THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

14 November 2014

Purpose
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

November 12, USA Today – (National) **Post office suspends telecommuting due to breach.** The U.S. Postal Service announced November 12 that it has shut down its secure virtual private network (VPN) and suspended all telecommuting for employees at its Washington, D.C. headquarters until further notice following a breach of its employee database that compromised information of over 800,000 workers. Source: http://www.usatoday.com/story/tech/2014/11/12/us-postal-service-suspends-telecommuting-breach-vpn/18915317/

November 12, WTNH 8 New Haven – (Connecticut) **Coast Guard contractor pleads guilty to stealing personal information.** A Pawcatuck man who ran a computer repair business and also worked as a contractor for the U.S. Coast Guard pleaded guilty November 12 to stealing personal information and data over 250 times from computers and other devices brought to him for repairs. Source: http://wtnh.com/2014/11/12/coast-guard-contractor-pleads-guilty-to-stealing-personal-information/

U.S. government warns on bug in Apple's iOS software

Reuters, 13 Nov 2014: The U.S. government warned iPhone and iPad users on Thursday to be on the alert for hackers who may exploit a vulnerability in Apple Inc's (AAPL.O) iOS operating system that would enable them to steal sensitive data. There was the potential for hacks using a newly identified technique known as the "Masque Attack," the government said in an online bulletin from the National Cybersecurity and Communications Integration Center and the U.S. Computer Emergency Readiness Teams. The network security company, FireEye Inc (FEYE.O), disclosed the vulnerability behind the "Masque Attack" earlier this week, saying it had been exploited to launch a campaign dubbed "WireLurker" and that more attacks could follow. [ID:L2N0T01H2] Hackers could potentially steal login credentials, access sensitive data stored on iOS devices and remotely monitor activity on those devices, the government said. Such attacks could be avoided if iPad and iPhone users only installed apps from Apple's App Store or from their own organizations, it said. Users should not click "Install" from pop-ups when surfing the web. If iOS flashes a warning that says "Untrusted App Developer," users should click on "Don't Trust" and immediately uninstall the app, the bulletin said. To read more click **HERE**

Default ATM passcodes still exploited by crooks

SoftPedia, 14 Nov 2014: Once again, ATMs have been "hacked" by individuals taking advantage of default, factory-set passcodes. This time the passcode hasn't been guessed, or ended up online for everyone to know because it was printed in the ATM's service manual - the individual who, with the help of an accomplice, managed to cash out $400,000 in 18 months was a former employee of the company that operated the kiosk ATMs they targeted. Tennessee-based Khaled Abdel Fattah had insider knowledge of the code that, when typed in, set the machines into Operator Mode, which allowed him and accomplice Chris Folad to reconfigure the ATM to dispense $20 bills when asked for $1 dollar ones. They would do this, then ask the machine to dispense, for example, $20, and they would get away with $400. After this, they would revert back the change so that the theft would go unnoticed. And it took 18 months for this to happen - the owner of one the businesses where one of these kiosk ATMs was set up noted that there was a problem when the machine was running out of money. What ultimately led the

Secret Service to the two fraudsters was the fact that their faces were captured by surveillance cameras and they used their own debit cards to make withdrawals. They also stuck to a rather limited set of ATMs, all located in Nashville. According to Wired, both men have been charged with 30 counts of computer fraud and conspiracy. This is not the first time that ATM heists like this happened. Around 2005, service manuals of ATMs manufactured by Tranax and Trident ended up online, and contained the passcodes that allowed anyone to access their Operator Mode. Street crooks began taking advantage of the fact, but it took over 18 months for the wider public to discover it. This forced the ATM vendors in question to make it mandatory for operators to change this default password when installing the machine. To read more click HERE

Facebook updates terms and policies, introduces interactive privacy guides

Heise Security, 14 November 2014. Facebook continues with its plan to make the social network's privacy settings easier to understand, and has introduced Privacy Basics. Private Basics is a page where users can go through a number of interactive guides that explain things like what others see about you, how to block other users, what to do if your account has been hacked, and so on. In short, this is the place where the most commonly asked questions about Facebook use are answered in a way that can be understood by all. Depending on the language you set on you Facebook account, you might see the information in your own language (the information is available in 36 languages). "We're also proposing updates to our terms, data policy, and cookies policy," Erin Egan, Facebook Chief Privacy Officer shared in a post. "We're updating our policies to explain how we get location information depending on the features you decide to use." Other changes have also been added, and some policies apparently simplified. If you are a Facebook user, I urge you to peruse the changes and to offer comments - if you have any. You should know what Facebook does with your information and how it tracks you online, so that you can make an informed choice about using (or stop using) the social network. The deadline is November 20. To read more click HERE

Best practices for government agencies to secure IT infrastructure

Heise Security, 14 Nov 2014: Many government agencies, departments, subcontractors, service providers, and organizations that operate IT systems on behalf of the government must ensure protection of their critical infrastructure and ensure data security and continuous systems operation. These requirements are documented in various international and national standards, regulations and statutes established by authorities and covered by best practices frameworks such as COBIT, NIST800-53, ISO/IEC 27001, ISO/IEC 15408 and ITIL. They demand that government agencies secure and protect the confidentiality, integrity, and availability of information systems and the data processed, stored, or transmitted by them. Staying compliant with these regulations is a question of reputation for a wide range of organizations including data clearinghouses, state departments, military subcontractors, and private vendors if their data is exchanged directly with government systems. Failure to meet the regulations may lead to direct and indirect financial losses and exclusion from operating within certain industries. To meet compliance requirements and ensure the security of IT infrastructure, government IT professionals should consider the following recommendations:

