THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

31 October 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

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

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

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

Ferguson Prosecutor: Twitter Account Hacked

Huffington Post, 30 Oct 2014: A Twitter account that claimed to have details about the grand jury investigation of police officer Darren Wilson was hacked, a prosecutor's investigation found on Thursday. In early October, someone operating the account @thesusannichols claimed to know a member of the grand jury and said the jury hadn't found enough evidence to "warrant an arrest" of Wilson in connection with the August shooting of 18-year-old Michael Brown in Ferguson, Missouri. After the tweet was posted, the office of St. Louis County Prosecutor Robert McCulloch opened an investigation. While not offering details on how his office determined that someone had hacked the Twitter account, McCulloch said in a statement on Thursday that the account "had, indeed, been hacked," but added that they didn't know who actually wrote the tweet in question. "A tweet several weeks ago claimed the author talked to a friend who is serving on the [grand jury] about the case. That did not happen," McCulloch said. "An investigation revealed that the account had, indeed, been hacked and the origin/author of the tweet is unknown. The owner of the account has no connection with any member of the grand jury." The Missouri woman who originally owned the account told CNN after the original tweet was posted that the Twitter account "had to have been hacked." The account was later changed to a different name and then deleted, and someone else took over the original Twitter handle. McCulloch also said that there had not been leaks from members of the grand jury and that whoever was releasing "piecemeal" information connected to the case "is doing a great disservice to the grand jury process." To read more click HERE

RIG Exploit Kit Used in Drupal CMS Exploit Incidents

Softpedia, 31 Oct 2014: The public disclosure of a critical SQL injection vulnerability affecting all builds of Drupal 7, save for the last one, gave way to increased cybercriminal activity leveraging the RIG Exploit Kit to compromise website visitors through drive-by download attacks. The bad actors would rely on a simple redirect method via an iframe injected into the code of the site, no traffic distribution system (TDS) being involved; thus, the URL in the iframe pointed straight at the landing page of the exploit kit, which would scan for unpatched versions of Java, Silverlight and Flash Player, and leverage them to add malware to the system. RiskIQ, a company providing website scanning and navigation solutions for malware detection, has observed that many of the Drupal sites compromised through the SQL injection attack redirected to RIG Exploit Kit. According to the data collected by the company systems, all instances of the malicious toolkit are hosted on a machine (46.182.30.198) part of the server fleet of Russian datacenter operator Selectel. Among the websites hit by the cybercriminals are advertise.com, typepad.com, homestead.com (web hosting company also affected) and popsci.com (Popular Science). RiskIQ says that Selectel is regularly used for criminal online activities by crooks in Eastern Europe. Most of the domains hosting the exploit kit contain the “corrosion” string, with different variations and top-level domains (.COM, .NET, .ORG). Checking some of them in Google Chrome shows that they are already blacklisted for containing malware. Drupal made a public service announcement on Wednesday, seeding panic among website administrators by saying that all websites that have not been updated within seven hours after the release of the patch for the code injection security slip-up (CVE-2014-3704) should be assumed compromised. Sounding the alarm was not unfounded, though, because multiple companies offering security solutions for websites recorded a massive wave of attacks the day of the disclosure, October 15. One recommendation from Drupal developers for administrators who did not hurry to apply the patch is to rebuild the site from scratch, since a compromised asset remains under the control of the unauthorized third-parties even if the latest Drupal update is applied. In the more optimistic scenario where a backup made before October 15 is available, the maintainers of the CMS advise taking the website offline, restoring the backup and patching Drupal before releasing the site online again. Trying to remove backdoors planted by the attackers is not recommended because the operation has low chances of rendering the website completely clean. To read more click HERE

