Daily Threat Intelligence Briefing

sage DATA SECURITY

News from Wednesday, December 6, 2017. Reported on Thursday, December 7, 2017.

Links to the articles highlighted in **blue** can be found in the footnotes. To use the link, copy and paste it into your browser, replace "**" with "tt" and remove the brackets around www[.].

Source	Article
US-CERT	**Apple Releases Security Updates[1]** Apple has released security updates to address vulnerabilities in multiple products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. US-CERT encourages users and administrators to review Apple security pages for the following products and apply the necessary updates: • iOS 11.2 • macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan • tvOS 11.2 • watchOS 4.2 **Google Releases Security Update for Chrome[2]** Google has released Chrome version 63.0.3239.84 for Windows, Mac, and Linux. This version addresses vulnerabilities that an attacker could exploit to take control of an affected system. US-CERT encourages users and administrators to review the Chrome Releases[3] page and apply the necessary update.
BankInfo Security Enews	**Researchers: Andromeda Bust Collared Cybercrime Mastermind[4]** • Global Takedown Spearheaded by FBI and Europol Disrupts Massive Botnet • Police say they have disrupted the long-running Andromeda botnet, aka Gamarue, which has been tied to a massive number of malware attacks, including ransomware campaigns. • An international police operation resulted in the seizure of servers and domains used to spread and control Andromeda malware as well as the arrest of an unnamed individual in Belarus who's been accused of being tied to the botnet. • The EU's law enforcement intelligence agency, Europol, on Monday said that 1,500 command-and-control and malware-distribution domains tied to Andromeda had been sinkholed, meaning they were rerouted to police-controlled servers. Microsoft, which assisted in the takedown, along with security firm ESET, said that in the first 48 hours of the sinkholing, approximately 2 million unique IP addresses - each an Andromeda-infected PC - from 223 countries were detected. **Insider Allegedly Steals Mental Health Data of 28,000 Patients[5]** • The alleged theft of mental health information on more than 28,000 patients in Texas, which went undetected for well over a year, is yet another reminder of the substantial risks that terminated employees can pose as well as the need to take extra steps to protect the most sensitive patient information. • The Center for Health Care Services, a provider of mental health services and substance abuse treatment based in San Antonio, Texas, is notifying 28,434 patients whose data was apparently stolen when a former employee allegedly took the information after he was fired in 2016. • The breach at the San Antonio clinic is the latest incident spotlighting the risks posed by fired employees and other insiders. Last week, the Department of Health and Human Services' Office for Civil Rights issued an alert reminding covered entities and business associates of the serious security and privacy risks that terminated employees can pose and offering advice for mitigating those risks. • **Among the advice offered by OCR, as well as privacy and security experts, is for organizations to quickly end employees' electronic and physical access to data when they leave their jobs for any reason.**

[1] h**ps://www[.]us-cert.gov/ncas/current-activity/2017/12/06/Apple-Releases-Security-Updates

[2] h**ps://www[.]us-cert.gov/ncas/current-activity/2017/12/06/Google-Releases-Security-Update-Chrome

[3] h**ps://chromereleases.googleblog.com/2017/12/stable-channel-update-for-desktop.html

[4] h**ps://www[.]bankinfosecurity.com/researchers-andromeda-bust-collared-cybercrime-mastermind-a-10515

[5] h**ps://www[.]healthcareinfosecurity.com/insider-allegedly-steals-mental-health-data-28000-patients-a-10517

