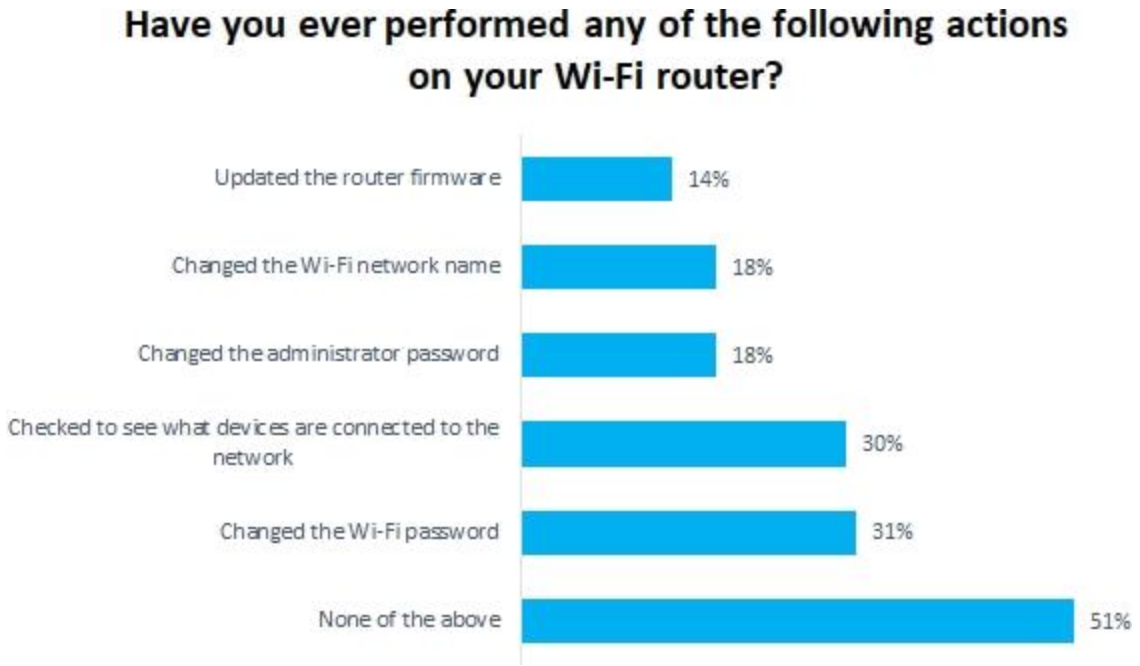
Security Now! #660 - 04-24-18

Azure Sphere

This week on Security Now!

This week we discuss Drupalgeddon2 continuing to unfold right on plan, the Orangeworm takes aim at medical equipment and companies, the FDA moves forward on requiring device updates, Microsoft leads a new Cybersecurity Tech Accord, another instance of loud noises and hard drives not mixing, considerations for naming your WiFi network, the unappreciated needs of consumer routers, Google's new unencrypted messaging app push, Amazon pulls the trigger on "in-car" package delivery, the first puzzle recommendation in a long time, and Microsoft's move to secure the IoT space.



Security News

Drupalgeddon2: (Unfortunately) Everything is proceeding according to plan.

Two weeks ago, tomorrow, on April 11th, Drupal released the critical patches to their CMS.

The next day the first PoC appeared. Several since.

Scan for vulnerable sites began within hours.

The passive scans quickly evolved into malicious activity: Coinminers, PHP backdoors, and Perl bots.

Several of the malicious payload are, themselves, scanners, meaning that we have Drupalgeddon2 based worms.

Three large "Tsunami" botnets have been seen to have added the Drupalgeddon 2 vulnerability to their existing exploit collection.

ArsTechnica: "Bug patched in March is still being exploited to take full control of servers." STILL?!?!? It is never =NOT= going to be exploited!!

