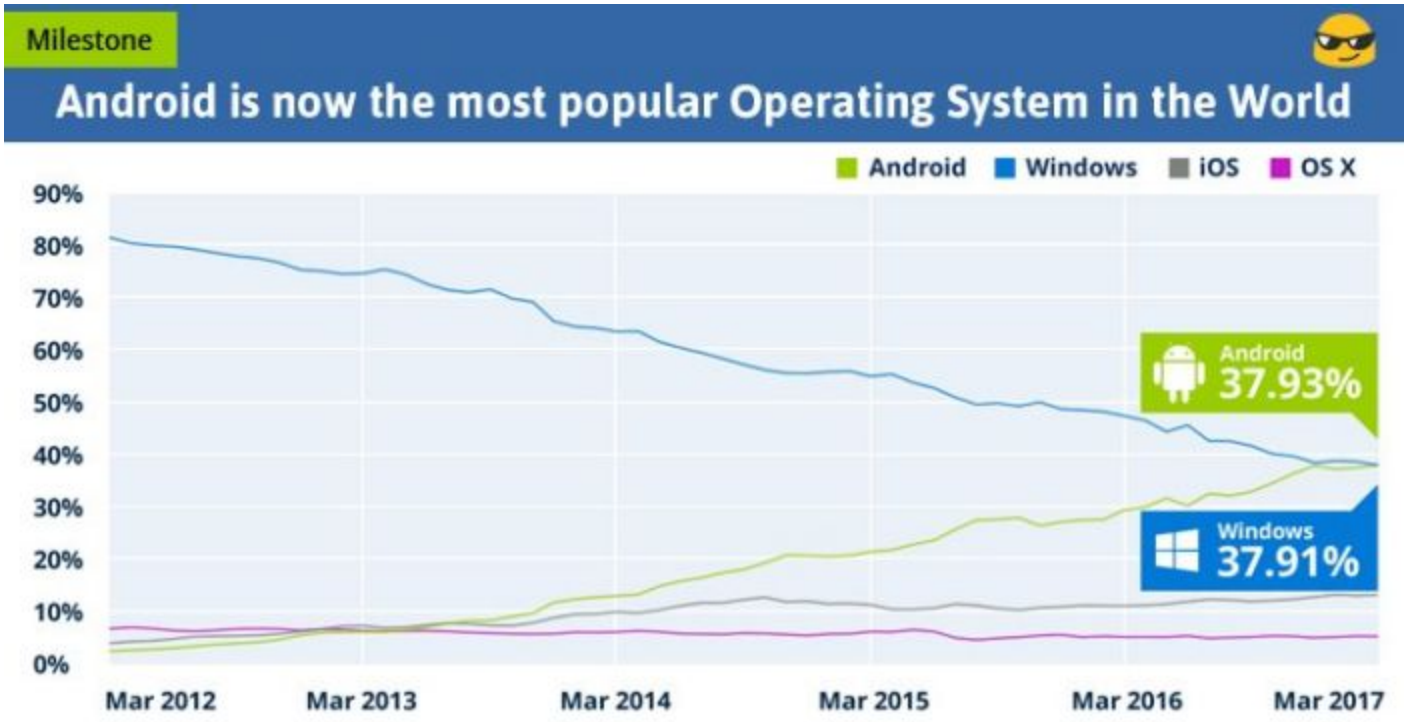
Security Now! #610 - 05-02-17

Intel’s Mismanagement Engine

This week on Security Now!

This week Steve and Leo discuss the long-expected remote vulnerability in Intel's super-secret motherboard Management Engine technology, exploitable open ports in Android apps, another IoT blows a suspect's timeline, new;y discovered problems in the Ghostscript interpreter, yet another way for ISPs and others to see where we go, a new bad problem in the Edge browser, Chrome changes its certificate policy, an interesting new "Vigilante Botnet" is growing fact, a proposed solution to smartphone-distracted driving, Ransomware as a service, Net Neutrality heads back to the chopping block (again), an intriguing new service from Cloudflare, the ongoing Symantec certificate issuance controversy. Then some fun errata, miscellany, and some closing-the-loop feedback from our terrific listeners.

Our Picture of the Week



Security News

A true May Day for Intel: A remote security exploit in all 2008+ Intel platforms
All Intel Management Engine (ME) systems from v6 - v11.6

- IAM - Intel Active Management
- SBT - Small Business Technology
- ISM - Intel Standard Manageability

What is the Intel Management Engine?