Source	Article
	• Some privacy and security experts say the recently revealed incident at the San Antonio clinic is also a reminder of the importance of safeguarding patient's most sensitive health data, such as mental health, substance abuse and HIV status information. • "**Healthcare organizations' infosec programs should include data classification**," says Kate Borten, president of The Marblehead Group consultancy. "**In terms of confidentiality, all PHI is confidential. But mental health and other types of PHI should be treated as highly confidential and deserving of more rigorous security controls.**"
Various	**Updates address vulnerabilities in Apache Struts versions 2.5 to 2.5.14**[6] • A pair of security updates released by the Apache Software Foundation patch vulnerabilities in Apache Struts versions 2.5 to 2.5.14 that would let a remote attacker take control of a system, according to a US-CERT alert[7]. **How the Major Intel ME Firmware Flaw Lets Attackers Get 'God Mode' on a Machine**[8] • Researchers at Black Hat Europe today revealed how a buffer overflow they discovered in the chip's firmware can be abused to take control of a machine - even when it's turned 'off.' • A recently discovered and now patched vulnerability in Intel microprocessors could be used by an attacker to burrow deep inside a machine and control processes and access data - even when a laptop, workstation, or server is powered down. • Researchers who discovered the flaw went public today at Black Hat Europe in London with details of their finding, a stack buffer overflow bug in the Intel Management Engine (ME) 11 system that's found in most Intel chips shipped since 2015. ME, which contains its own operating system, is a system efficiency feature that runs during startup and while the computer is on or asleep, and handles much of the communications between the processor and external devices. • **An attacker would need physical, local access to a victim's machine to pull off the hack, which would give him or her so-called "god mode" control over the system**, according to Positive Technologies security researchers Mark Ermolov and Maxim Goryachy, who found the flaw. **"Process Doppelgänging" Attack Works on All Windows Versions**[9] • At the Black Hat Europe 2017 security conference in London, two security researchers from cyber-security firm enSilo have described a new code injection technique called "Process Doppelgänging." • This new attack works on all Windows versions and researchers say it bypasses most of today's major security products. • Researchers say malicious code that utilizes Process Doppelgänging is never saved to disk (fileless attack), which makes it invisible to all major security products. • Researchers successfully tested their attack on products from Kaspersky, Bitdefender, ESET, Symantec, McAfee, Norton, Windows Defender, AVG, Sophos, Trend Micro, Avast, and Panda. Furthermore, even advanced forensics tools such as Volatility will not detect it. • Everything looks OK to security products because the malicious process will look legitimate, and will be mapped correctly to an image file on disk, just like any legit process. There will be no "unmapped code," which is usually what security products look for. • The good news is that "there are a lot of technical challenges" in making Process Doppelgänging work, and attackers need to know "a lot of undocumented details on process creation." • The bad news is that the attack "cannot be patched since it exploits fundamental features and the core design of the process loading mechanism in Windows." • Process Doppelgänging now joins the list of new attack methods discovered in the past year that are hard to detect and mitigate for modern AVs, such as Atom Bombing, GhostHook, and PROPagate.

[6] h**ps://www[.]scmagazine.com/updates-address-vulnerabilities-in-apache-struts-versions-25-to-2514/article/712037/

[7] h**ps://www[.]us-cert.gov/ncas/current-activity/2017/12/04/Apache-Software-Foundation-Releases-Security-Updates

[8] h**ps://www[.]darkreading.com/vulnerabilities---threats/how-the-major-intel-me-firmware-flaw-lets-attackers-get-god-mode-on-a-machine/d/d-id/1330565

[9] h**ps://www[.]bleepingcomputer.com/news/security/-process-doppelg-nging-attack-works-on-all-windows-versions/

