Security Now! #654 - 03-13-18

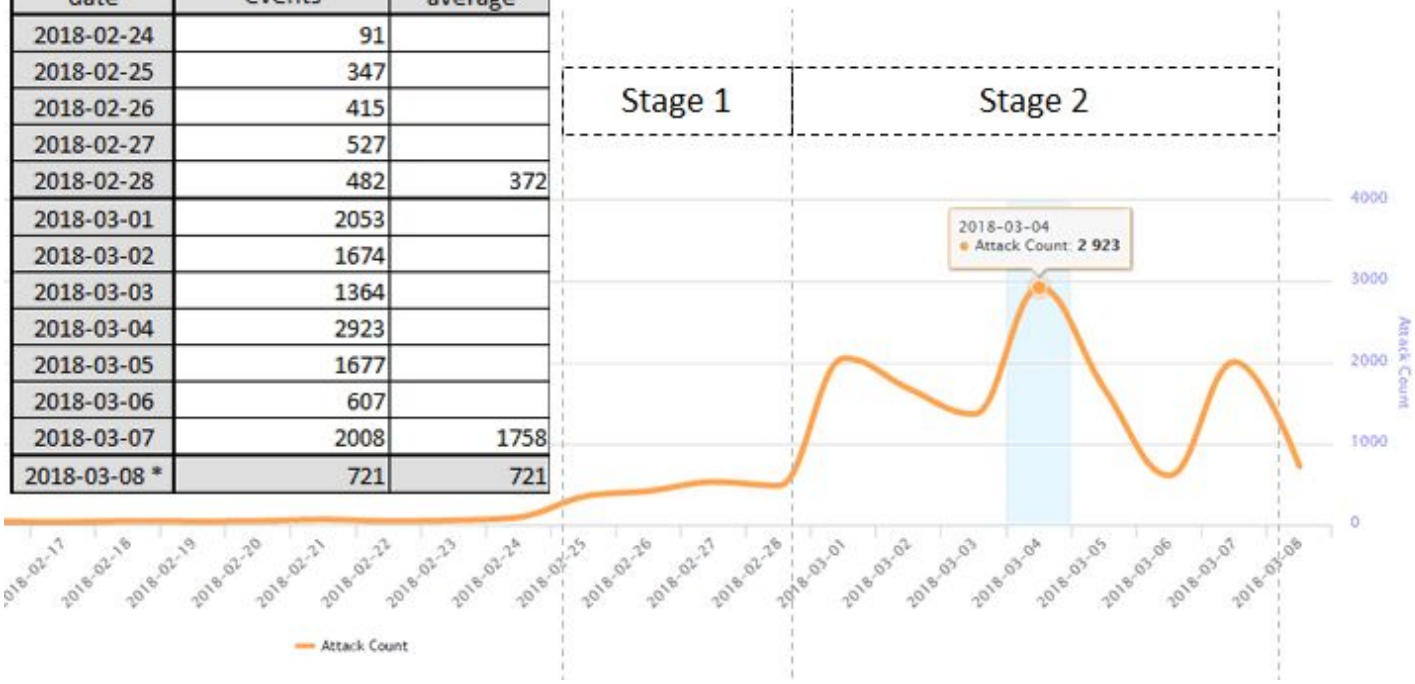
AMD Chipset Disaster

This week on Security Now!

This week we discuss the just-released news of major trouble for AMD's chipset security, ISPs actively spreading state-sponsored malware, Windows 10 S coming soon, a large pile of cryptocurrency mining-driven shenanigans, tomorrow's Pwn2Own competition start, surprising stats about Spam botnet penetration, and a week #2 update on the new Memcached DrDoS attacks.

More than 15,000 Memcached DDoS Attacks Hit 7,100 Sites in Last 10 Days

date	memcache DRDoS events	average
2018-02-24	91	
2018-02-25	347	
2018-02-26	415	
2018-02-27	527	
2018-02-28	482	372
2018-03-01	2053	
2018-03-02	1674	
2018-03-03	1364	
2018-03-04	2923	
2018-03-05	1677	
2018-03-06	607	
2018-03-07	2008	1758
2018-03-08 *	721	721



Security News

A brand new set of 13 critical flaws have just been reported to affect AMD Ryzen and EPYC processors.
https://amdflaws.com/

CTS-Labs, a Tel Aviv, Israel-based team of researchers who gave AMD only 24 hours of advance notice before going public.