Recent Intel x86 processors implement a secret, powerful control mechanism that runs on a separate chip that no one is allowed to audit or examine. When these are eventually compromised, they'll expose all affected systems to nearly unkillable, undetectable rootkit attacks. I've made it my mission to open up this system and make free, open replacements, before it's too late.

The Intel Management Engine (ME) is a subsystem composed of a special 32-bit ARC microprocessor that's physically located inside the chipset. It is an extra general purpose computer running a firmware blob that is sold as a management system for big enterprise deployments.

When you purchase your system with a mainboard and Intel x86 CPU, you are also buying this hardware add-on: an extra computer that controls the main CPU. This extra computer runs completely out-of-band with the main x86 CPU meaning that it can function totally independently even when your main CPU is in a low power state like S3 (suspend).

On some chipsets, the firmware running on the ME implements a system called Intel's Active Management Technology (AMT). This is entirely transparent to the operating system, which means that this extra computer can do its job regardless of which operating system is installed and running on the main CPU.

<<but wait!... it gets worse!...>>

The purpose of AMT is to provide a way to manage computers remotely (this is similar to an older system called "Intelligent Platform Management Interface" or IPMI, but more powerful). To achieve this task, the ME is capable of accessing any memory region without the main x86 CPU knowing about the existence of these accesses. It also runs a TCP/IP server on your network interface and packets entering and leaving your machine on certain ports bypass any firewall running on your system.

While AMT can be a great value-add, it has several troubling disadvantages. ME is classified by security researchers as "Ring -3". Rings of security can be defined as layers of security that affect particular parts of a system, with a smaller ring number corresponding to an area closer to the hardware. For example, Ring 3 threats are defined as security threats that manifest in "userspace" mode. Ring 0 threats occur in "kernel" level, Ring -1 threats occur in a "hypervisor" level, one level lower than the kernel, while Ring -2 threats occur in a special CPU mode called "SMM" mode. SMM stands for System-Management-Mode, a special mode that Intel CPUs can be put into that runs a separately defined chunk of code. If attackers can modify the SMM code and trigger the mode, they can get arbitrary execution of code on a CPU.

Although the ME firmware is cryptographically protected with RSA 2048, researchers have been able to exploit weaknesses in the ME firmware and take partial control of the ME on early models. This makes ME a huge security loophole, and it has been called a very powerful rootkit

mechanism. Once a system is compromised by a rootkit, attackers can gain administration access and undetectably attack the computer.

So this is essentially a built-in, hardware based, Ring -3 Rootkit that we have been hoping didn't have any problems and wouldn't get hacked. On newer systems, ME cannot be disabled. And it operates completely out-of-band, the OS can't even scan ME to see if it's been compromised and can't disinfect a hacked ME chip.

Intel rates this as a CRITICAL remotely exploitable.

Wikipedia's page has already been updated:

Intel Active Management Technology (AMT) is hardware and firmware technology for remote out-of-band management of personal computers, in order to monitor, maintain, update, upgrade, and repair them. Out-of-band (OOB) or hardware-based management is different from software-based (or in-band) management and software management agents. Intel has confirmed and patched a Remote Elevation of Privilege bug(CVE-2017-5689) in its Management Technology, on 1st May 2017. Every Intel platform with either Intel Standard Manageability, Active Management Technology, or Small Business Technology, from Nehalem in 2008 to Kaby Lake in 2017 has a remotely exploitable security hole in the IME (Intel Management Engine).

Wikipedia also notes: Currently, AMT is available in desktops, servers, ultrabooks, tablets, and laptops with Intel Core vPro processor family, including Intel Core i3, i5, i7, and Intel Xeon processor E3-1200 product family.

<Intel quote> "There is an escalation of privilege vulnerability in Intel® Active Management Technology (AMT), Intel® Standard Manageability (ISM), and Intel® Small Business Technology versions firmware versions 6.x, 7.x, 8.x 9.x, 10.x, 11.0, 11.5, and 11.6 that can allow an unprivileged attacker to gain control of the manageability features provided by these products. This vulnerability does not exist on Intel-based consumer PCs.

The vulnerability is BOTH remotely and locally exploitable.

Google: Intel Management Engine Verification Utility
https://downloadcenter.intel.com/download/19009
Dated May 12th, 2010 with support for XP through Win7... but likely Win10 too.