And, now... there's ==ANOTHER== new problem with Drupal:

Date: 2018-April-18 / https://www.drupal.org/sa-core-2018-003

"Moderately Critical": CKEditor, a third-party JavaScript library included in Drupal core, has fixed a cross-site scripting (XSS) vulnerability. The vulnerability stemmed from the fact that it was possible to execute XSS inside CKEditor when using the image2 plugin (which Drupal 8 core also uses).

https://ckeditor.com/blog/CKEditor-4.9.2-with-a-security-patch-released/

According to a security advisory released by CKEditor, the XSS vulnerability stems from the improper validation of "img" tag in Enhanced Image plugin for CKEditor 4.5.11 and later versions. This could allow an attacker to execute arbitrary HTML and JavaScript code in the victim's browser and gain access to sensitive information.

Enhanced Image plugin was introduced in CKEditor 4.3 and supports an advanced way of inserting images into the content using an editor.

CKEditor has patched the vulnerability with the release of CKEditor version 4.9.2, which has also been patched in the CMS by the Drupal security team with the release of Drupal version 8.5.2 and Drupal 8.4.7.

The "Orangeworm"
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Since early 2015, someone has been quietly targeting medical organizations.

Dubbed "Orangeworm," an unknown hacking group has been found installing a wormable trojan on machines hosting software used for controlling high-tech imaging devices, such as X-Ray and MRI machines, as well as machines used to assist patients in completing consent forms.

<SYMANTEC> Symantec has identified a previously unknown group called Orangeworm that has been observed installing a custom backdoor called Trojan.Kwampirs within large international corporations that operate within the healthcare sector in the United States, Europe, and Asia.

First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply-chain attack in order to reach their intended victims. Known victims include healthcare providers, pharmaceuticals, IT solution providers for healthcare and equipment manufacturers that serve the healthcare industry, likely for the purpose of corporate espionage.

Based on the list of known victims, Orangeworm does not select its targets randomly or conduct opportunistic hacking. Rather, the group appears to choose its targets carefully and deliberately, conducting a good amount of planning before launching an attack.

While Orangeworm is known to have been active for at least several years, we do not believe that the group bears any hallmarks of a state-sponsored actor—it is likely the work of an individual or a small group of individuals. There are currently no technical or operational indicators to ascertain the origin of the group.

The FDA takes action on medical devices.
https://assets.documentcloud.org/documents/4442378/Medical-Device-Safety-Action-Plan.pdf

"Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health"

Introduction
Medical devices play a crucial role in the treatment and diagnosis of illness and disease. They range from common medical supplies (bandages, hospital gowns) to complex instruments that help save and sustain life (heart valves, artificial pancreas). They include tools that aid in the detection of disease (MRIs, in vitro diagnostics) and digital technology that is driving a revolution in health care (medical apps, surgical planning tools, closed loop drug delivery devices). The Food and Drug Administration (FDA) regulates over 190,000 different devices, which are manufactured by more than 18,000 firms in more than 21,000 medical device facilities worldwide. Although medical devices provide great benefits to patients, they also present risks. FDA’s public health responsibilities span the life cycle of medical devices and, at every stage, FDA must make well-supported regulatory decisions, taking into account the totality of the evidence,
to determine whether the benefits outweigh the risks.

4. Advance medical device cybersecurity

FDA plans to:
Consider potential new premarket authorities to require firms, on the front end, to: (i) build-in capability to update and patch device security into a product's design and to provide appropriate data regarding this capability to FDA as part of the device's premarket submission; and, (ii) develop a "Software Bill of Materials" that must be provided to FDA as part of a premarket submission and made available to medical device customers and users, so that they can better manage their networked assets and be aware of which devices in their inventory or use may be subject to vulnerabilities. In addition, availability of a "Software Bill of Materials" will enable streamlining of timely postmarket mitigations.

The "Cybersecurity Tech Accord"
First described at LAST year's RSA conference by Microsoft's Chief Legal Officer Brad Smith.

