kindred

Security Newsletter

19 February 2018

Subscribe to this newsletter

Destructive Malware Wreaks Havoc at PyeongChang 2018 Winter Olympics

Destructive malware intent on sabotaging PCs is to blame for the IT problems reported during the PyeongChang 2018 Winter Olympics opening ceremony. The issues, first reported on Friday by UK paper The Guardian, consisted of failing Internet and television systems for on-site journalists attending and reporting the opening ceremony. While initially, Olympics organizers were quiet, officials finally admitted on Sunday that the IT failures were no accident and their network has been the victim of a malicious and coordinated cyber-attack.

According to Cisco researchers, attackers deployed a never-before-seen malware strain that was intent on data destruction and data destruction only. "The destructive nature of this malware aims to render the machine unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment. This is something we have witnessed previously with BadRabbit and Nyetya," Mercer and Rascagneres added.

Cisco published an initial analysis (now updated) of this threat, revealing that Olympic Destroyer was capable of mangling a computer's data recovery procedures and deleting crucial Windows services, rendering Windows computers unable to boot. According to the Windows Defender team, Olympic Destroyer appears to have been deployed via one of the NSA exploits leaked by the Shadow Brokers last year —namely EternalRomance.

Read More

Even More

Attack more complex than previously thought

Facebook wants you to install a VPN app accused of spying on users

Facebook has begun releasing a controversial app for its Android and iPhone (iOS) users which is a free VPN program from Onavo, an Israeli company bought by Facebook in October 2013, which promises to protect users' browsing data. However, the program is accused of monitoring user traffic and tracking the major competitors of Mark Zuckerberg's company.

Sccording to the report, is that Onavo collects data on what apps users are using and how much they are using them. This helps Facebook spot emerging trends to hedge its M&A bets, the report said, but could be a problem for privacy-conscious users.

Some tens of millions of people have already installed the Onavo app, the report said, and many might not know exactly what information it collects. Privacy-conscious professionals, especially those that work from their phone or may have a competitive product to Facebook, should seriously consider ditching the app and finding a new VPN client.

Read More

Even More

One in Three SOC Analysts Now Job-Hunting

Landing a job as an entry-level security operations center (SOC) analyst often provides a foot in the door to the cybersecurity field, but a new survey shows the more seasoned a SOC staffer gets, the more likely he or she will become disillusioned with the position.

New data from the Cyentia Institute's "Voice of the Analyst Study" of security operations center teams shows that while three in four SOC analysts are satisfied with their jobs, some 45% say the reality of the SOC isn't what they had expected. Some 70% of entry-level (one- to two years' experience) SOC analysts say their job meets their expectations, while just 43% of more experienced SOC analysts say so, according to the report, commissioned by SOC automation vendor Respond Software.

SOC analysts say they were drawn to their positions for a new challenge, skills, more money, and as a way to make a difference, but those same incentives also are what's drawing them to leave their current jobs, according to the report. "If you want to keep them around, offering those same positives in-house is just as important as eliminating the negatives that drive them out," the report says. "Roughly 3 out of 4 point to a desire for more intellectually challenging work, the chance to learn new skills, and/or a chance to defend and help the business."

Read More

Cryptomining script poisons government websites – What to do

We saw a pretty big event take place over the weekend where a 3rd party provider was compromised and their JS library was altered. The alteration introduced a crypto mining script that was then subsequently included on over 4,000 websites that I know of, many of which were UK/AU Government websites.