Source	Article
	Nearly 2/3 of Industrial Companies Lack Security[10] • A new Honeywell survey shows more than half of industrial sector organizations have suffered cyberattacks. The survey also shows that industrial sector networks are still playing catch-up in cybersecurity. • While more than half of the 130 decision-makers from industrial organizations in the survey say they work in a facility that has suffered a breach, just 37% of the respondents say their organizations monitor networks for suspicious activity and traffic. • Nearly half, 45%, say they don't have an enterprise leader for cybersecurity, and one-fifth are not employing risk assessments on a regular basis.
NIST	**NIST Seeks Comments on Draft Two of the Cybersecurity Framework Version 1.1** • NIST has published the second draft of the proposed update to the Framework for Improving Critical Infrastructure Cybersecurity[11] (a.k.a., draft 2 of Cybersecurity Framework version 1.1). This second draft update aims to clarify, refine and enhance the Cybersecurity Framework, amplifying its value and making it easier to use. The new draft reflects comments received to date, including those from a public review process launched in January 2017 and a workshop in May 2017. • Public comments for draft 2 of Cybersecurity Framework version 1.1 and the draft Roadmap are due to NIST by 11:59 p.m. on Friday, January 19, 2018, via cyberframework@nist.gov. NIST anticipates finalizing Cybersecurity Framework version 1.1 in the spring of 2018. • More Information is available on the Fact Sheet[12].
Wired	**'Mailsploit' Lets Hackers Forge Perfect Email Spoofs[13]** Pretending to be someone you're not in an email has never been quite hard enough—hence phishing, that eternal scourge of internet security. But now one researcher has dug up a new collection of bugs in email programs that in many cases strip away even the existing, imperfect protections against email impersonation, allowing anyone to undetectably spoof a message with no hint at all to the recipient. On Tuesday, security researcher and programmer Sabri Haddouche revealed Mailsploit, an array of methods for spoofing email in more than a dozen common email clients, including Apple Mail for iOS and macOS, Mozilla's Thunderbird, Microsoft Mail, and Outlook 2016, as well as a long list of less common clients including Opera Mail, Airmail, Spark, Guerrilla Mail and Aol Mail. By combining the bugs in those email clients with quirks in how operating systems handle certain kinds of text, Haddouche was able to craft email headers that, to the recipient, give every indication of having been sent from whatever address the fraudster chooses. The potential for phishing schemes is enormous. A demo Haddouche has made available on his website describing the Mailsploit attack[14] lets anyone send emails from any address they choose; think potus@whitehouse.gov, tcook@apple.com, john.podesta@gmail.com or any other corporate executive, politician, friend, family member, or associate that might trick someone into giving up their secrets. Thanks to Mailsploit's tricks, no amount of scrutiny in the email client can reveal the fakery. Email spoofing is a hacker trick as old as email itself. But over the years, administrators of email servers have increasingly adopted authentication systems, most recently one known as Domain-based Message Authentication, Reporting and Conformance, which blocks spoofed emails by carefully filtering out those whose headers pretend to come from a different source than the server that sent them. Partly as a result, phishers today generally have to use fake domains—the part of the email address after the "@"—that resemble real ones, or cram real-looking domains into the "name" field of their email. Either case is fairly easy to spot, if you're careful to hover over or click on the "from" field of any suspicious-looking email.

[10] h**ps://www[.]darkreading.com/risk/nearly-2-3-of-industrial-companies-lack-security-monitoring/d/d-id/1330570

[11] h**ps://www[.]nist.gov/cybersecurity-framework/cybersecurity-framework-draft-version-11

[12] h**ps://www[.]nist.gov/sites/default/files/documents/2017/12/05/fact_sheet_framework1.1_and_roadmap_12_5_2017.pdf

[13] h**ps://www[.]wired.com/story/mailsploit-lets-hackers-forge-perfect-email-spoofs/

[14] h**ps://www[.]mailsploit.com/index

Source	Article
	But Mailsploit's tricks defeat DMARC by exploiting how email servers handle text data differently than desktop and mobile operating systems. By crafting email headers to take advantage of flawed implementation of a 25-year-old system for coding ASCII characters in email headers known as RFC-1342, and the idiosyncrasies of how Windows, Android, iOS, and macOS handle text, Haddouche has shown that he can trick email servers into reading email headers one way, while email client programs read them differently. Haddouche says he contacted all of the affected firms months ago to warn them about the vulnerabilities he's found. Yahoo Mail, Protonmail and Hushmail have already fixed their bugs, while Apple and Microsoft have told Haddouche they're working on a fix, he says. A **Microsoft spokesperson wrote to WIRED to note that Outlook.com, Office 365, and Exchange 2016 aren't affected by the attack.** Most other affected services haven't responded, Haddouche says. Haddouche's full list of affected email clients and their responses to his Mailsploit research is here[15]. And in the meantime, it's always wise to treat emails with caution. Before opening an attachment or even clicking a link, it's worth reaching out to the person via another channel for confirmation the message comes from who it claims to come from. And if you do get a message from potus@whitehouse.gov, don't give him your PayPal password.

[15] h**ps://docs.google.com/spreadsheets/d/1jkb_ZybbAoUA43K902lL-sB7c1HMQ78-fhQ8nowJCQk/htmlview?sle=true#gid=0