THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

12 June 2014

Tool for creating booby-trapped PDFs made public

Heise Security, 12 Jun 2014: Freelance security researcher Claes Spett has made available a tool he dubbed "PDF Exploit Generator," which allows penetration testers - but also malicious attackers - to create a booby-trapped PDF in a matter of minutes. "The tool weaves existing exploits into PDFs, allowing attacks against Adobe Reader and Acrobat versions 8.x prior to 8.2.1 and 9.x before 9.3.1," Darren Pauli explained. "Users can insert their own URL pointers into the program, which then spits out an exploited PDF." The exploits used are old, and most - if not all - security solutions will detect them. Still, there are many users who don't use any, and they could be successfully targeted. Spett has apparently created the tool while developing an exploit kit aimed to be used by penetration testers. Users are advised to use the PDF Exploit Generator responsibly, but of course, nothing can prevent malicious attackers from using it, too. To read more click HERE

Automatic updating of Android apps becomes riskier

Heise Security, 12 Jun 2014: Google has made unwelcome changes to the way new app permissions are disclosed to users: no warnings will be shown if a new permission if is in the same category as an old one that has previously been accepted. The change has been introduced with the recently released new version of the Play store app, and has apparently made to streamline the installing of updates and to avoid confusing users. With this update, a user who has previously permitted an app to access the device's coarse GPS location will not be notified when the new version of the app starts collecting information about the device's fine location, as both permissions belong to the same category. Similarly, an app that initially only had the permission to read the call log could now be updated to initiate phone calls without the user's knowledge. Or if it originally was permitted to read the contents of the SD card, it can be updated to write to it. Find out more about the different permission groups here. "Unfortunately, most groups contain at least one 'innocent' or common permission that many apps on the Store use next to some more nasty ones," noted a software developer that goes by the online handle "Tubeman," who created an app named Permission Tester to test for this "latest Google security screw up." If you are not comfortable with this new change, you can prevent it by turning off auto-updates for specific apps by opening the Play Store app, touching the app's icon, selecting "My Apps", selecting the app, and unchecking the box next to "Auto-update" in the Menu. A 2nd "improvement" announced by Google makes the "full Internet access" permission disappear from the primary permissions screen and get automatically approved. "These days, apps typically access the Internet," Google explained, and says that Google Play's app review systems already check all apps for abuse of these access permissions. To read more click HERE

Home Articles P.F. Chang's Breach: Link to Target?

GovInfoSecurity, 12 Jun 2014: Restaurant chain P.F. Chang's China Bistro continues to investigate an apparent payments breach and subsequent payment card fraud. But several security experts and cyber-intelligence researchers say they believe the chain suffered a malware attack similar to those that compromised the point-of-sale networks of U.S. retailers Target Corp., Neiman Marcus and Sally Beauty Holdings Corp.. Other experts, however, say it's too soon to tell what the cause of the latest breach was, and whether it was linked to any previous breaches. But while the experts disagree about the details of this latest alleged breach, they agree it's time for retailers to tighten network security. "It's really

got the retail industry up in arms," says financial fraud expert Avivah Litan, an analyst at the consultancy Gartner. "CISOs are scared of getting fired, they are afraid of the consumer reaction and they're just trying to get handle on all of this." The high-profile nature of the recent card compromises is putting more emphasis on retail network security, Litan adds. "No one even depends on PCI compliance anymore for security," Litan says. "Everyone realizes it's not working. Retailers want card data out of their network, so these attacks really have promoted greater security. And I think you will see a lot of retailers moving to point-to-point encryption and tokenization as a result." P.F. Chang's says it's working with authorities to learn more about the nature of the apparent breach and subsequent fraud that has been reported at several of its locations nationwide (see P.F. Chang's Investigating Card Breach). Simon Eappariello, senior vice president at iboss Network Security, says it's too early to say with certainty what may have happened at P.F. Chang's. But based on the what's known so far, it appears that malware infected the chain's POS network in a way that resembles what has been seen in other retail attacks, he says. "The fact that multiple locations are implicated would suggest that either a central point on the network was infiltrated and then used to exfiltrate data from a central database, or was used as an internal attack point to spread malware to POS equipment at the branch locations," Eappariello says. "It's also possible their network was compromised some time ago and then access to their network was sold on the digital underground market to someone looking to exploit this type of data - possibly even an insider targeted attack." Litan says the apparent P.F. Chang's attack seems to be based on the same variations of BlackPOS malware used in many of the recent retail attacks reported over the last year. She reaches that conclusion because the cards allegedly tied to P.F. Chang's apparently have cropped up for sale in the same underground forum where cards breached through Target and Sally were sold. Card numbers connected to P.F. Chang's reportedly appeared this week in a black-market carding forum run by a hacker known as Rescator - where hackers also posted numbers linked to purchases at Target and Sally Beauty, according to security blogger Brian Krebs (see Sally Beauty Breach: Link to Target?). To read more click **HERE**

Advanced cyber-attacks rely on privileged credential exploitation

Heise Security, 12 Jun 2014: While new and sophisticated malware variants were continually developed to exploit systems in 2013, criminals, hacktivists and advanced attacks continue to do the most damage by exploiting privileged accounts. CyberSheath's analysis of 10 of 2013's most notable cyber-attacks found that privileged accounts were on each attacker's critical path to success 100 percent of the time, regardless of the perimeter attack vector. The research uncovered that increased visibility and actionable intelligence on privileged accounts within an organization's IT environment greatly increased the ability for those organizations to successfully detect and disrupt an attack. Looking closely at the advanced attack patterns leveraged in 10 benchmark breaches reveals that the theft, misuse, and exploitation of privileged accounts is a critical step in attack methodology. Key takeaways for CISOs include:

- The attacks that matter to business exploit privileged accounts 100 percent of the time.
- Big company or small, organizations have more privileged accounts than they know about and the risk of exposure they represent makes them urgent priorities.
- Protecting privileged accounts gives CISOs an opportunity to quantify risk reduction and deliver results that can be measured.
- Privileged accounts represent a clear case for providing a return on investment and reduce risk.
- Protecting privileged accounts is an opportunity to become a challenging target and take back ground in the fight against advanced threats.
- Automated privileged account security solutions reduce human error, overhead and operational costs.

