TIPS & TRICKS

Security Awareness Tips for the month

1. **If you handle personally identifiable information, make sure you understand the privacy laws and your organization's guidelines that protect it:** Personally Identifiable Information, or PII, is a protected subset of info that is considered sensitive & confidential. This info is what identity thieves search for to steal your identity. This data is almost always required to be secured by local privacy laws. If you are not clear about requirements for compliance regarding PII, or if you're not sure whether you deal with PII, you should contact your supervisor immediately. Proper protocols & technology must be in place to protect PII to include data loss prevention, encryption & various security controls.

2. **Be suspicious of people you don't know who ask for sensitive information:** "Social engineers" use lies & manipulation to trick people into giving away sensitive info, such as usernames, passwords & credit card numbers. Don't fall for it! Follow these best practices: always maintain a healthy sense of skepticism when dealing with unknown individuals, especially if they ask for any internal or sensitive information.

3. **Take special precautions to protect private, confidential & sensitive information:** Each document & email should be clearly classified based on its value & sensitivity level, such as public, private, or confidential. Your org's info management policy should define classifications used by the org. Appropriate protections should be defined for each classification level for documents when it is in storage, in transit, who it may be shared with encryption & its secure disposal.

4. **Help ensure your org's security by monitoring work environment & reporting breaches of policy, data protection, or security:** If you notice an unescorted visitor, escort them to the security guard. If you find sensitive documents, protect them & turn them into the concerned department. Close & lock emergency door that has been open & report to security department.

5. **Do not access workplace data on mobile devices unless authorized & necessary:** For purposes of mobile device security, you should only access workplace data on your mobile device when you are authorized to do so & it is necessary. You should follow your org's policy & always connect using a secure & encrypted connection. Additionally, any device that you use to access business network or workplace data should be approved for business use & meet minimum security requirements defined by IT department & your org's Bring Your Own Device (BYOD) policy.

6. **Disable location services for apps unless they are required for the app to work:** Many apps ask for permission to share your location. Hackers & others with malicious intent could use this info to compromise your online or physical security. Turn off location services for apps that do not require them to function.

7. **Review your credit card statements to verify all your transactions:** Suspicious activity on your credit card or bank account statements might go unnoticed at first. Often, identity thieves will test out an account with a small charge before stealing more. Look through your credit card statements carefully & contact your bank immediately if you notice any unauthorized charges, even if the transaction was later reversed. These charges may be a small as Rs. 1 & may be from a variety of online shopping venues. If the small charge is accepted, the criminal has a level of assurance that the card can be used for larger purchases.

Source

KNOWLEDGE ARTICLES

Executives Remain Weak Link in Cyber security Chain

Despite their high-ranking positions, senior executives are reportedly the weak link in corporate cyber security chain with a new report from The Bunker, which finds that cyber-criminals often target this known vulnerability.

A recently published white paper, found that those at the top are guilty of a bit of grandiosity. They disregard cyber security threats & policies under the misguided perception that the rules don't apply to their unique positions.

"Professional hackers & adversaries will usually do a thorough investigation into a senior executive or board level director, including full analysis which could entail in-depth monitoring of the company website & associated social media accounts," the report said.

Most executives make the same five mistakes, according to the report. Senior executives fail to realize that they are prime targets for cybercriminals, which is potentially a result of their view that cyber security is an IT responsibility that doesn't have anything to do with their executive positions.

In reality, though, the report said, "IT security has now become the remit of all individuals, especially those in the highest positions of each department & senior executives need to take ownership for IT security best practice in their day-to-day behavior."

Another common mistake among senior executives is that they believe cyber security threats are attacks that happen to the business by some external malicious actor rather than being the result of internal threats or accidents.

Many top executives also reportedly believe that a cloud provider is responsible for the backup and security of all info, though they fail to use cloud hosted email securely.

However, cybercriminals know that top executives often have privileged access to company information, so hackers intentionally target their personal accounts.

"Reviewing corporate policies, with a focus on people, premises, processes, systems & suppliers will provide valuable insights into which areas to improve & by championing a 'security first' corporate culture, organizations & their senior executives will be well positioned to avoid the high financial costs, reputational damage & unexpected downtime that could result from a cyber-attack or data breach," said Phil Bindley, managing director, at The Bunker.

Source

NEWS & ALERTS

GandCrab ransom ware and Ursnif virus spreading via MS Word macros

Security researchers have discovered two separate malware campaigns, one of which is distributing the Ursnif data-stealing Trojan & the GandCrab ransom ware in the wild, whereas the second one is only infecting victims with Ursnif malware.

Though both malware campaigns appear to be a work of two separate cybercriminal groups, we find many similarities in them. Both attacks start from phishing emails containing an attached Microsoft Word document embedded with malicious macros & then use PowerShell to deliver file less malware.

Ursnif is a data-stealing malware that typically steals sensitive information from compromised computers with an ability to harvest banking credentials, browsing activities, collect keystrokes, system & process info, & deploy additional backdoors.

Discovered earlier last year, GandCrab is a widespread ransom ware threat that, like every other ransom ware in the market, encrypts files on an infected system and insists victims to pay a ransom in digital currency to unlock them. Its developers ask payments primarily in DASH, which is more complex to track.

