E/15/280

Prematthilaka M.P.U

**Short Notes**

**a) Formjacking**

Fromjacking is stealing your privacy information, basically credit card details from payment forms by using a JavaScript code. In a commercial website when a customer submits their details through a forum malicious JavaScript code that has been injected there by the cybercriminals collects all entered information, such as payment card details and the user's name and address. Symantec data shows that 4,818 unique websites were compromised with formjacking code every month in 2018. According to Symantec, all companies and legal entities operating a website or payment transactions online are at risk to formjacking. To avoid formjacking script blocking extensions should be used in your web browsers. Some of the script blocking extensions are ScriptSafe, NoScript and JSBlocker. To avoid formjacking in a website it is needed to maintain a high level of regular auditing of the codes.

Formjacking is a new tool for a major improvement on how social engineering works, it is less hassle for the cybercriminals. The users themselves voluntarily surrender their information in a form they believe is legitimate and secure. Once the information is stolen, the threat actors now have the information of the user, useful for a future identity theft operation, bank fraud and other criminal activity where they start pretending as the person of the stolen information. The global statistics all of us are facing according to Symantec is the nasty situation that users are always at risk of losing their personally identifiable information to unknown third parties, thanks to formjacking. Since August 13, 2018, alone, Symantec has detected and blocked 248,000 formjacking incidents. The instances of formjacking attacks are estimated to increase, as it is very effective in capturing user information with the minimal set of efforts.

**b) Cryptojacking**

Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads cryptomining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser. The cryptomining code then works in the background as unsuspecting victims use their computers normally. The only sign they might notice is slower performance or lags in execution. The other method is to inject a script on a website or an ad that is delivered to multiple websites. Once victims visit the website or the infected ad pops up in their browsers, the script automatically executes. No code is stored on the victims' computers. Whichever method is used, the code runs complex mathematical problems on the victims' computers and sends the results to a server that the hacker controls.
In January 2018, researchers discovered the Smominru cryptomining botnet, which infected more than a half-million machines, mostly in Russia, India, and Taiwan. The botnet targeted Windows servers to mine Monero, and cybersecurity firm Proofpoint estimated that it had generated as much as $3.6 million in value as of the end of January. Cryptojacking doesn't even require significant technical skills. According to the report, The New Gold Rush Cryptocurrencies Are the New Frontier of Fraud, from Digital Shadows, cryptojacking kits are available on the dark web for as little as $30. The risk of being caught and identified is also much less than with ransomware. The cryptomining code runs surreptitiously and can go undetected for a long time. Once discovered, it's very hard to trace back to the source, and the victims have little incentive to do so since nothing was stolen or encrypted. Hackers tend to prefer anonymous cryptocurrencies like Monero and Zcash over the more popular Bitcoin because it is harder to track the illegal activity back to them.

**c) Ransomware**

Ransomware is a form of *malware* that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin. There are a number of vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer. By Norton internet security, it is advised not to pay for the ransom. Because it encourages and funds this attackers. To prevent ransomware,

- Reputable antivirus software and a firewall should be maintained on the computer
- Keep OS patched up and UpToDate
- Back up your files

Categories of Ransomware,

1. Encrypting Ransomware
   Encrypting Ransomware is ransomware that combines innovative encryption algorithms intended to block access to files requiring a ransom payment for file decryption. Examples of encrypting ransomware are “CryptoLocker”, “Locky”, CryptoWall” with the most recent being “WannaCrypt”.

2. Locker Ransomware
   Locker Ransomware is a type of malware that locks the target out of the operating system, consequently preventing access to the targets desktop, applications and files. An example of locker ransomware is the “Winlocker”.

A crypto-ransomware named “Locky” infiltrates a victims system through email camouflaged as an invoice with a conforming Microsoft Word document that is embedded with malicious [6] macros. These macros execute malware upon download. Generally macros are disabled by default in Microsoft Word; however enabling macros makes a system vulnerable to potential malicious code. Once a system is infected, the malware Locky searches for directly attached and network attached drives and encrypt files with a “.locky” extension leaving behind a ransom note for file decryption. Malicious Email Links - are URLs (Uniform Resource Locator) in the body of the email and are sent from supposedly trusted sources. Upon clicking these URLs, malicious files are download from the Internet infected the system and holding its files for ransom. The evolutions of malware attacks have simplified its execution consequently making any organization or individual a possible ransomware victim. Exploit Kits - Sophisticated toolkits that exploit vulnerabilities are defined as exploit kits which are executed when a victim visits a compromised website. Malvertisement are malicious code hidden frequently in an advertisement redirecting one to the exploit kit web page in an unobserved fashion. On an unprotected system, a drive-by download of a malicious payload will be executed thus infecting the system and holding its files for ransom. The present most destructive ransomware exploit kit is the “Wanna Cry” or “WannaCrypt” ransomware.

**d) Living off the Land, and Supply Chain attacks**

In the cyber security world, living off the land attacks describe those attacks that make use of tools already installed on targeted computers or attacks that run simple scripts and shellcode directly in memory. Attackers use these tactics because they hide in plain sight and create fewer

new files (or no new files) on the hard disk. There is less chance of being detected by traditional security tools and, ultimately, less risk of an attack being blocked.