How-To Geek: "How to Remotely Control Your PC (Even When it Crashes)"
https://www.howtogeek.com/56538/how-to-remotely-control-your-pc-even-when-it-crashes/

How To Find Intel® vPro™ Technology Based PCs
https://communities.intel.com/docs/DOC-5693

Links:
http://semiaccurate.com/2017/05/01/remote-security-exploit-2008-intel-platforms/
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr

Open Ports Create Backdoors in Millions of Smartphones

Five researchers at the University of Michigan have published their research which was presented at last week's IEEE European Symposium on Security and Privacy 2017.
"Open Doors for Bob and Mallory: Open Port Usage in Android Apps and Security Implications"

Abstract

Open ports are typically used by server software to serve remote clients, and the usage historically leads to remote exploitation due to insufficient protection. Smartphone operating systems inherit the open port support, but since they are significantly different from traditional server machines in performance and availability guarantees, little is known about how smartphone applications use open ports and what the security implications are. In this paper, we perform the first systematic study of open port usage on mobile platform and their security implications. To achieve this goal, we design and implement OPAnalyzer, a static analysis tool which can effectively identify and characterize vulnerable open port usage in Android applications.

Using OPAnalyzer, we perform extensive usage and vulnerability analysis on a dataset with over 100K Android applications. OPAnalyzer successfully classifies 99% of the mobile usage of open ports into 5 distinct families, and from the output, we are able to identify several mobile-specific usage scenarios such as data sharing in physical proximity. In our subsequent vulnerability analysis, we find that nearly half of the usage is unprotected and can be directly exploited remotely. From the identified vulnerable usage, we discover 410 vulnerable applications with 956 potential exploits in total. We manually confirmed the vulnerabilities for 57 applications, including popular ones with 10 to 50 million downloads on the official market, and also an app that is pre-installed on some device models. These vulnerabilities can be exploited to cause highly-severe damage such as remotely stealing contacts, photos, and even security credentials, and also performing sensitive actions such as malware installation and malicious code execution. We have reported these vulnerabilities and already got acknowledged by the application developers for some of them. We also propose countermeasures and improved practices for each usage scenario.

To get an initial estimate on the impact of these vulnerabilities in the wild, we performed a port scanning in our campus network, and immediately found a number of mobile devices in 2 minutes which were potentially using these vulnerable apps. we have reported these vulnerabilities to the relevant parties through vulnerability tracking systems including CVE and CERT, and some of them have been acknowledged (e.g., CVE-2016-5227, VR-176). We encourage readers to view several short attack video demos at:
https://sites.google.com/site/openportsec/

Threat model:
The threat to an app with open ports comes from the attackers with the ability to reach these ports. In the design of popular smartphone operating systems such as Android, ports are reachable from both the same device, e.g., another app or a script on the web page, and another host in the same network with the victim device. Thus, compared to the majority of previously-reported smartphone app vulnerabilities that only consider the threat from on-device malware, open port apps additionally face threats from network attackers, e.g., local network attacks, and web attackers, e.g., malicious scripts, which is much more diverse and also of wider

range. More specifically, in this paper we consider the following three adversary types:

(1) Malware on the same device. A malicious app, or malware, installed by the smartphone user can use netstat command or proc file /proc/<pid>/net/tcp to find the listening ports on the same device and send exploitation traffic.

(2) Local network attacker. For victims behind NAT or using private WiFi networks, attackers sharing the same local network can use ARP scanning [4] to find reachable smartphone IP addresses at first, and then launch targeted port scanning to discover vulnerable open ports.

(3) Malicious scripts on the web. When a victim user visits an attacker-controlled website using their mobile device, malicious scripts running in the handset's browser can exploit the vulnerable open ports on the device by sending network requests, which doesn't require any permission. For each of these three threat models, we have prepared short attack video demos on our website [11] to help readers more concretely understand their practicality.

Links:

- https://www.bleepingcomputer.com/news/security/open-ports-create-backdoors-in-millions-of-smartphones/
- http://mashable.com/2017/04/28/smartphones-hack-android-open-ports-google-play
- http://web.eecs.umich.edu/~jackjia/material/open_euro17.pdf

Sophos Naked Security News: Murder victim's Fitbit contradicts husband's version of events

- https://nakedsecurity.sophos.com/2017/04/27/murder-victims-fitbit-contradicts-husbands-version-of-events/
- Bizarre story... but the defendant husband's testimony about the timeline of what had transpired was completely undercut by the Fitbit his murdered wife was wearing.
- 357 Magnum / Zip-tied one arm and one leg, with his other wrist zip-tied around his neck.
- Alleging a large 6'2" hooded cammo intruder… and so on.