Press Release: March 13, 2018 10:00 AM Eastern Daylight Time

TEL AVIV, Israel–(BUSINESS WIRE)–CTS Labs, a cyber-security research firm and consultancy, today released a severe security advisory on Advanced Micro Devices, Inc. ("AMD" or "the Company") (NASDAQ:AMD) processors.

A CTS Labs security audit revealed multiple critical security vulnerabilities and manufacturer backdoors in AMD's latest EPYC, Ryzen, Ryzen Pro, and Ryzen Mobile processors. These vulnerabilities have the potential to put organizations at significantly increased risk of cyber-attacks.

CTS Labs has produced a white paper report further detailing these vulnerabilities available at amdflaws.com. CTS Labs has also shared this information with AMD, Microsoft, HP, Dell, and select security companies, in order that they may work on developing mitigations and patches, and examine and research these and any other potential vulnerabilities at the Company. CTS Labs has also shared this information with relevant U.S. regulators.

CTS Labs is a cyber-security research firm and consultancy based in Tel Aviv, Israel specializing in hardware and embedded systems security. For more information about CTS Labs, please see cts-labs.com.

The vulnerabilities don't affect AMD's Zen CPU cores themselves, but rather two other chips that are part of the Rzyen and EPYC system. The first is the ARM based AMD Secure Processor and the second is the ASMedia Promontory chipset.

AMD: "At AMD, security is a top priority and we are continually working to ensure the safety of our users as new risks arise. We are investigating this report, which we just received, to understand the methodology and merit of the findings,"

What happened?
13 Critical Security Vulnerabilities and Manufacturer Backdoors discovered throughout AMD Ryzen & EPYC product lines.

Am I affected?
Any consumer or organization purchasing AMD Servers, Workstations, or Laptops are affected by these vulnerabilities.

What is this site for?

This site is to inform the public about the vulnerabilities and call upon AMD and the security community to fix the vulnerable products.

https://safefirmware.com/amdflaws_whitepaper.pdf

Four vulnerabilities - three in firmware and one in hardware.

- Ryzenfall / three firmware vulnerabilities
- Fallout
- Masterkey
- Chimera / an unfixable hardware vulnerability.

CHIMERA: Backdoors Inside Ryzen Chipset

The CHIMERA vulnerabilities are an array of hidden manufacturer backdoors inside AMD's Promontory chipsets. These chipsets are an integral part of all Ryzen and Ryzen Pro workstations. There exist two sets of backdoors, differentiated by their implementation: one is implemented within the firmware running on the chip, while the other is inside the chip's ASIC hardware. Because the latter has been manufactured into the chip, a direct fix may not be possible and the solution may involve either a workaround or a recall.

The backdoors outlined in this section provide multiple pathways for malicious code execution inside the chipset's internal processor. Because the chipset is a core system component, running malware inside the chip could have far reaching security implications.

The diagram below was taken from the instruction manual of ASUS Crosshair VI Hero Ryzen motherboard. It can be seen that not only is the chipset connected to the computer's USB, SATA, and PCI-E ports, it is also linked to the computer's LAN, WiFi, and Bluetooth.

In our research we have been able to execute our own code inside the chipset, and then leverage the latter's Direct Memory Access (DMA) engine to manipulate the operating system running on the main processor. These two capabilities form the foundation for malware, and provide a proof-of-concept. We believe that with additional research a determined attacker may also be able to reach the following capabilities:

Key Logger – It may be possible to implement a stealthy key logger by listening to USB traffic that flows through the chipset.

Network Access – It may be possible to implement network-based malware by leveraging the chipset's position as a middle-man for the machine's LAN, WiFi, and Bluetooth components.

Bypass Memory Protection – It may be possible to leverage the chipset's position to access protected memory areas such as System Management RAM (SMRAM). We have verified this works on a small set of desktop motherboards.