"Companies of all sizes today face an unprecedented number of cyber-attacks from organized, patient and well-funded groups," said Eric Noonan, CEO, CyberSheath. We're starting to see CISO's shift from band aid point-solution purchases to integrated technologies built on intelligence-gathering features to combat advanced threats." To read more click **HERE**

Microsoft Releases 2 Critical Updates, Patches 59 IE Holes

Dark Reading, 11 Jun 2014: Patch Tuesday resolved 66 vulnerabilities in all, including two that had already been publicly disclosed without patches. Microsoft released seven security bulletins yesterday including a massive critical Internet Explorer update that patches 59 vulnerabilities, two of which were already publicly disclosed without patches. Two of the bulletins were categorized as critical (five as important) and three cover vulnerabilities that allow for remote code execution. In all, Microsoft patched 66 unique common vulnerabilities and exposures in Microsoft Windows, Office, Internet Explorer, Live Meeting, Lync, and Lync Server. To Microsoft's knowledge, none of the vulnerabilities are being exploited in the wild at this time. Many of the vulnerabilities patched yesterday are less important to users who adhere to principle of "least privilege." "Customers should apply all of the security updates provided in the June 2014 security bulletin release and note the updates for Word and Internet Explorer as the top deployment priorities for this month," says Dustin Childs, group manager of Microsoft Trustworthy Computing. "While there are a number of things being addressed this time around, it's important to note that, to our knowledge, none of these now-addressed CVEs have caused any customer impact to date." The big update is MS14-035, a cumulative security update for Internet Explorer. In addition to 58 other vulnerabilities, it resolves a memory corruption vulnerability in IE8, disclosed by Tipping Point May 21 after Microsoft missed the 180-day deadline Tipping Point had set. Microsoft says that exploit code is likely to be written for the vast majority of these vulnerabilities. "MS14-035 is the bulletin you have been looking for," says Marc Maiffret, CTO of BeyondTrust. "In short, Internet Explorer was broken every which way today. There are a significant number of Internet Explorer code execution and related vulnerabilities patched by this bulletin. Essentially if you [are] running Internet Explorer 6 through 11, you are vulnerable." According to Microsoft: The most severe of these [IE] vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Maiffret says: By default Internet Explorer runs code in low-integrity mode which means when it is exploited an attacker can do less with a system," says Maiffret. "There are three different vulnerabilities fixed here though that allow an attacker to go from low-integrity to medium-integrity; or basically to run code as the user of Internet Explorer. This is another great reminder of the need to implement least-privilege so that even when an attacker breaks out of Internet Explores low privilege modes they are still not obtain Administrator without a fight. Jeff Davis, vice president of engineering at Quarri Technologies, says: Browsers are always going to have new zero day vulnerabilities pop up every now and again. It makes using a browser feel like a lower-stakes game of Russian Roulette -- is today the day your fully-patched browser gets exploited? Security conscious individuals and organizations need extra layers of protection to keep their machines safe from these attacks. For example, you could run your browser in a virtual machine that you roll back after each session, use a separate device (like a Chromebook) for web surfing, or run a third-party secure browser product. MS-035 also includes updates to IE's XSS Filter to block more cross-site scripting attacks. The other critical update released yesterday is MS14-036, which addresses vulnerabilities in the Microsoft Graphics Component used in Windows, Office, and Lync, that could allow remote code execution if a user opens a specially crafted file or web page. Maiffret continued: MS14-036 brings back even more fun with GDI+. GDI+ is a graphics device interface for Windows and a reoccurring pain point from a vulnerability perspective. Part of the challenge is because GDI+ vulnerabilities tend to affect multiple Microsoft products, including in this case base operating systems and Microsoft Office. Good news again here for those running Office 2013; it is not affected. But the bad news is as mentioned this also affects base OS components which in this case is every supported OS version from Microsoft. And not to pile on further bad news but Microsoft also suggest exploit code is likely. Chris Goettl, product manager at Shavlik, says: This vulnerability is triggered when users open a specially crafted website or file, which means a phishing campaign is involved. If you look at the affected software list, GDI+ is a component you will see repeatedly. It's a very common core graphics component and its widespread nature throughout the Windows ecosystem is what makes this vulnerability critical, in spite of the mitigating factors, which

include reducing user rights below admin level and encouraging users to avoid clicking on links or open files that may be linked to a phishing attack. There is one other patch that addresses remote code execution vulnerability, but it is only classified as "important" (not critical), since it only applies to Microsoft Word in Office 2007. Although Microsoft only calls it "important," Maiffret describes it as "a critical vulnerability for Microsoft Word that you likely will see active exploits for. The good news though is that the latest major release versions of Word, such as included with Office 2013, are not affected." "This is a great reminder that sometimes when budgeting and thinking about security it is not simply about buying some new protection appliance but making sure your organization has migrated from things like Office 2007 to Office 2013, etc." Yesterday's patches also resolve vulnerabilities in Lync Server and Microsoft XML Core Services that could enable information disclosure; one in the Windows TCP protocol that could allow denial of service, and; one in the Remote Desktop Protocol that could allow tampering if the attacker gains access to the same network segment as the targeted system during a RDP session. To read more click **HERE**