Another mega-interpreter bites us: Ghostscript

GhostScript has been around for 28 years, since 1988. It's an extremely popular interpreter Postscript and PDF interpreter which reads vector language and outputs raster bitmap page images.

Researcher Kamil Frankowicz took a close look at the latest release and discovered multiple significant vulnerabilities:

Ghostscript improperly handles parameters to the rsdparams and eqproc commands. An attacker could use these to craft a malicious document that could disable OS protections, thereby allowing the execution of arbitrary code, or cause a denial of service (application crash). (CVE-2017-8291)

He also found a use-after-free vulnerability in the color management module of Ghostscript. An attacker could use this to cause a denial of service (application crash). (CVE-2016-10217)

And he found a divide-by-zero error in the scan conversion code in Ghostscript. An attacker could use this to cause a denial of service (application crash). (CVE-2016-10219)

And, finally, he discovered multiple NULL pointer dereference errors in Ghostscript. An attacker could use these to cause a denial of service (application crash). (CVE-2016-10220, CVE-2017-5951, CVE-2017-7207)

Affected are, at least:
Ubuntu 17.04, Ubuntu 16.10, Ubuntu 16.04 LTS, Ubuntu 14.04 LTS, Ubuntu 12.04 LTS

https://packetstormsecurity.com/files/142343/USN-3272-1.txt

Yet another way for an ISP (or anyone) to see what you're doing: SNI

- All browsers, some for 11 years.
- SNI was added to the IETF's Internet RFCs in June 2003
- Even the popular "WGET" command line tool.
- https://en.wikipedia.org/wiki/Server_Name_Indication
- Nice simple explainer:
- https://journal.paul.querna.org/articles/2005/04/24/tls-server-name-indication/

Microsoft Edge Vulnerability Allows Cookie and Password Theft

A SERIOUS Same Origin Policy (SOP) Bypass has been found in Microsoft's Edge Browser by a browser security researcher Manuel Caballero, based in Buenos Aires. He has a long history of finding security problems in browsers... and he apparently has no interest in responsible disclosure.

The problem surrounds Edge's handling of "domainless pages" such as "about:blank".

This Edge browser vulnerability can be exploited to allow an attacker to obtain a user's password and cookie files for online accounts. This vulnerability is currently unpatched.

Versions of the proof-of-concept demos are hosted online, and since users may not wish to have their own cookies and passwords exposed, video demos are also available.

Manuel noted that the vulnerability can be customized to dump the passwords or cookies of any other online service, including Facebook, Amazon, and others. The flaw affects only Edge because Universal Cross-Site Scripting / Same Origin Policy bypasses tend to be specific to individual browsers.

Because modern ads deliver JavaScript code to browsers, attackers can leverage malvertising campaigns to automate the delivery of this exploit to thousands of victims, or more.

Manual explained that attackers are able to use malvertising to push their malicious code into cheap banners shown on popular sites. If an attacker is hosted inside a Yahoo banner and the user is logged in into their Twitter account, that user will be owned with no interactions at all.

Links:

- https://www.bleepingcomputer.com/news/security/microsoft-edge-vulnerability-allows-cookie-and-password-theft/
- http://www.brokenbrowser.com/sop-bypass-uxss-tweeting-like-charles-darwin/

Chrome Deprecates Subject CN Matching

For a long time, certificates have had two ways to express the domain/IP they are bound to:

The original way, the "Common Name" was never rigorously defined or well structured and can be ambiguous.

The later "Subject Alternative Name" (SAN) is well defined.

In the absence of any subjectAltNames, Chrome has been falling back to comparing the domain against the commonName, if present.

With Chrome 58 this fallback path is removed.

Motivation:

Since 1997 (X.509v3's ratification), certificates have had two ways to express a binding to a domain name - either via the commonName attribute within the certificate's subject, or via the explicitly typed (dNSName or iPAddress) of the SubjectAlternativeName Extension.

Since RFC 2818 (published in 2000, first drafted in January 1998), the use of the commonName field has been considered deprecated, because it's ambiguous and untyped - that is, it might contain a human-readable name or it might be a domain name.