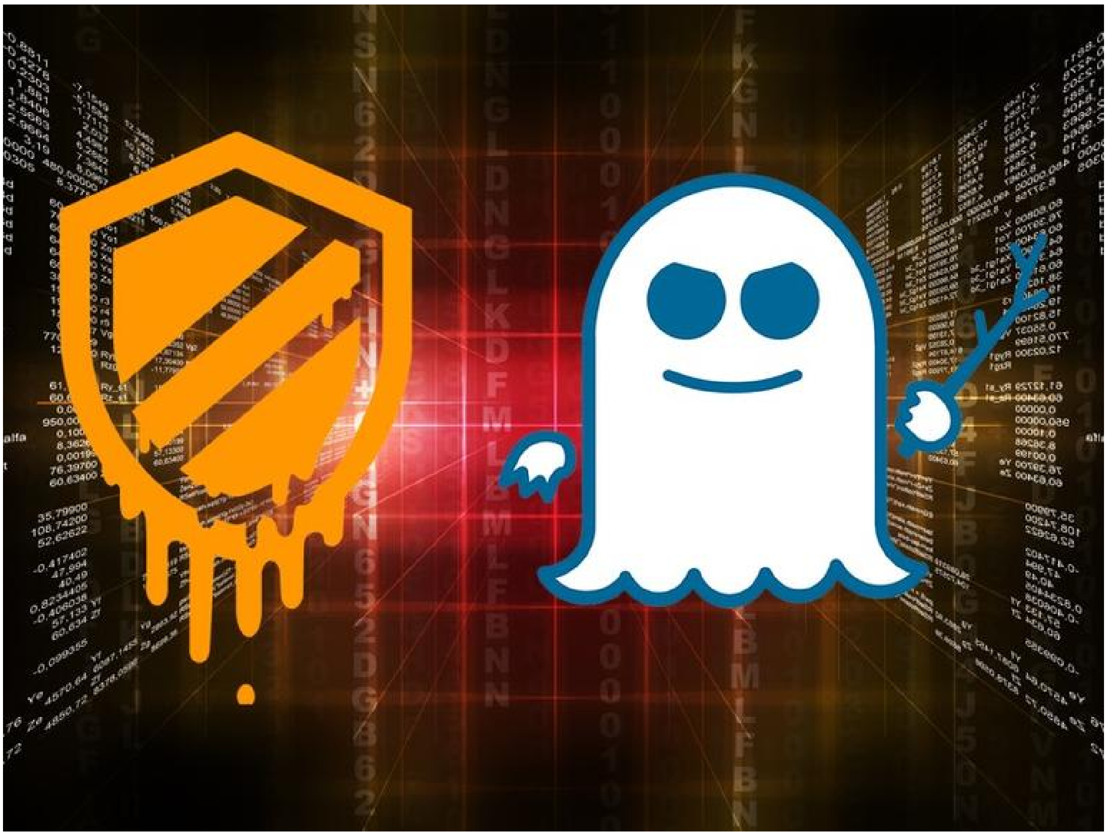
If you want to load a crypto miner on 1,000+ websites you don't attack 1,000+ websites, you attack the 1 website that they all load content from. In this case it turned out that Text Help, an assistive technology provider, had been compromised and one of their hosted script files changed.

This is not a particularly new attack and we've known for a long time that CDNs or other hosted assets are a prime target to compromise a single target and then infect potentially many thousands of websites. The thing is though, there's a pretty easy way to defend yourself against this attack. Now, onto solutions. We have a very robust, well-proven defence for this in subresource integrity (SRI). You add the file's hash as an attribute of the script tag. If - for whatever reason - that library is modified upstream of my website, the sha256 hash of the file will be different to the one specified above and the browser simply won't run it. Finally, we have content security policies (CSP) which provide another layer of defence. A good policy would have stopped the cryptominer from being loaded from coinhive.com in the first place as it wouldn't have appeared as a white-listed script source.

Read More

Protect your site from Cryptojacking with CSP + SRI

New Spectre, Meltdown variants leave victims open to side-channel attacks



Security researchers from NVIDIA and Princeton have discovered new variants of the Meltdown and Spectre flaws that may be more difficult to tackle than the originals. Dubbed MeltdownPrime and SpectrePrime, these flaws were further detailed in a recent research paper.

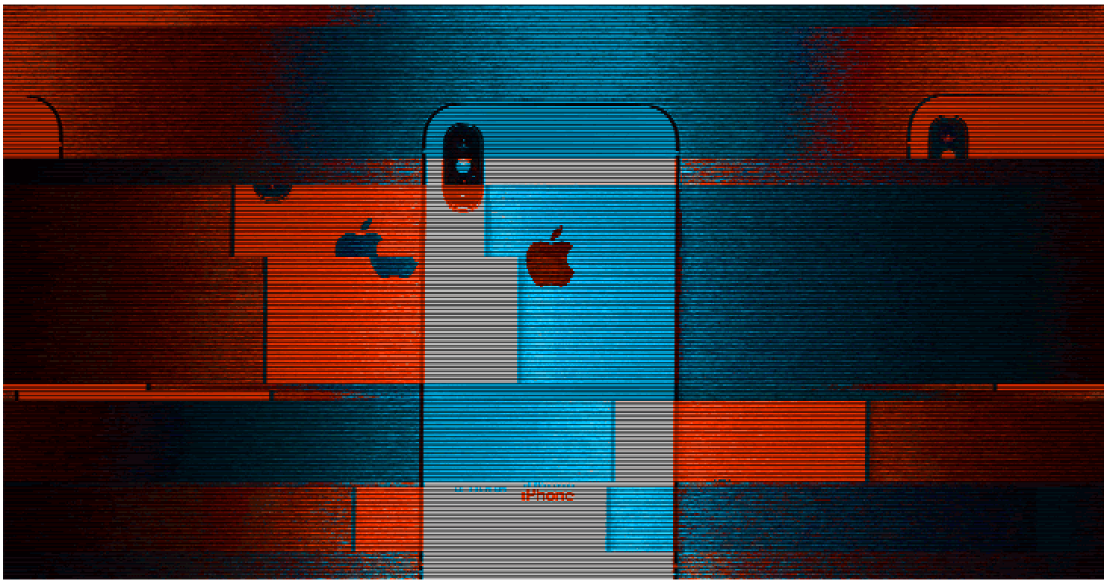
The software changes already underway will likely take care of these two exploits, but the coming hardware fixes won't, the researchers noted in the paper. The researchers said they believe the "hardware protection against them will be distinct," which means that chip makers may need to further change their designs to mitigate the threats.