At THIS year's RSA conference the 'accord' was announced.

https://cybertechaccord.org/
https://cybertechaccord.org/accord/

- Strong defense - Tech companies should do their best to protect users from any type of cyber-attack, regardless of source, or the user's native country.

- No offensive development - Tech companies should never provide material support to government-backed cyber-attacks.

- Capacity building - Companies should build and provide customers with the necessary tools to protect their data and themselves from state-sponsored attacks.

- Collective action - Companies will collaborate with each other to share data on attacks and disclose attacks to affected users.

The accord notes that while companies may have already been adhering to some or all of these principles prior to the accord, and may have done so without a public commitment... this agreement represents a public shared commitment to collaborate on cybersecurity efforts. The Tech Accord remains open to consideration of new private sector signatories, large or small and regardless of sector, who are trusted, have high cybersecurity standards and will adhere unreservedly to the Accord’s principles.

Kevin Simzer, Chief Operating Officer, Trend Micro: “The real world consequences of cyber threats have been repeatedly proven. As an industry, we must band together to fight cybercriminals and stop future attacks from causing even more damage.”

The victims of cyberattacks are businesses and organizations of all sizes, with economic losses expected to reach $8 trillion by 2022.* Recent cyberattacks have caused small businesses to shutter their doors, hospitals to delay surgeries and governments to halt services, among other disruptions and safety risks.

Carolyn Herzog, General Counsel, Arm: “The Tech Accord will help to protect the integrity of the one trillion connected devices we expect to see deployed within the next 20 years. It aligns the resources, expertise and thinking of some of the world’s most important technology companies to help to build a trusted foundation for technology users who will benefit immensely from a more security connected world.”

Companies that signed the accord plan to hold their first meeting during the security-focused RSA Conference taking place in San Francisco, and will focus on capacity building and collective action. Future actions may include jointly developed guidelines or broadly deployed features, as well as information sharing and partnering to combat specific threats to make the online world a safer place for people and businesses everywhere — and uphold the promise and benefit technology offers society.

Who's in and who's not?

34 tech companies we all know are in:
ABB, ARM, AVAST, BITDEFENDER, BT, CA TECHNOLOGIES, CISCO, CLOUDFLARE, DATASTAX, DELL, DOCUSIGN, FACEBOOK, FASTLY, FIREEYE, F-SECURE, GITHUB, GUARDTIME, HP INC, HPE, INTUIT, JUNIPER NETWORKS, LINKEDIN, MICROSOFT, NIELSEN, NOKIA, ORACLE, RSA, SAP, STRIPE, SYMANTEC, TELEFONICA, TENABLE, TREND MICRO, VMWARE

Notably absent are Amazon, Apple, Google and Intel.

Screaming at Hard Drives is not a good idea...
https://www.bleepingcomputer.com/news/technology/loud-sound-from-fire-alarm-system-shuts-down-nasdaqs-scandinavian-data-center/

In the early hours of last Wednesday, April 18th, the loud sound emitted by the high pressure release of inert gas used in a data center's fire suppression system destroyed the hard drives of a Swedish data center, taking down the NASDAQ stock exchange operations across Northern Europe.

Sound is vibration... and modern drives are known to be very sensitive to vibration.

When this is coupled with resonance, the effect can be amplified.

Be careful what you name your WiFi network...
https://www.bleepingcomputer.com/news/legal/are-wifi-network-names-protected-by-the-first-amendment/

Michigan police were called at a Planet Fitness gym earlier this month to investigate a bomb threat that ended up being only a prank after someone at the gym named their WiFi network "Remote Detonator."

The gym patron spotted the suspicious WiFi network name and called the police, following the gym's normal procedures. The gym re-opened the same day, three hours later, after bomb-sniffing dogs swept the building without finding any explosive devices.

The Saginaw Township Police Chief Donald Pussehl told a local paper: "Everything is perfectly legal from a police standpoint. There was no crime or threat. No call saying there was a bomb."