The use of the subjectAlternativeName fields leaves it unambiguous whether a certificate is expressing a binding to an IP address or a domain name, and is fully defined in terms of its interaction with Name Constraints. commonName, however, is ambiguous, and because of this, support for the commonName has been a source of security bugs - in both Chrome and the libraries it uses and within the TLS ecosystem at large.

The only big impact may be on those using self-signed certificates since some of the older certificate signing tools are only able to place the certificate's name into the Common Name.

https://textslashplain.com/2017/03/10/chrome-deprecates-subject-cn-matching/

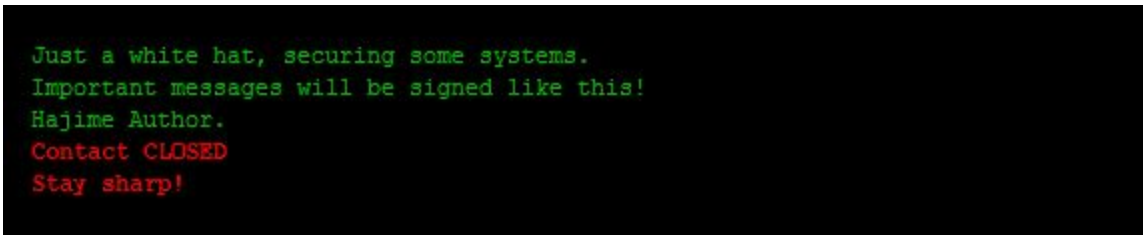
A new IoT-infecting 'Vigilante Botnet' is growing rapidly.
It is now resident in more than 300,000 IoT devices worldwide

The so-called Hajime (Ha' -jim - eh) botnet is extremely well-designed and sophisticated with a robustness and feature set that surpasses its overtly-malicious rivals. And it is expending a huge amount of effort into infecting IoT devices.

However, unlike Mirai, once Hajime infects an IoT device it closed the backdoors behind itself, securing the devices against further attack by blocking access to ports 23, 7547, 5555, and 5358, which are known to be the most widely used vectors for infecting IoT devices. Thus, at least temporarily, sanitizing the device in its wake.

Rather than using the more common fixed command-and-control server architecture, Hajime employs a decentralized peer-to-peer network to issue updates to infected devices. This makes it far more difficult for the botnet to be taken down -- by anyone.

When injected devices are equipped with display terminals it displays a cryptographically signed message approximately every 10 minutes, describing its creators as "Just a white hat, securing some systems."



Unlike Mirai and other IoT botnets, Hajime lacks DDoS capabilities and other hacking skills except for the propagation code that lets one infected IoT device search for other vulnerable devices and infects them.

Kaspersky security researchers noted that: "The most intriguing thing about Hajime is its purpose. While the botnet is getting bigger and bigger, partly due to new exploitation modules, its purpose remains unknown. We haven't seen it being used in any type of attack or malicious activity. Its real purpose remains unknown."

Radware's write up provided some additional interesting technical details:

The distributed bot network used for command and control and updating is overlaid as a traceless torrent on top of the well-know public BitTorrent peer-to-peer network using dynamic info_hashes that change on a daily basis. All communications through BitTorrent are signed and encrypted using RC4 and private/public keys.

The current extension module provides scan and loader services to discover and infect new victims. The efficient SYN scanner implementation scans for open ports TCP/23 (telnet) and TCP/5358 (WSDAPI). Upon discovering open Telnet ports, the extension module tries to exploit the victim using brute force shell login much the same way Mirai did. For this purpose, Hajime

uses a list consisting of the 61 factory default passwords from Mirai and adds two new entries, 'root/5up' and 'Admin/5up,' which are factory defaults for Atheros wireless routers and access points. In addition, Hajime is capable of exploiting ARRIS modems using the password-of-the-day "backdoor" with the default seed as outlined here.

Hajime does not rashly follow a fixed sequence of credentials, from Radware's honeypot logs, we could conclude that the credentials used during an exploit change depending on the login banner of the victim. In doing so, Hajime increases its chances of successfully exploiting the device within a limited set of attempts and avoid the system account being locked or its IP being blacklisted for a set amount of time.

Radware also suggested that the flexible and extensible nature of the Hajime botnet would allow it to be used for malicious purposes including conducting real-time mass surveillance from Internet-connected webcams.

However, since Hajime has no persistence mechanism, as soon as the infected device is rebooted, it goes back to its previously unsecured state, with default passwords and the Telnet port open to the world.