Third-Party Chip Design Plagued with Hidden Backdoors

In November 2014, it was announced that AMD signed a contract with the Taiwanese chip

manufacturer ASMedia, according to which ASMedia would design12 AMD's chipset for the upcoming Zen processor series. This chipset, code-named Promontory, plays a central role within the company's latest generation Ryzen and Ryzen Pro workstations. It is responsible for linking the processor to external devices such as Hard Drives, USB devices, PCI Express cards, and occasionally also Network, Wi-Fi, and Bluetooth controllers.

Although it is branded AMD, the Promontory chipset is not based on AMD technology. Rather, it is an amalgamation of several Integrated Circuits that ASMedia has been selling to OEMs for years, all merged together on a single silicon die.

Q&A: Doesn't this publication put users at risk?

No. All technical details that could be used to reproduce the vulnerabilities have been redacted from this publication. CTS has shared this information with AMD, Microsoft, and a small number of companies that could produce patches and mitigations.

ISPs inside Turkey, Syria and Egypt caught spreading FinFisher and StrongPity malware in a massive espionage campaign
https://www.cyberscoop.com/isps-inside-turkey-egypt-spread-finfisher-spyware-massive-espionage-campaign/
https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/

Deep packet inspection hardware: Sandvine "PacketLogic" devices.

According to the report by Citizen Lab, Turkey's Telecom network (which had some overlaps with Syrian ISPs) was using Sandvine PacketLogic devices to redirect hundreds of targeted users (journalists, lawyers, and human rights defenders) to malicious versions of legitimate programs bundled with FinFisher and StrongPity spyware, when they tried to download them from official sources.

HTTP redirects ... Get a load of this: "This redirection was possible because official websites for these programs, even though they might have supported HTTPS, directed users to non-HTTPS downloads by default."

Unwitting Internet users were silently redirected to malicious versions of Avast Antivirus, CCleaner, Opera, and 7-Zip.

However, in Egypt, the Sandvine Packetlogic devices were being used to make money in two ways:
Secretly injecting a cryptocurrency mining script into every HTTP web page users visited in order to mine the Monero cryptocurrency.
Redirecting Egyptian users to web pages with affiliate ads.

Citizen Lab researchers reported Sandvine of their findings, but the company called their report "false, misleading, and wrong," and also demanded them to return the second-hand PacketLogic device they used to confirm attribution of their fingerprint.

Windows 10 'S Mode' Coming Soon — For Security and Performance
https://thehackernews.com/2018/03/windows-10-s-mode.html

Windows 10 'S' Mode: Simplicity • Security • Speed

Windows 10 in S Mode coming soon to all editions of Windows 10
By Joe Belfiore / Corporate Vice President, Windows

Wednesday evening at 5:13 PM:

Some of you may have seen a discussion around our plans for Windows 10 S on Twitter today, and given some additional questions I've received, I thought it might be helpful to share more about our plans with Windows 10 S.

Last year we introduced Windows 10 S – an effort to provide a Windows experience that delivers predictable performance and quality through Microsoft-verified apps via the Microsoft Store. This configuration was offered initially as part of the Surface Laptop and has been adopted by our customers and partners for its performance and reliability.

Since that time, we've received great feedback from customers and partners on Windows 10 S. Customers love the security, faster boot time, better battery life and consistent performance over time. Our partners have brought to market more than 20 devices with Windows 10 S enabled. We have also heard feedback that the naming was a bit confusing for both customers and partners.

Based on that feedback, we are simplifying the experience for our customers. Starting with the next update to Windows 10, coming soon, customers can choose to buy a new Windows 10 Home or Windows 10 Pro PC with S mode enabled, and commercial customers will be able to deploy Windows 10 Enterprise with S mode enabled.

We expect the majority of customers to enjoy the benefits of Windows 10 in S mode. If a customer does want to switch out of S mode, they will be able to do so at no charge, regardless of edition. We expect to see new Windows 10 devices ship with S mode, available from our partners in the coming months, so check back here for updates.

We hope this new approach will simplify and make it possible for more customers to start using Windows in S mode: a familiar, productive Windows experience that is streamlined for security and performance across all our editions.

