitored. Using multi-part authentication techniques can also be used to secure root access.

27. **Sniffing Attacks:** Sniffing attacks involve capturing, decoding, inspecting and interpreting the information inside network packets on TCP/IP networks. Attackers "sniff" network packets in order to gain access to private information such as passwords, system information and network details. Sniffing is a passive type of attack that is difficult to detect. This is the reason security professionals recommend that information should be transmitted securely across networks using encrypted protocols such as SSH.

28. **Social Engineering:** Social engineering is the practice of tricking, cajoling or intimidating people into performing actions, revealing information, allowing access to private areas or machines, etc. Social engineering attacks can be carried out in person, over the telephone, using email or over the Internet and are leading tools used by attackers to defeat defense mechanisms used by organizations to protect their private information and infrastructures.
29. **Unsupported Operating Systems and Software Applications:** See the patching / updating / upgrading section above.
30. **Vulnerabilities:** Vulnerabilities are flaws in application coding, operating systems, system configurations, network architectures or hardware devices that allow attackers to bypass security mechanisms, cause denial of service, gain access to private information or otherwise compromise the security of computer systems and networks.
31. **Watering Hole:** A watering hole is a website frequented by a particular interest group such as a profession or industry.
32. **Watering Hole Attacks:** A watering hole attack is an indirect type of attack. In a watering hole attack, attackers identify websites that are frequented by the group they are interested in and then infect those websites with malware in the hope of infecting machines employed by group members they are interested in.
33. **Zero Day Exploits:** Zero day exploits are mechanisms/methodologies used to exploit vulnerabilities that have not yet been identified by legitimate concerns such as vendors or security professionals. Attackers most often employ zero day exploits to attack high value or highly secured target systems. These exploits are very dangerous as they are generally immune to standard security systems such as anti-virus software or IDS/IPS. Zero day exploits are often employed by nation states or large cyber-criminal organizations since they are difficult to develop and very expensive to purchase.