Links:

- https://security.radware.com/ddos-threats-attacks/hajime-iot-botnet/
- http://thehackernews.com/2017/04/vigilante-hacker-iot-botnet_26.html
- https://arstechnica.com/security/2017/04/a-vigilante-is-putting-huge-amount-of-work-into-infecting-iot-devices/

'Textalyzer' Aims To Curb Distracted Driving, But What About Privacy?
NPR reports:

If you're one of the many who text, read email or view Facebook on your phone while driving, be warned: Police in your community may soon have a tool for catching you red-handed. The new "textalyzer" technology is modeled after the Breathalyzer, and would determine if you had been using your phone illegally on the road.

Lawmakers in New York and a handful of other cities and states are considering allowing police to use the device to crack into phones because, they say, too many people get away with texting and driving and causing crashes.

"Phone records — as I found out the hard way — they're tough to get [and] it's an agonizing process," says Ben Lieberman of New Castle, N.Y., whose 19-year-old son was killed in a car crash in the Hudson Valley, north of New York City, in 2011.

The driver of the car his son Evan was in drifted over the center line and hit another vehicle head-on. Evan, who was sitting in the back seat with his seat belt on, suffered massive internal injuries and died a month later.

The driver initially told police he dozed off while driving, but in reality he had been texting behind the wheel. It took Lieberman six months to figure that out.

"Astonishingly, the phone was in the car, wrecked in the car, and it was at a tow yard," he says. "It was there for weeks — it was just sitting there."

Lieberman says police couldn't check the driver's phone to see if he was lying because they needed probable cause to get a warrant.

"We often hear, 'just get a warrant' or 'just get the phone records.' ... The implication is that the warrant is like filling out some minor form," he says. "It's not. In New York, it involves a D.A. and a judge. Imagine getting a D.A. and a judge involved in every breathalyzer that's administered, every sobriety test that's administered."

Lieberman filed a civil lawsuit to subpoena the phone records, which showed the driver had been texting before the crash. But even getting the phone records won't tell you much, he says. "It doesn't detect any of the important distractions, like email, social media or Web browsing."

So even though New York and most other states ban texting and other kinds of cellphone use while driving, Lieberman says those laws are difficult to enforce.

"The takeaway is, our current law is a joke," he says.

Lieberman — along with the advocacy group he co-founded — has been working with a company called Cellebrite to develop the"Textalyzer." It would be able to determine whether a driver illegally was using a phone in the moments before a crash.

Cellebrite engineer Lee Papathanasiou demonstrated the device for lawmakers and reporters at the New York State Capitol in Albany earlier this week.

He says a police officer just goes to the driver and attaches a cord to connect the device to the phone. The driver doesn't even have to let go of the device.

Papathanasiou said: "They simply tap one button. It will process for about 90 seconds or so then display what the last activities were — again that could be a text message and so on — with a time stamp,"

The device would display a summary of what apps on the phone were open and in use, he says, as well as screen taps and swipes. "For example, if it was a WhatsApp message, or a call, it will indicate what the source was, the time stamp, and then what the direction of the communication was — so if it was an outgoing call versus an incoming call."

Papathanasiou says the technology still is not yet fully developed, but would be tailored to what's legal in each jurisdiction that approves its use. And he insists that the textalyzer would only capture taps and swipes to determine if a driver was using the phone — that it would not download content — and that it would be able to tell if the driver was using a phone legally, hands-free.

In New York, the bill authorizing police to use the textalyzer has passed out of one committee and is pending in another. Lawmakers are interested in the device in New Jersey and Tennessee,

and in Chicago and other cities, too, as they consider ways to get drivers to focus on the road instead of their phones.

http://www.npr.org/sections/alltechconsidered/2017/04/27/525729013/textalyzer-aims-to-curb-distracted-driving-but-what-about-privacy

We've had SaaS, now we have RaaS: Ransomware As A Service:
At $175, a new ransomware service on offer from a Russian-speaking user, will be a boon to less technical cybercriminals.

Going by the name "Karmen", anyone can deploy this easy-to-use drop-in ransomware kit without any need to understand its inner workings.

The security firm Recorded Future posted last week that a Russian-speaking user called DevBitox has been advertising the ransomware in underground forums.

Karmen is part of a worrisome new trend know as Ransomware-As-A-Service. It allows less technically skilled amateur hackers with little technical know-how to inexpensively purchase access, in return for which they receive a complete suite of web-based tools to develop their own ransomware attacks.