An interesting collection of CryptoCurrency / Malmining / CryptoJacking news:

I caught a note by Lawrence Abrams' on his terrific BleepingComputer site:
<quote> "It has been a pretty slow ransomware week as most of the malware developers have started pushing cryptominers."

Report: Three of Top Four Malware Threats Are In-Browser Cryptocurrency Miners
https://www.bleepingcomputer.com/news/security/report-three-of-top-four-malware-threats-are-in-browser-cryptocurrency-miners/

Three in-browser cryptocurrency mining scripts ranked first, second, and fourth in Check Point's most active malware top ten, outranking classic high-output malware distribution infrastructures such as spam botnets, malvertising, and exploit kit operations.

The three are Coinhive (ranked #1), Crypto-Loot (ranked #2), and JSEcoin (ranked #4). These three are online services that offer JavaScript libraries that website owners can embed on their sites and generate profit by using their visitors' CPU resources to mine the Monero cryptocurrency.

While all three are legitimate services, the JavaScript libraries provided by these three services have been abused by malware authors.

In Check Point's case, the company says that its security products have detected cryptojacking detections across 42% of the organizations they protect. Coinhive was the leader, with detections found on 20% of all customers, followed by Crypto-Loot with 16%.

Ad network uses advanced malware technique to conceal CPU-draining mining ads
https://arstechnica.com/information-technology/2018/02/ad-network-uses-advanced-malware-technique-to-conceal-cpu-draining-mining-ads/

The backlash against mining

Working to bypass ad-blocking.

DGA's -- Domain name generation algorithms.

So... it didn't take long for the quaint solution of blocking "coinhive.com" to be bypassed.

Coinminer Campaigns Target Redis, Apache Solr, and Windows Servers
https://www.bleepingcomputer.com/news/security/coinminer-campaigns-target-redis-apache-solr-and-windows-servers/

Two new cryptocurrency mining campaigns have appeared in the past week.

The Imperva crew discovered CryptoJacking malware targeting Redis server (Redis is a BSD-based caching server platform with services similar to Memcached) and some CryptoJacking

malware also attacking Windows-based servers.

The SANS security folks also spotted another campaign targeting Apache Solr which is a large scaleable searchable open source database system.

As usual, publicly accessible server are being probed for well known and previously patched vulnerabilities of which there continue to be too many. In the case of the Redis servers, last month a different campaign netted nearly $1 million by infecting Redis and OrientDB servers with similar cryptocurrency mining malware. So there's money to be made... and where there's money there's incentive.

The SANS researchers determined that around 1,777 infections of Apache Solr had succeeded between February 28 and March 8.

New Cryptocurrency Mining Malware Infected Over 500,000 PCs in Just Few Hours
https://thehackernews.com/2018/03/cryptocurrency-mining-malware.html

And... Exactly one week ago, on March 6th, Microsoft detected a rapidly spreading crypto-currency malware which successfully infected nearly 500,000 machines within 12 hours.

Windows Defender suddenly detected more than 80,000 instances of malware named "Dofoil" or "Smoke Loader" which was dropping a cryptocurrency miner as its payload to mine "Electroneum" coins. By the time Windows Defender could respond, nearly another 400,000 more infections were in place. These infections were rapidly spreading across Russia, Turkey, and Ukraine.

The question which has so far gone unanswered by Microsoft is how such a large audience became infected in such a short period.