After creating their own tool to synthesize the Spectre and Meltdown flaws, the researchers were able to use their findings to conduct side-channel attacks, or attacks that take advantage of the physical hardware related to a system's security. By leveraging software dependencies, the paper said, Flush+Reload attacks can also be altered to go after any memory location, not just shared memory. What's at stake here? Well, according to the researchers, these attacks can lead to a leak of privileged kernel memory as well. By leveraging software dependencies, the paper said, Flush+Reload attacks can also be altered to go after any memory location, not just shared memory. What's at stake here? Well, according to the researchers, these attacks can lead to a leak of privileged kernel memory as well.

Read More

Even More

TextBomb: Indian Text Character Crashes Many iOS and macOS Apps



Only a single character can crash your iPhone and block access to the Messaging app in iOS as well as popular apps like WhatsApp, Facebook Messenger, Outlook for iOS, and Gmail.

First spotted by Italian Blog Mobile World, a potentially new severe bug affects not only iPhones but also a wide range of Apple devices, including iPads, Macs and even Watch OS devices running the latest versions of their operating software.

Once the recipient receives a simple message containing the symbol or typed that symbol into the text editor, the character immediately instigates crashes on iPhones, iPads, Macs, Apple Watches and Apple TVs running Apple's iOS Springboard. Apps that receive the text bomb tries to load the character, but fails and refuses to function properly until the character is removed—which usually can be done by deleting the entire conversation. The easiest way to delete the offending message is by asking someone else to send a message to the app that is crashing due to the text bomb. This would allow you to jump directly into the notification and delete the entire thread containing the character.

Read More

Cutting room floor

- Microsoft delivers free Meltdown-Spectre assessment tool for IT pros
- Microsoft Patch Tuesday, February 2018 Edition
- Serious security flaws in Outlook and Edge are headlining a busy Microsoft Patch Tuesday.
- Windows password decryption possible from dump files, mounting offline partitions
- Lenovo Patches Critical Wi-Fi Vulnerabilities
- Equifax hack worse than previously thought
- Security Updates Available for Popular Netgear Routers
- Hackers Exploit 'Telegram Messenger' Zero-Day Flaw to Spread Malware
- Researcher Uses macOS App Screenshot Feature to Steal Passwords, Tokens, Keys
- Researcher Uses macOS App Screenshot Feature to Steal Passwords, Tokens, Keys
- It's 2018 and You Can Still p0wn Your Linux Box by Plugging in a USB Stick
- Making Light of the "Dark Web" (and Debunking the FUD)
- Multi-Stage Word Attack Infects Users Without Using Macros
- Leaked FedEx customer data was stored on Amazon S3 server with no password
- New EU Privacy Law May Weaken Security

#Tech and #Tools

- StaCoAn is a crossplatform tool which aids developers, bugbounty hunters and ethical hackers performing static code analysis on mobile applications.
- ReelPhish: A Real-Time Two-Factor Phishing Tool
- Malicious Installer Plugins
- GoPhish: Open-Source Phishing Framework
- Going beyond Wireshark: experiments in visualising network traffic
- The Easiest Metasploit Guide You'll Ever Read
- Command and control server in social media
- JavaScript AntiDebugging Tricks
- Replicator: Burp plugin helping developers to reproduce issues discovered by pen testers.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us