In Karmen's case, it offers an easy-to-use dashboard interface. Buyers can modify the ransomware, view what machines they've infected, and see how much they've earned.

Links:

- http://www.pcworld.com/article/3190852/security/at-175-this-ransomware-service-is-a-boon-to-cybercriminals.html

FCC announces plan to reverse Title II net neutrality

The Verge:

The Federal Communications Commission is cracking open the net neutrality debate again with a proposal to undo the 2015 rules that implemented net neutrality with Title II classification.

FCC chairman Ajit Pai called the rules "heavy handed" and said their implementation was "all about politics." He argued that they hurt investment and said that small internet providers don't have "the means or the margins" to withstand the regulatory onslaught.

Ajit Pai said last Wednesday: "Earlier today I shared with my fellow commissioners a proposal to reverse the mistake of Title II and return to the light touch framework that served us so well during the Clinton administration, Bush administration, and first six years of the Obama administration."

The Verge writes:

His proposal will do three things: first, it'll reclassify internet providers as Title I information services; second, it'll prevent the FCC from adapting any net neutrality rules to practices that internet providers haven't thought up yet; and third, it'll open questions about what to do with several key net neutrality rules — like no blocking or throttling of apps and websites — that were implemented in 2015.

Pai said the full text of his net neutrality proposal would be published (last) Thursday afternoon. It'll be voted on by the FCC at a meeting on May 18th. From there, months of debate will follow as the item is opened up for public comment. The commission will then revise its rules based on the feedback it receives before taking a final vote to enact them.

Strong net neutrality rules were passed in 2015 and have been in place for about two years. Those rules reclassified internet providers as "common carriers" under Title II of the Telecommunications Act, which subject them to tough, utility-style regulation.

The FCC has previously mandated, under Title II, that internet providers follow a few key rules: no blocking of sites and apps, no throttling the speed of sites and apps, and no paid fast lanes. The rules applied to both wired and wireless internet providers and also gave the commission oversight of "interconnect" agreements between internet providers and big content companies like Netflix.

Internet providers have, of course, been unhappy about this, as they'd rather not have the FCC looking over their shoulder and limiting what they're able to do with their network. They sued to overturn the rules, but so far the rules have been held up in court.

But that may not last.

https://www.theverge.com/2017/4/26/15437840/fcc-plans-end-title-ii-net-neutrality

Cloudflare Launches "Orbit", a new service to Protect IoT Devices
(Note that Cloudflare is a sponsor of TWiT Network netcasts)
https://www.cloudflare.com/orbit/

Cloudflare: Technology is changing — shifting towards a world where low cost, connected chips power products used by billions of people around the world. Everything from jet turbines and oil rigs, to cars, cameras, and clothing are coming online. And while these tiny chips unlock incredible potential, they are a liability if not secure.

When PC vulnerabilities are discovered, software vendors issue a patch, which end users are required to download and install. These patches keep PC software up-to-date and secure. IoT devices also require patches, but the PC security model can't scale to 22 billion devices; IoT manufacturers often haven't built over-the-air (OTA) update mechanisms and are terrified that updates will brick a user's device. In the meantime, consumers never think about having to upgrade their internet-connected "toaster."

Cloudflare Orbit solves this problem at the network level by creating a secure and authenticated connection between an IoT device and its origin server. Orbit takes the Internet out of IoT: Behind Orbit, devices are I*oT.

Orbit allows device manufacturers to instantly deploy “virtual patches” and block vulnerabilities across all devices on the network simultaneously. This keeps malicious requests from reaching devices, buys time for IoT manufacturers to carefully QA their updates, and keeps devices from leaking data or launching DDoS attacks.

Orbit uses "mutual authentication" with client-side TLS certificates.

A spokesperson for Cloudflare said: “Orbit sits one layer before the device and provides a shield of security, so even if the device is running past its operating system’s expiration date, Cloudflare protects it from exploits. And while devices may be seldom patched, the Cloudflare security team is shipping code every day, adding new firewall rules to Cloudflare’s edge”

Orbit has been built in collaboration with a number of IoT vendors, and already protects over 120 million IoT devices. It allows IoT companies to write logic on Cloudflare’s edge and create firewall rules that are immediately updated to the Cloudflare Orbit layer for all devices, without having to write and ship a patch.

http://www.securityweek.com/cloudflare-launches-service-protect-iot-devices

Draft: Mozilla Proposal re: Symantec

- https://docs.google.com/document/d/1RhDcwbMeqgE2Cb5e6xaPq-lUPmatQZwx3Sn2NPz9jF8/mobilebasic
- Lots of back and forth between the Google Chrome team, Mozilla and Symantec.
- Symantec is, of course, pushing back as fiercely as possible and wanting to do as little as possible... while the browsers are attempting to both be and appear understanding and reasonable -- while also feeling that their true responsibility lies with their users who are inherently trusting their browsers to keep them safe.