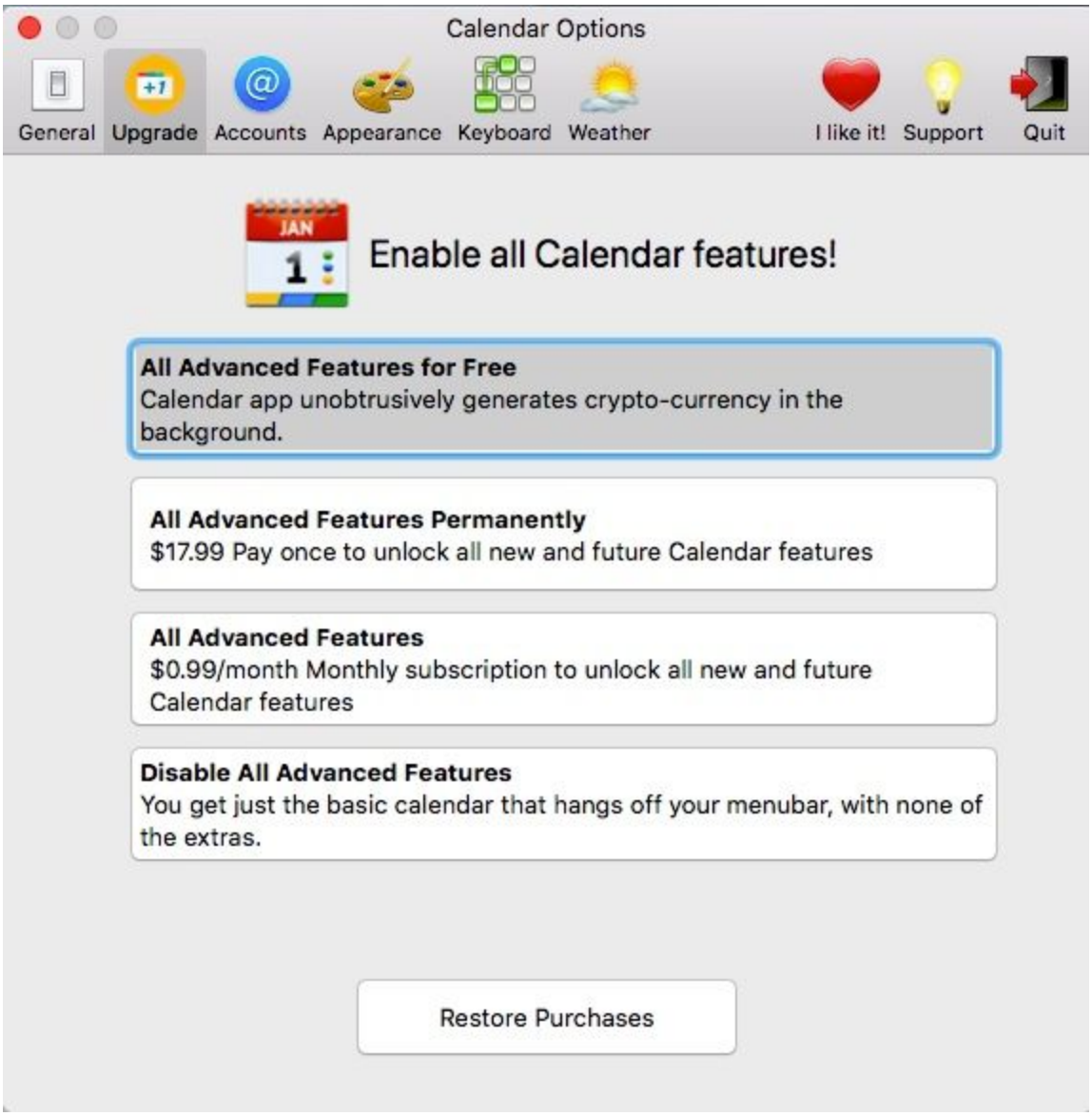
There's a currency miner in the Mac App Store, and Apple seems OK with it
Popular Calendar 2 app mines Monero by default, but at least it discloses it.
https://arstechnica.com/information-technology/2018/03/theres-a-currency-miner-in-the-mac-app-store-and-apple-seems-ok-with-it/

The idea was: Rather than charging for the app's premium features, allow it to mine on user's iOS devices.

Given how many are mobile, that seems like a really bad idea.

- It was =defaulting= to mining without permission.
- In some cases it was mining without permission.
- And it was often taking WAY MORE than 10-20% of the CPU.

Calendar 2's author blamed the 3rd-party mining library he had dropped in, and has said that he planned to remove that feature.



