THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

8 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

133 DDoS attacks over 100Gbps so far in 2014

Heise Security, 8 Oct 2014: Arbor Networks released global DDoS attack data for Q3 2014 showing a remarkable increase in Simple Service Discovery Protocol (SSDP) reflection attacks. Arbor monitored very few attacks using SSDP as a reflection mechanism in Q2, but nearly 30,000 attacks with this source port in Q3 alone, with one such attack reaching 124Gbps. The data confirms what Arbor has called The Hockey Stick Era, with a continuing trend towards large volumetric attacks, a consistent theme throughout 2014. Key findings:

- Significant growth in use of SSDP for reflection attacks in Q3; 4% of all attacks and 42% of all attacks greater than 10Gbps appeared to use SSDP reflection in Q3.
- NTP reflection attacks still significant, but continuing to fall away proportionally (post the Q1 storm); however, over 50% of all attacks greater than 100Gbps were still NTP reflection attacks.
- Very large volumetric attacks far more frequent than in the past, with 133 attacks over 100Gbps this year so far.
- Average monitored attack in Q3 was 858.98Mbps; peak attack of 264.6Gbps.
- Q3 saw 16.5% of all attacks above 1Gbps, up from 15.3% in Q2.
- Proportion of events lasting less than 1 hour is gradually increasing, now at 91.2%
- Ranking sources for events larger than 10Gbps: U.S. (7.6%), China (5.9%), Brazil (1.1%)
- Ranking destinations for events larger than 10Gbps: U.S. (17.6%), France (10.8%), Denmark (8.4%)

"Everyone is aware of the huge storm of NTP reflection DDoS attacks in Q1 and early Q2, but although NTP reflection is still significant there isn't as much going on now as there was – unfortunately, it is looking more and more like SSDP will be the next protocol to be exploited in this way. Organizations should take heed and ensure that their DDoS defense is multi-layered, and designed to deal with both attacks that can saturate their connectivity, and more stealthy, sophisticated application layer attacks," said Arbor Networks Director of Solutions Architects Darren Anstee. Arbor's data is gathered through ATLAS, a collaborative partnership with nearly 300 service provider customers who share anonymous traffic data with Arbor in order to deliver an aggregated view of global traffic and threats. ATLAS collects statistics that represent 90Tbps of Internet traffic and provides the data for the Digital Attack Map, a visualization of global attack traffic created in collaboration with Google Ideas. To read more click **HERE**

BYOD Policy Guidebook

Heise Security, 8 Oct 2014: This policy guidebook (link) was created to help guide you through the questions to ask and provide some best practices to consider when establishing your own BYOD policies. Your employees want to use their own mobile devices for work. This represents a tremendous opportunity for you to extend the benefits of mobile technology to all employees. As more companies embrace the Bring Your Own Device (BYOD) model, many questions arise. To read more click **HERE**

Every fifth Android user faces cyber attacks

Heise Security, 7 Oct 2014: A total of 1,000,000 Android device users around the world encountered dangerous software between August 2013 and July 2014, according to the results of a survey carried out by Kaspersky Lab and INTERPOL. In fact, this period was the peak of cyber attacks registered in recent years. The most popular malicious programs are SMS Trojans that send messages to premium rate numbers without the owner's awareness. Users in Russia, India, Kazakhstan, Vietnam, Ukraine and Germany are among the main targets for cyber attacks targeting Android. Mostly this is because people in these countries often pay for content and online services via SMS; for cybercriminals it is an attractive way to monetize malicious attacks because they can use these services to quickly and anonymously transfer money from prepaid mobile accounts to third-party bank accounts. The main reason for the increase in the number of attacks and attacked users was the use of Trojan-SMS family programs. These accounted for 57.08% of all detections made by Kaspersky Lab security solutions for Android-based devices. Second came RiskTool (21.52% positives), conditionally legitimate programs which can, however, be used for malicious purposes (sending SMS notifications of paid messages, transmitting geo-data, etc.). Applications with aggressive advertising (pop-ups, notifications in the status bar, etc.) were in third place (7.37%). "We often hear experts saying that Android users have nothing to worry about, that although malicious programs for this system appear regularly, the number of attacks is not significant. Until recently, that could be regarded as a fair comment. However, the situation has changed dramatically over the last year – and not for the better", said Roman Unuchek, senior virus analyst at Kaspersky Lab. However, it cannot be concluded that the threat landscape for Android-based devices was entirely pessimistic during the reporting period. In April 2014, Kaspersky Lab experts noted a serious decline in the total number of attacks that happened, mostly due to a serious drop in the number of Trojan-SMS attacks. This may have been the result of new rules for the services paid via SMS introduced by Russia's telecoms regulator. Now all Russian operators must be sent a confirmation message from any subscriber who is trying to pay for services via SMS. Since July 2014 the number of attacks has started increasing once more, it is possible that the new legislation contributed to the fall in April, indirectly confirming the effectiveness of legislation against cyber-fraud. "INTERPOL and Kaspersky Lab have produced a report highlighting the currents threats and trends picked up over the course of 2013 and 2014. This report again underlines that cybercrime is not exclusively a new form of crime. What we see here is the model and structure of traditional organized crime encapsulated in a technologically advanced form", - said Dr. Madan Oberoi, Director of Cyber Innovation & Outreach at INTERPOL To read more click **HERE**

UPDATED - Final smart grid interoperability standards guide released by NIST

Fierce Government IT, 6 Oct 2014: The smart grid essentially integrates automated, two-way digital communication technology to better monitor and measure the electrical delivery system and address issues. An advanced grid would automatically heal from power disruptions and better protect it from cyber attacks. According to an Oct. 1 press release from NIST, the most recent document (link), which sought public input earlier this year, includes several new developments such as:

- Addressing the deployment of synchrophasors, which help engineers monitor the electrical flow along the grid to better maintain stability and efficiency.
- Incorporating seven new standards that support interoperability bringing the total to 74 standards and protocols.
- Updating the reference architecture model to reflect the increasing significance of so-called "distributed energy resources" that include non-traditional power sources such as customer-owned solar and wind systems. The model is also more in line with a similar European one.
- Discussing the role of cybersecurity of other critical infrastructures as well as other new security developments and publications.
- Expanding the dialogue on testing and certification as industry reaches agreement on the underlying smart grid standards.