Errata

Erwin Wessels (@htwj)
Hi @Sgrc, there are not individual emojis for each skin tone variety; they’re modifiers/ligatures!
"Emoji Diversity"
http://www.unicode.org/reports/tr51/#Diversity

The original "Smurf Yellow" -- and now five "human" skin tones.

From the Unicode / Emoji / Diversity spec:
People all over the world want to have emoji that reflect more human diversity, especially for skin tone. The Unicode emoji characters for people and body parts are meant to be generic, yet

following the precedents set by the original Japanese carrier images, they are often shown with a light skin tone instead of a more generic (nonhuman) appearance, such as a yellow/orange color or a silhouette.

Five symbol modifier characters that provide for a range of skin tones for human emoji are planned for Unicode Version 8.0 (released back in mid-2015). These characters are based on the six tones of the Fitzpatrick scale, a recognized standard for dermatology. The exact shades may vary between implementations.

F4Lc0N LoWNOISE (@falcon_lownoise)

- @SGgrc On #609: ETERNAL* & DOUBLE PULSAR came from NSA tools (EquationGroup) released by Shadow Brokers. Not part of @wikileaks Vault7 (CIA)

Joel Dittmer (@jdgeek)

(From the "There's got to be a simpler way to say this, dept.)

- (Re: punycode #securitynow #TWIT)
  Classic @SGgrc: *"I don't disagree that this was never not a bad idea!"*

Miscellany

https://badssl.com

- A slick test for the state of browser security features
- Also: https://www.ssllabs.com/ssltest/viewMyClient.html

Create a proxy server on an Amazon EC2 (VPC) instance

- https://gist.github.com/webinista/812c20247a6c21e639ce
- This will create a proxy server in whatever your availability zone your VPC is in. For me, that's us-east-1b. For you, that may be something different. Steps 10+ should more or less work regardless of your provider since those steps cover the setup and configuration of TinyProxy.

Agent 420, Jame Bong (@cybersexwario)

- @SGgrc I desperately need to play around with ChromaZone! How do I get it!?

Missile Guidance Explained Wonderfully

- https://www.youtube.com/watch?v=8e1ktRjeOuI

The Muppets Cookie Monster eats a machine...

- Google: Muppets Analytical Computer (4min : 10secs)
- https://www.youtube.com/watch?v=7IgF6_jVaj8

Keith Pottratz (@KeithPottratz)

- @SGgrc Got the first frontier saga book!
  Let me tell you wow amazing and I haven't been able to out it down!!!!

SpinRite

Brent Longborough (Brent Longborough)

- Hi, Steve. After years of shameless freeloading off a friend's Spinrite, today I purchased my own copy. Thanks and apologies.

Engrpiman (@Engrpiman)

- @SGgrc SpinRite saved my database server.
  RAID 1 disk failed. Used SR to bring drive back to life.
  Made Backup, Got new drives, restored from backup.

Closing The Loop Feedback:

John (@Mr_John_Morris)

- @SGgrc Listening to SN607 and thought I'd share the reality of Chrome Cookie settings, not respecting settings pic.twitter.com/xBBvFCT3ua

  (Some browsers will continue to store but not to send cookies. Some will even continue to receive and update but not store cookies. This is why I created the Cookie Forensics page.)

Richard Hardy (@PatronusOpacus)

- @SGgrc Watching the Security Now Double Pulsar. I had a thought about the port 445 being, what about PCs being in DMZ?

Joan (@joanlarma)

- @SGgrc There are ads related to my location popping up on my facebook feed. How do I stopped this if setting up a vpn isn't enough?

Nate G. (@nategies)

- @SGgrc The biggest roadblock w/ getting friends & family onboard with a password vault solution has been the master p/w. Any suggestions?
- @SGgrc My wife, for example, sees the benefit of them, but has had problems remembering a high entropy p/w in the past. Unwilling to try again now.

  Nate, Best advice would be to use five memorable real words with one deliberate misspelling. Not the best possible, but not a bad compromise.