This Heater Not Only Heats Your Home But Also Mines Ethereum
https://www.bleepingcomputer.com/news/cryptocurrency/this-heater-not-only-heats-your-home-but-also-mines-ethereum/

A French heater manufacturing company, Qarnot, is actually selling (or at least offering to sell) a CryptoCurrecy-mining based space heater.
Crypto Heater QC-1: https://www.qarnot.com/crypto-heater_qc1/

Earn crypto currency while heating - The heat of your QC-1 is generated by the 2 graphics cards embedded in the device and mining crypto-currencies or blockchain transactions: while heating, you create money. You can watch in real time how crypto markets are trending, on your mobile app and on your QC-1 LEDs.

Noiseless & high-end design - The QC-1 crypto heater is the only one in the market to be perfectly noiseless! It doesn't embed any mobile part (no fans, no hard drives). This system, developed by Qarnot, is IP-protected.

Intuitive interface - Designed as a plug-and-mine device, the QC-1 crypto heater can be set up in only 10 minutes. You can monitor the mining level of your device, activate a heating booster mode in addition to the mining level when you are cold, on the device and on your app.

2 GPU : NITRO+ RADEON RX 580 8G RAM, solving 60 MH/s

The QC-1 heater costs $2,900 Euros or ~$3,600.

60 MH/s equates to around $120 worth of Ethereum per month... which, of course, doesn't take into consideration the cost of electricity.

Switch to the upcoming Pwn2Own competition...

Pwn2Own 2018
https://www.thezdi.com/blog/2018/1/25/pwn2own-returns-for-2018-partners-with-microsoft-and-sponsored-by-vmware

Tomorrow (March 14th), Thursday & Friday.

The first was 2007, so this is the 12th annual competition.

Pwn2Own returns for 2018 with five categories of targets: virtualization, web browsers, enterprise applications, servers, and a special Microsoft Windows Insider Preview Challenge category.

Zero Day Initiative partners with Microsoft for the event and welcomes VMware as a sponsor. Their support enable up to $2 Million USD in cash and prizes.

Microsoft offers a Windows Insider Preview Challenge that tests their latest pre-release offerings combined with their configuration on their hardware.

The title "Master of Pwn" will be awarded to the team with the most points at the end of the contest.

Of this year's plans, ZDI wrote:

Since its inception in 2007, Pwn2Own has increased the challenge level at each new competition, and this year is no different. Web browsers return as a target, as do virtual machine guest-to-host escapes. Enterprise applications remain as targets for this year, and for 2018, Outlook makes its Pwn2Own debut. Our virtualization category grows by two as Oracle becomes a target, and the Windows Insider Preview Challenge includes brand new targets for their virtualization-based security stack. Server targets expand this year as well. Apache was included in last year’s event and is joined this year by NGINX, OpenSSL, and Windows SMB server. Over the years, we’ve seen some ground-breaking research demonstrated, so we can’t wait to see what contestants bring this year.

... however... this year there will be no hacking entrant's from the previous year's winning

Country:

China's government is keeping its security researchers from attending conferences
https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/

My first thought was that this might be to prevent them from being detained as Marcus Hutchins was after last summer's BlackHat Conference in Las Vegas.

Brian Gorenc, director of Trend Micro's Zero Day Initiative said: "There have been regulatory changes in some countries that no longer allow participation in global exploit contests, such as Pwn2Own and Capture the Flag competitions." ... and Brian was specifically referring China.

So there will be no Chinese research teams at Pwn2Own this year... which will likely be felt since for the last several years Chinese teams have dominated the competition.

Prior year Chinese winners were contacted and asked for comment, but none would remark other than to indicate that they would not be attending the competitions.

Chinese Intelligence Agencies Are Doctoring the Country's Vulnerability Database
https://www.bleepingcomputer.com/news/security/chinese-intelligence-agencies-are-doctoring-the-countrys-vulnerability-database/

Much as we have the CVE -- Common Vulnerabilities and Exposures -- database at cve.mitre.org

China has their CNNVD - Chinese National Vulnerabilities Database.

But, according to a report released last Friday by the US threat intelligence firm "Recorded Future", China has been playing fast and loose with the facts and altering their public vulnerability database to conceal the influence of the Chinese Ministry of State Security.

https://go.recordedfuture.com/hubfs/reports/cta-2018-0309.pdf

Four Key Judgements:

- CNNVD altered the original publication dates in its public database for at least 267 vulnerabilities we identified as statistical outliers in our research published in November 2017.