All Unpatched Drupal 7 Versions Should Be Assumed Compromised

SoftPedia, 30 Oct 2014: All websites running version 7 of Drupal CMS (content management system) that have not been updated to build 7.32 shortly after the disclosure of a highly critical SQL vulnerability on October 15 should be considered hacked, a security advisory from Drupal alerts. Administrators of Drupal websites should have been on high alert at the middle of the month and should apply the patch released by the CMS developers in a new version of the product. The security glitch, tracked as CVE-2014-3704, allows a potential attacker to execute arbitrary commands remotely without authentication, by sending specially crafted SQL requests, which can lead to complete compromise of the website; the issue is extremely serious because there may be no trace of the incident. Ironically, the exploit leverages an API designed to sanitize SQL queries and prevent this type of incident. Drupal developers issued a public service announcement on Wednesday, informing that automated attacks taking advantage of this flaw were recorded just hours after the public disclosure. “You should proceed under the assumption that every Drupal 7 website was compromised unless updated or patched before Oct 15th, 11pm UTC, that is 7 hours after the announcement,” the advisory says. Statistics show that more than 400,000 websites run on Drupal. According to data published by w3techs on October 30, 1.9% of all the websites online rely on Drupal, and 1.3% of them run version 7 of the CMS; of these, only 8.2% are updated to build 7.32. Because of its low complexity, the glitch is considered highly critical and multiple security companies announced at the time that some of their clients had been compromised. Sucuri detected incidents in the wild taking advantage of the weakness about eight hours after the public disclosure. Volexity observed wide spread scanning of websites that could be taken over, even on those running a different CMS product. The company also noticed activity from IP addresses associated with APT groups. Proof-of-concept code soon emerged in the public space, allowing an even easier deployment of an attack. Drupal says that a compromised website updating to the latest build of the CMS is not off the hook and backdoors still remain on the site. Patching does not remove any of the malicious files already uploaded by the cybercriminals, it just closes the bug that allowed the attack. It appears that in some cases the cybercriminals would apply the patch themselves, after having gained control of the website; the reason behind this would be to keep other bad actors from achieving administrative privileges on the asset. On the same note, crooks know that hosting providers often take the responsibility of updating the website software themselves. Patching the site after taking control increases the chances of the compromise passing unnoticed. Cleaning the websites of all the backdoors that may have been planted by the bad actors is a highly difficult task and does not guarantee that all access point elements are found. This is why the Drupal security team recommends either rebuilding from scratch or restoring a backup of the site taken before October 15, the day the vulnerability was disclosed. The Drupal security team recommends taking offline the potentially affected website and alerting the server administrator of the potential risk to other assets hosted there. Restoring a backup copy of the website, applying the latest patch and putting the site back online are the next steps to take. Everything imported from the potentially hacked site (code, files) should be closely verified to make sure that no backdoors are passed to the safe configuration. To read more click HERE

Malicious Code Served at Popular Science Website

SoftPedia, 30 Oct 2014: Users visiting the Popular Science website have been targeted with a drive-by download attack that relied on RIG Exploit Kit (EK) to deliver malicious files to their computers. The cybercriminals managed to inject code in the website that would redirect visitors to an online location hosting the EK. Usually, such browser-based crimeware scan for vulnerable plug-ins (Flash, Silverlight or Java) and then leverage a weakness in them to download malware. However, in this case, security researchers from Websense observed that the EK first checked the target system for the presence of certain antivirus software and proceeded with the plug-in exploitation only if none of the products on its list were encountered. In order to do this, the cybercriminals leverage another vulnerability, this time in the XMLDOM ActiveX control in Windows 8.1 and lower, which also allows enumeration of local resources. Abel Toro of Websense says that this tactic has begun to become integrated more often in exploit kits, being present in versions of Nuclear Pack and Angler EKs as well. Another particularity is that no TDS (traffic distribution system) is employed and the malicious iframe injected into the code of Popular Science site leads straight to RIG EK’s landing page. In his analysis of the attack, Toro observed that the landing page for the exploit kit was highly obfuscated. This is a common tactic used by cybercriminals to make security researchers’ job more difficult. Patching plug-ins sooner rather than later is always a good idea Keeping the browsers updated and relying on the most recent versions of browser plug-ins is an easy way to stay protected against this type of attacks. Concocting an exploit for a vulnerability takes some time, and except for zero-day vulnerabilities, developers provide a patch long before the cybercriminals manage to find a way to leverage the weakness. This would give users plenty of time to apply the patch. On the other hand, cyber crooks in the higher tiers of the organized crime may benefit from incredible resources and come up with an exploit in a very short amount of time. This was the case of the recently updated Adobe Reader, which saw exploits for the fixed vulnerabilities being used in the wild a week after the developer pushed the patch. Speculation has it that a skilled reverse engineer analyzed the update code and found a way to construct an exploit. Another theory says that the malicious individuals somehow received relevant information. To read more click HERE