MS Docs + VBS macros = Ursnif & GandCrab Infection

The first malware campaign distributing two malware threats was discovered by security researchers at Carbon Black who located approximately 180 variants of MS Word documents in the wild that target users with malicious VBS macros.

If successfully executed, the malicious VBS macro runs a PowerShell script, which then uses a series of techniques to download & execute both Ursnif & GandCrab on the targeted systems.

MS Docs + VBS macros = Ursnif Data-Stealing Malware

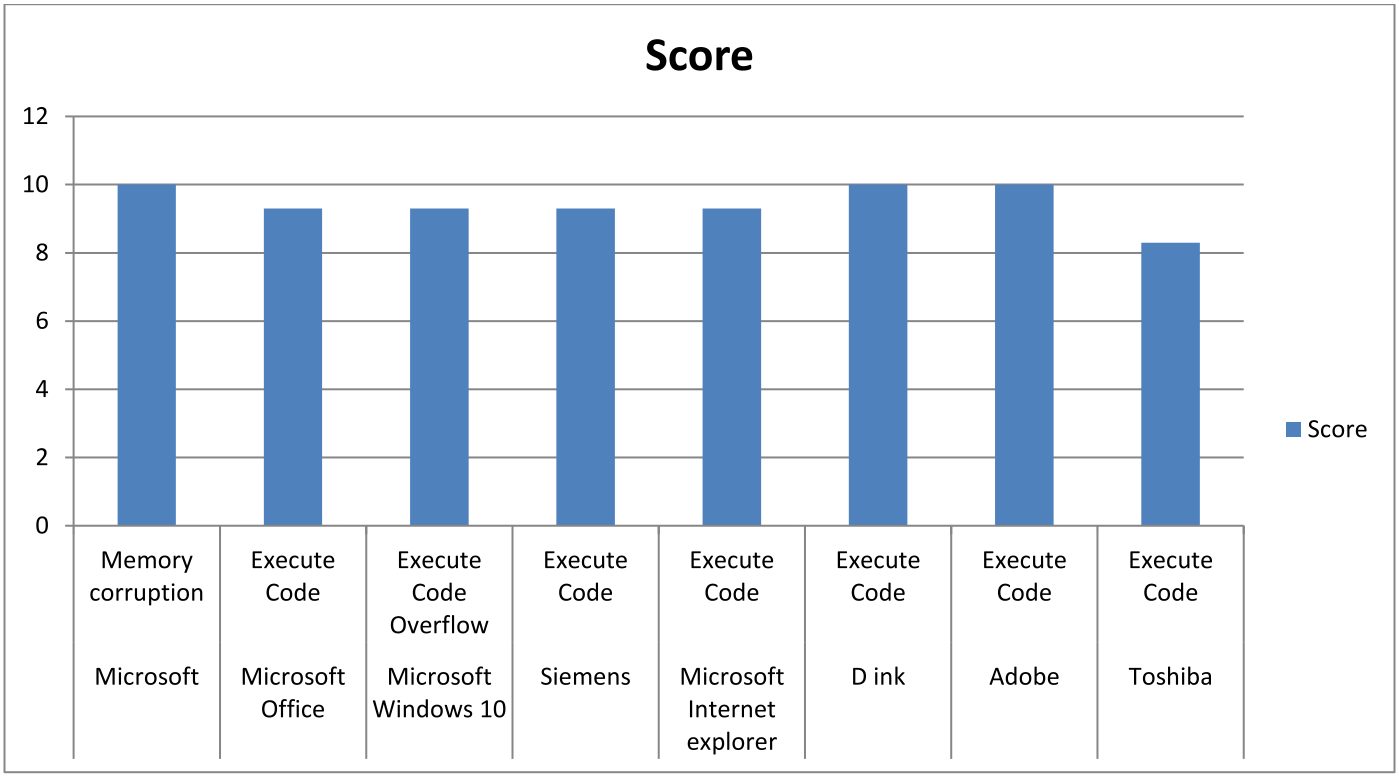
Similarly, the second malware campaign that was spotted by security researchers at Cisco Talos leverages a Microsoft Word document containing a malicious VBA macro to deliver another variant of same Ursnif malware. This malware attack also compromises targeted systems in multiple stages, starting from phishing emails to running malicious PowerShell commands to gain file less persistence & then downloading & installing Ursnif data-stealing computer virus.

Once executed on the victim computer, the malware collects information from the system, puts into a CAB file format, & then sends it to its command-and-control server over HTTPS secure connection.

Talos researchers have published a list of indicators of compromise (IOCs), along with the names of payload file names dropped on compromised machines, on their blog post that can help you detect & stop the Ursnif malware before it infects your network.

Source

VULNERABILITIES IN LIMELIGHT


Score
Memory corruption
Microsoft
Execute Code
Microsoft Office
Execute Code Overflow
Microsoft Windows 10
Execute Code
Siemens
Execute Code
Microsoft Internet explorer
Execute Code
D ink
Execute Code
Adobe
Execute Code
Toshiba
Score