- We assessed in November that CNNVD had a formal vulnerability evaluation process in which high-threat CVEs were evaluated for their operational utility by the MSS before publication, and that the publication lag was one way to identify vulnerabilities that the MSS was likely considering for use in offensive cyber operations. CNNVD's outright manipulation of these dates implicitly confirmed this assessment.

- By retroactively changing the original publication dates on these statistical outliers, CNNVD attempted to hide the evidence of this evaluation process, obfuscate which vulnerabilities the MSS may be utilizing, and limit the methods researchers can use to

anticipate Chinese APT behavior.

- This large-scale manipulation of vulnerability data undermines trust in the CNNVD process and could compromise security operations relying solely on the CNNVD for that information.

Victims can sue Yahoo for massive breaches, federal judge says
https://www.cyberscoop.com/yahoo-breach-lawsuit-motion-to-dismiss/

Meanwhile, also last Friday:

U.S. District Judge Lucy Koh denied in part a motion by Verizon, which owns Yahoo, to dismiss a case brought by plaintiffs who are suing Yahoo! for failing to adequately protect their users' security and for neglecting to respond to known and dangerous vulnerabilities.

Since Yahoo's breaches affected virtually every user, the plaintiffs are seeking class certification.

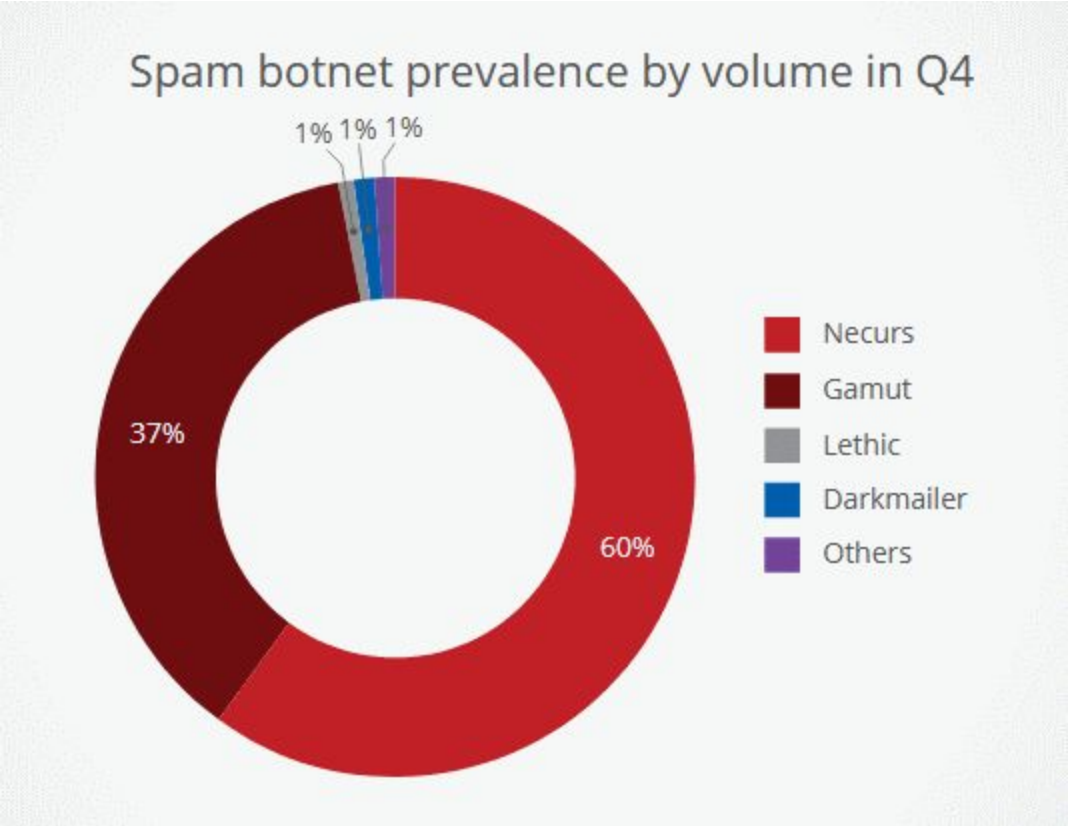
Judge Koh wrote in her ruling, Friday: "Plaintiffs explain that, had they known about the inadequacy of these security measures, they 'would have taken measures to protect themselves. Plaintiffs' allegations are sufficient to show that they would have behaved differently had Defendants disclosed the security weaknesses of the Yahoo Mail system."