Humans are largely the problem in cyber security failures

Phys Org, 31 Oct 2014: When people think about cyber and information security they often think about anti-virus software and firewalls; however, according to an information security expert from the University of Adelaide, organisations would become a lot more secure if employers invested in more security-related training for staff. Dr Malcolm Pattison says until recently, research into information security (electronic and physical data security) focused on computers, software, data communications and policies, and while these are important, the human aspect was largely overlooked. "While high-quality hardware and software plays a critical role in the security of an organisation, there is now a growing body of research that suggests the behaviours of computer users can be one of the biggest threats to an organisation's information security," says Dr Pattinson, a research fellow in the University of Adelaide's Business School. "For example, the best password processed by the most sophisticated software, using the latest in computer facilities becomes useless when the password is written on a sticky note and stuck on a monitor for easy access. "Humans are a major problem. What we think, what we know, what we do, how we do it and why we do it are perhaps the key to attaining and maintaining an acceptable level of information and cyber security in an organisation," he says. Dr Pattinson says security breaches don't just happen at computers - staff also need to be conscious of storage and disposal of physical documents. "Information security usually refers to digital data security; however, it also refers to physical data security," Dr Pattinson says. "Many organisations provide secure bins for confidential documents to be shredded but it's still up to individuals to dispose of material correctly." Dr Pattinson says the good news is that staff training can be a lot more affordable than purchasing the latest hardware and software, and there are a few key behavioural changes that would make an organisation considerably more secure. "Small changes like locking a computer when someone leaves their desk; not using public wifi on work computers and mobile devices; keeping passwords secret; correctly disposing of documents; and reporting any unidentifiable visitors can lead to a safer workplace," he says. To read more click HERE

The security threat of unsanctioned file sharing

Heise Security, 31 Oct 2014: Organisational leadership is failing to respond to the escalating risk of ungoverned file sharing practices among their employees, and employees routinely breach IT policies and place company data in jeopardy, say the results of the “Breaking Bad: The Risk of Unsecure File Sharing” report by Intralinks Holdings and Ponemon Institute. The research found that file sharing poses a major threat to enterprise security, and that senior managers at organisations are having difficulty setting and enforcing effective policies to safeguard against data leakage. The report concludes that many organisations are vulnerable to both data loss and non-compliance due to cloud file sharing and improper file sharing practices – and it starts from the top down. Further, it is clear that the enterprise IT department has lost control of user application decision-making, as well as of company data. More than 1,000 IT security professionals from the United States, United Kingdom, and Germany were surveyed. Key findings from the report include:

- Almost half (49 percent) of respondents believe their company lacks clear visibility into employees’ use of file sharing/file sync and share applications.
- Half of respondents (51 percent) aren’t convinced their organisations have the ability to manage and control user access to sensitive documents and how they are shared.
- The majority of organisations have policies governing the use of file sharing, but policies are not being communicated to employees effectively.
- Only 54 percent of respondents say their IT department is involved in the adoption of new technologies for end users, including cloud-based services.
- More sobering, approximately 61 percent of respondents confessed that they have “often or frequently” done the following:
- Accidentally forwarded files or documents to individuals not authorised to see them.
- Used their personal file-sharing/file sync-and-share apps in the workplace.
- Shared files through unencrypted email.
- Failed to delete confidential documents or files as required by policies.

These file-sharing issues are making enterprises extremely vulnerable to data loss and compliance violations. This vulnerability is heightened for regulated industries like financial services, where the risks and repercussions of data loss are more severe. The research also showed that employees are acting badly when it comes to data sharing and collaboration, routinely violating IT policy in order to get things done faster. Survey respondents indicated a lack of senior-level accountability in their organisations for developing and implementing file-sharing policies. Of senior level respondents, 44% did not believe they had the ability to manage and control user access to sensitive documents and how they are shared. Among respondents who do have that ability, their confidence in asserting it was mixed.“Data leakage and loss from negligent file sharing is now just as significant a risk as data theft,” noted Larry Ponemon, chairman of the Ponemon Institute. “While most companies take steps to protect themselves from hacking and other malicious activities, this report shows that these same organisations are entirely unprepared to guard against risky and ungoverned file sharing using consumer-grade applications like Dropbox. To read more click HERE