"Living off the land" (LotL) style of attacks has made the malicious use of PowerShell a "staple" for cybercrimes, showcased by a 1,000% uptick of blocked malicious PowerShell scripts on the endpoint in 2018, according to Symantec's Internet Security Threat Report. Nearly half of malicious email attachments are Microsoft Office files. Hacker groups like Mealybug and Necurs leverage macros in Office files to "propagate malicious payloads" and experiment with XML files, according to the report. Supply chain attacks, where attackers can compromise a company through its use of third-party services, increased nearly 80% in 2018. Attackers exploit developers by hacking third-party libraries "that are integrated into larger software projects," according to Symantec.

**Here's how simple it is for an attacker to live off the land:**

1. A user visits a website using Firefox, perhaps driven there from a cleverly disguised spam message.
2. On this page, Flash is loaded. Flash is a common attack vector due to its seemingly never-ending set of vulnerabilities.
3. Flash invokes PowerShell, an OS tool that exists on every Windows machine, and feeds it instructions through the command line — all operating in memory.
4. PowerShell connects to a stealth command and control server, where it downloads a malicious PowerShell script that finds sensitive data and sends it to the attacker.

### e) The rise of Targeted Attacks

A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim's defenses.

Targeted attacks often employ similar methods found in traditional online threats such as malicious emails, compromised or malicious sites, exploits, and malware. Targeted attacks differ from traditional online threats in many ways:

- Targeted attacks are typically conducted as campaigns. APTs are often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target's network—and are thus not isolated incidents.
- They usually target specific industries such as businesses, government agencies, or political groups. Attackers often have long-term goals in mind, with motives that include, but are not limited to, political gain, monetary profit, or business data theft.

### f) Security Challenges of Cloud

Sometimes, we fail to save all of our data into our device system. We need another place to save them all or a few of them. To solve this problem, we use the cloud to store data. Both small and large companies and even individuals store data in the cloud. When we store data in the cloud, there could be few possible challenges to face. DDOS attack is one of the problems. Thereafter, user will not be able to access data. The next challenge is data breaching and data loss. If the cloud data base is not well protected data breaches could be occurred. And also, attacks can be executed. The next challenge would be insecure of access point. The main

advantage of cloud computing is we can access our data from anywhere while having an internet connection. Depending on the access point we use our data could be insecure. These are some of common cloud computing attacks.

- **Malware injection attack**: In the cloud system, as the client's request is executed based on authentication and authorization there is a huge possibility of Meta data exchange between the web server and web browser. An attacker can take advantage during this exchange of metadata. Either the adversary makes his own instance or the adversary may try to intrude with malicious code. In this case, either the injected malicious service or code appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping and deadlocks, which forces a legitimate user to wait until the completion of a job which was not generated by the user. This type of attack is also known as a meta-data spoofing attack.
- **Flooding attack problem**: In a cloud system, all the computational servers work in a service specific manner, with internal communication between them. Whenever a server is overloaded or has reached the threshold limit, it transfers some of its jobs to a nearest and similar service-specific server to offload itself. This sharing approach makes the cloud more efficient and faster executing requests. When an adversary has achieved the authorization to make a request to the cloud, then he/she can easily create bogus data and pose these requests to the cloud server. When processing these requests, the server first checks the authenticity of the requested jobs. Non-legitimate requests must be checked to determine their authenticity, but checking consumes CPU utilization, memory and engages the IaaS to a great extent, and as a result the server will offload its services to another server. Again, the same thing will occur and the adversary is successful in engaging the whole cloud system just by interrupting the usual processing of one server, in essence flooding the system.

**g) IoT attacks**

With the high use of IoT, there are some attacks aiming IoT. One is Botnet attack. A single IoT device infected with malware does not pose any real threat; it is a collection of them that can bring down anything. To perform a botnet attack, a hacker creates an army of bots by infecting them with malware and directs them to send thousands of requests per second to bring down the target. And also, IoT devices are highly vulnerable to malware attacks. They do not have the regular software security updates that a computer has. So they are quickly turned into infected zombies and used as weapons to send incredibly vast amounts of traffic.

These types of attacks tamper with the hardware components and are relatively harder to perform because it requires expensive material. Some examples are de-packaging of chip, layout reconstruction, micro-probing, and particle beam techniques. These attacks are based on "side channel Information" that can be retrieved from the encryption device that is neither the plaintext to be encrypted nor the ciphertext resulting from the encryption process. Encryption devices produce timing information that is easily measurable, radiation of various sorts, power consumption statistics, and more. Side channel attacks makes use of some or all of this information to recover the key the device is using. It is based on the fact that logic operations have physical characteristics that depend on the input data. Examples of side channel information are timing attacks, power analysis attacks, fault analysis attacks, electromagnetic attacks, environmental attacks. These attacks are focused on the ciphertext and they try to break the encryption, i.e. find the encryption key to obtain the plaintext. Examples of cryptanalysis attacks include Ciphertext-only attack, Known-plaintext attack, Chosen- plaintext attack, Man-in-the-middle attack, etc. Software Attacks are the major source of security vulnerabilities in any system.

Software attacks exploit implementation vulnerabilities in the system through its own communication interface.

**h) Election Interference 2018**

The United States Intelligence Community concluded in early 2018 that the Russian government was already attempting to influence the 2018 United States mid-term elections by generating discord through social media. Primaries for candidates of parties began in some states in March and would continue through September. The leaders of intelligence agencies have noted that Russia is spreading disinformation through fake social media accounts in order to divide American society and foster anti-Americanism

Just one month after Election Day had passed, the National Republican Congressional Committee (NRCC) confirmed its email system was hacked by an unknown third party in the run-up to the midterms. The hackers reportedly gained access to the email accounts of four senior NRCC aides and may have collected thousands of emails over the course of several months.