NIST also published a revision to its Guidelines for Smart Grid Cybersecurity, an update of the original 2010 version. This updated document includes new sections describing the relationship of smart grid cybersecurity to the NIST Cybersecurity Framework, cyber-physical attacks, testing and certification, and regulatory changes involving privacy. To read more click **HERE**

Apple updates definitions to prevent "iWorm" botnet malware on Macs

Heise Security, 6 Oct 2014: In case you missed it over the weekend, MacRumors reports that Apple has updated OS X's built-in XProtect malware definitions list to include the Mac.BackDoor.iWorm malware we reported on late last week. The iWorm malware allegedly managed to infect more than 17,000 Macs worldwide, and it was apparently using a (now closed) Minecraftserverlists board on reddit to distribute the IP addresses of control servers to infected Macs. XProtect was first introduced to OS X in Snow Leopard in response to the MacDefender malware that managed to infect some OS X systems back in 2011. While the complete list is only 40 items long as of this writing, OS X silently checks for XProtect updates daily, and Apple also uses the list to mandate the usage of up-to-date versions of Java and Flash. While XProtect doesn't do anything to clean existing infections, it can prevent new ones by telling users explicitly that they're attempting to install known malware. To read more click **HERE**

AT&T Employee Breaches Customer Account Privacy Policy

Softpedia, 7 Oct 2014: AT&T mobile carrier announced that it had to deal with an inside breach that resulted in personal customer information being exposed to an unauthorized individual. The incident did not occur as a result of a cyber-attack, but because a company employee violated the privacy and security guidelines imposed for accessing information about customers. Without having any authorization to do so, the employee accessed account details that included social security numbers and driver's license number. Phone call details have also been accessed. In a letter to the affected customers, AT&T director of finance billing operation, Michael Chiaramonte, explained that apart from these details, the individual also viewed the Customer Proprietary Network Information (CPNI). CPNI contains details about the telecommunication services purchased from the company. At first, it may not sound like much, but this actually refers to the numbers a customer calls, along with other information accompanying them, such as duration of the conversation, time and date. Based on this information, mobile carriers issue the phone bill. As such, the AT&T employee had access to all the details included in the list of charges. AT&T offers one year of free credit monitoring. Among the steps taken by the company to address the issue was terminating the contract of the employee who caused the incident. Furthermore, the mobile carrier informs that if unauthorized changes or charges occur to an affected account, these would be reversed. A greater danger is posed by the exposure of the clients' social security number, which could lead to identity theft. Because personally identifiable information was accessed and potentially copied, according to Vermont's Security Breach Notice Act, companies have a duty to notify consumers of a security breach. The organizations also have to send to the Attorney General a copy of the letter addressed to its customers. AT&T recommends its customers to increase the security of their account by locking it with a password. If a countersign already protects access to the account, then the recommendation is to change it. Also as a precaution, it is advisable to contact major credit reporting entities and place a fraud alert on the credit report. To read more click **HERE**

Largest US Bond Insurer Suffers Major Data Leak

Softpedia, 8 Oct 2014: Sensitive information about customers has been inadvertently leaked online by MBIA Inc, resulting in search engines indexing the data. The mistake leading to the incident was a misconfigured security setting in an Oracle Reports database server. As a result, the information became public and search engines were quick at indexing customer account numbers, balances, dividends, account holder names, and even instructions on how to authorize new bank accounts for deposits. According to security blogger Brian Krebs, who notified MBIA of the incident, Google included in its results about 230 pages containing such information. The leak was discovered by independent security expert Bryan Selly at Seely Security, who found the sensitive details through a search engine. In a conversation with Krebs,

Seely said that the poorly configured server also exposed a reports diagnostics page, which contained credentials for accessing almost all customer account data stored on the machine. MBIA, formerly known as the Municipal Bond Insurance Association, is a financial services company that provides municipal bond insurance, investment management products and consulting services. "Malicious hackers finding dozens of universities or companies with Social Security numbers, health data or other information is devastating, but stumbling on bank accounts and the instructions for how to empty them is potentially catastrophic," Seely told Krebs. Data touching on multiple investment pools has been exposed, including Texas CLASS, the Louisiana Asset Management Pool, the New Hampshire Public Deposit Investment Pool, Connecticut CLASS Plus, and the Town of Richmond, NH. "Billions in taxpayer funds, invested into one of the largest institutions in the world that were essentially being guarded by a sleeping security guard," commented Seely. The organization said in a statement that an investigation was initiated to determine the cause of the leak and the necessary measures that need to be applied to protect the customer data and improve security of the systems. At the moment, the vulnerable server has been taken offline, but there is no information about the measures taken by Google to remove access to the sensitive documents from web search results. For a period of time, content indexed by Google can still be accessed from a cached copy of the original. After a while, the cached content is removed from the data center and can no longer be accessed. Alternatively, the owner of the content can issue a request for Google to remove the cached copy of the original content. To read more click **HERE**