The plaintiffs argue that the breaches have put them at risk of identity theft and forced them to spend time and money mitigating that risk. As a result, they say they would have chosen a different email provider had they been aware of Yahoo's risks.

As we know, and covered here, in December of 2016 Yahoo first disclosed the 2013 breach which compromised the credentials of 1 billion users. Then last October that assessment was updated to 3 billion impacted accounts.

Necurs and Gamut Botnets Account for 97% of the Internet's Spam Emails
https://www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/

According to a report released by McAfee yesterday, only two botnets accounted for 97% of all spam emails in the last three months of 2017.



For most of these months, Necurs has spent its time churning out "lonely girl" spam lures for adult websites, pump-and-dump schemes [1, 2], and delivering ransomware payloads. Overall, nearly two out of three spam emails sent in the last quarter of 2017 were sent from the infrastructure of this mammoth botnet.

Second on the list was the Gamut botnet, also built on Windows machines infected with malware that hijacks systems to send out spam. Gamut —while smaller in size when compared to Necurs— had previously been more active in Q3, sending more spam than the aforementioned.

In Q4, Gamut activity went down, but the botnet still accounted for 37% of all email spam, compared to Necurs' 60%. Most of Gamut's email subjects were related to job offer–themed phishing and money mule recruitment (tricking people to buy products with stolen money and sending the products to crooks; relaying money from hijacked bank accounts to crooks' accounts).

SpinRite

Eric in Wisconsin
Subject: Yet Another SRSTD story!
Date: 27 Feb 2018 16:46:42
:
SRSTD = SpinRiteSavesTheDay

Steve,

First of all...THANK YOU for your great SpinRite product and have been meaning to pass along a story of yet another of SPinRite's successes or me for quite some time. I have often thought this may just be another "run of the mill" testimonial of how SR has saved the day but thought I would share it anyway and let you be the judge; besides, I had to say 'Thanks!'

A dentist's office was referred to me for support when their <insert well known brand here> NAS device was indicating multiple drive failures and they could not access any of their data for the office (because the NAS wouldn't boot). Of course, I asked about their current backup process and was "shocked" (not really) to hear they had been meaning to address that hole in their process for some time.

This particular NAS was bootable from its USB port, so I booted it into SpinRite and let SpinRite go to work. By now, everyone knows that a happy ending usually ensues, and that is an understatement in this case. SpinRite plowed through the entire array and upon reboot was happily serving data again. For safe keeping and I was also able to get a copy of their never-backed-up data off of the NAS.

Needless to say they were ecstatic about the recovery and also now have a good local and offsite backup process in place. I did recommend to them to go purchase their own copy of SR to express their satisfaction and I believe they have done so.

Thank you again for ALL that you do! Look forward to listening to about 350 more SN episodes! Keep up the good work!

Eric in Wisconsin.

MemCrashed Follow-Up

Over 15,000 Memcached DDoS Attacks Hit 7,100 Sites in Last 10 Days
https://thehackernews.com/2018/03/memcached-ddos-attack.html

Code for massive 'Memcrashed' DDoS attack made public
https://www.cyberscoop.com/ddos-attack-code-posted-memcrashed/

Memcached DDoS Exploit Code and List of 17,000 Vulnerable Servers Released
https://thehackernews.com/2018/03/memcached-ddos-exploit-code.html

It just got much easier to wage record-breaking DDoSes
Exploits that abuse memcached servers threaten the stability of the Internet.
https://arstechnica.com/information-technology/2018/03/it-just-got-much-easier-to-wage-record-breaking-ddoses/

'Kill Switch' to Mitigate Memcached DDoS Attacks — Flush 'Em All
https://thehackernews.com/2018/03/prevent-memcached-ddos.html