- Establish control over users and their activities. A large part of data security requirements lies within access control, account management, and separation of duties. In fact, today these are some of the cornerstones of any security policy, established in response to the dramatic increase in security incidents or as a part of compliance efforts. In order to avoid critical issues such as internal misuse of information systems, it is important to monitor user activity, ensure that permissions are granted to users on a need-to-know basis, and implement continuous tracking of modifications made to user accounts.
- Gain complete visibility and accountability with audit reports. Responding to compliance regulations, organizations may be required to submit reports with various levels of detail for an arbitrary period, proving effective implementation of security controls and adherence to enacted

policies. However, because it is extremely impractical to collect, consolidate, and correlate data manually on configurations, security settings, and activities in databases, file servers, and virtual environments manually, a change-auditing solution will notify you of all changes across all IT systems and provide comprehensive custom reports.

- Monitor and evaluate your environment. Being compliant in many aspects means being sure that security policies and procedures are functioning properly and are helping with risk reduction. Having your IT infrastructure constantly audited validates that you have complete visibility across all your IT systems and proves that your IT environment is under permanent control.Control access and modifications to shared resources. When it comes to data stored in critical systems such as SQL, file servers, and SharePoint, it is necessary to know who did what, when, and where. Consider deploying a solution that will provide you with a detailed view, including before and after values, on any attempt to access, modify, or delete sensitive data.

To read more click HERE

Tor Exit Node Used to Deliver New Malware Family OnionDuke

Softpedia, 14 Nov 2014: A malicious exit server in the anonymity network Tor has been found to distribute a new family of malware researchers dubbed OnionDuke because of its connection to the group behind the cyber-espionage tool MiniDuke. This type of attack is an uncommon one and has been discovered by Josh Pitts, penetration tester at Leviathan Security. He found that the bad exit node would modify the uncompressed binaries passing through it by repackaging them and adding a malicious executable in the process; this method would help the attacker bypass integrity checks associated with the original file. Security researchers at F-Secure studied this new malware distribution technique and confirmed the information presented by Pitts, offering details about how the payload was executed, its communication with the command and control (C&C) server and the embedded functionality. They found that as soon as the binary downloaded through the bad Tor server is launched, it executes both the original executable and the second one, which is a malware dropper. This action would not raise any suspicions to the victim since the legitimate software component is added to the system. Artturi Lehtiö analyzed the behavior of the dropper and noticed that it contained an encrypted DLL posing as a GIF image. After decrypting the DLL, the dropper would store it on the disk and execute it. The chain of malicious activities continues with decrypting configuration file and trying to connect to a hard-coded C&C server that would deliver further instructions to the malware. Several OnionDuke components have been identified during the analysis, revealing its capabilities. Stealing credentials is on the list of intended purposes for the malware, and in order to achieve persistence on the affected system, the author added routines for detecting the presence of security products (antivirus, firewall). It was in one of these components that the researchers found the connection between OnionDuke and MiniDuke, which consisted in a C&C domain that was registered in 2011 under the alias John Kasai and was used for registering others two weeks later, employed by the espionage tool. According to the researcher, there is evidence that OnionDuke has been used in targeted attacks against European government agencies. Downloading non-encrypted executable files through Tor is a risky action because the identity of the exit node is not known; Lehtiö suggests using a VPN connection that would encrypt the connection end-to end. To read more click HERE

Unused IP Addresses Are Hijacked by Spammers through Technical Loophole

Softpedia, 14 Nov 2014: A weakness in the way some countries manage the IP address ranges assigned to Internet Service Providers (ISPs) and hosting providers has been abused by spammers, who have hijacked them for nefarious activities. The scam can be achieved by setting up businesses pretending to be an ISP or a host service provider and claiming the unused address space assigned to the legitimate authorities administering the IPs. If no complaint is shot their way, the crooks can use the addresses as they like. This way, cybercriminals pass as the authority that has been allocated the respective addresses; the service taking over the addresses does not necessarily have to be fake, as legitimate

organizations can also dabble with this sort of activity. Security blogger Brian Krebs has been tracking the activity of a spammer who admitted to sending junk email via two hosting providers in Bulgaria, Mega-Spred and Kandi EOOD. According to Krebs, the two entities "commandeered tens of thousands of Internet addresses from ISPs around the globe, including Brazil, China, India, Japan, Mexico, South Africa, Taiwan and Vietnam." His investigation revealed that Mega Spred had been hijacking IP address spaces from all over the world since late August this year. The problem stems from the fact that regional Internet registry (RIR) authorities do not verify the authenticity of an ownership claim from a network operator over an IP range and simply accept it. A graver issue is that the RIR that blindly accepts the claim also passes the fake information to databases that are used for checking the validity of an IP route. As such, the parties doing this basically make the verification based on fake data. RIPE NCC (Réseaux IP Européens Network Coordination Centre) is the RIR that supervises the allocation and registration of IPs for service providers in Europe, the Middle East, and some countries in Central Asia. However, in a statement on the matter emailed to Krebs, the authority said that it could not "verify the routing information entered into Internet Routing Registries or monitor the accuracy of the route objects," although they are the ones accepting the claims and the routing records from the fraudulent network operators in the first place. On the other hand, RIPE provides Resource Certification (RPKI) service as a solution for network operators to protect against IP hijacking. This permits requesting of a digital certificate with the IP resources an operator has. Thus, other parties can verify if a resource is used by the legitimate holder or not. To read more click **HERE**