The chief said the WiFi name falls under what is considered "protected speech" under the First Amendment.

<quote> But we at Bleeping Computer wanted to confirm the Saginaw Township Police Chief's statement to see whether WiFi network names do really fall under the First Amendment. So we asked one of the leading law firms specialized in free speech cases, the Walters Law Group, the firm behind the FirstAmendment.com website.

"All speech that is intended to convey a message is presumed to be protected by the First Amendment," a spokesperson for the Walters Law Group told Bleeping Computer earlier this week via email.

"This can get complicated with identifiers like telephone numbers, addresses, or domain names, which typically do not enjoy First Amendment protection," the spokesperson said. "But there are exceptions."

"A domain name could be both convey a message and identify a location at the same time. The same goes for a WiFi network name," he said. "While typically used to identify a network, the chosen name could be used to convey a message of humor, politics, or even danger."

Name your WiFi responsibly...

Situations like these happened in the past. For example, in 2016, a passenger on a Qantas flight had named his WiFi hotspot "Mobile Detonation Device," which grounded a flight for hours before it was cleared to take off.

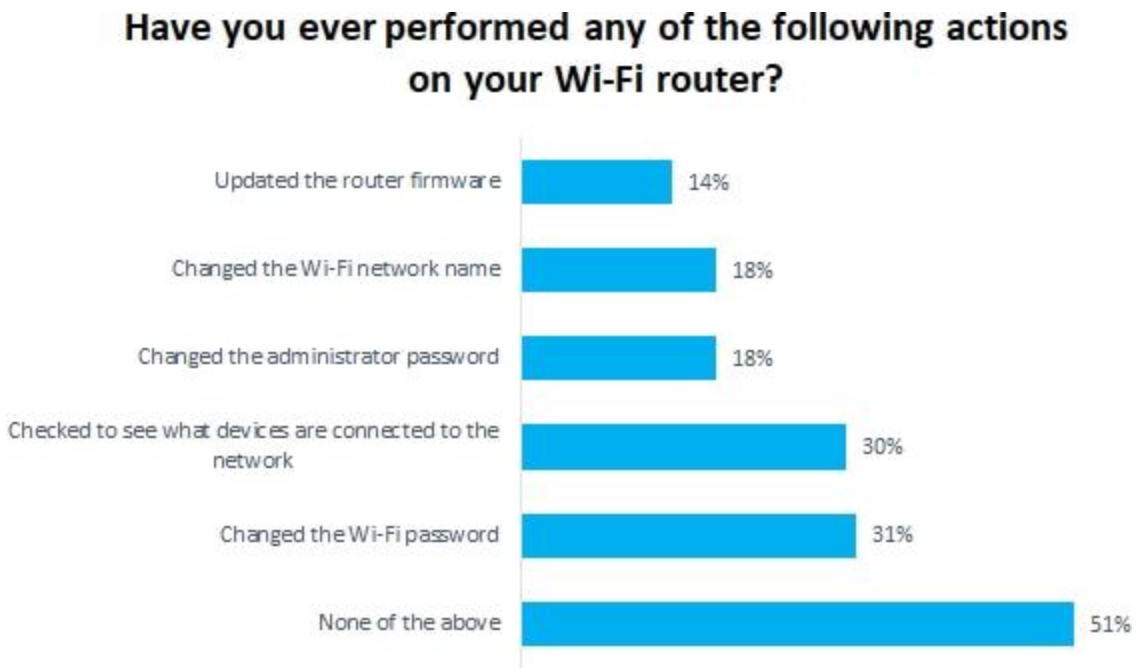
In 2017, a Turkish Airlines airplane made an emergency landing at a Sudan airport after a passenger discovered a WiFi network created by another passenger named "Bomb on board."

The trouble with our consumer routers:

- They are "plug n' go"
- They use DHCP to get their IP from the ISP.
- They serve DHCP to connect everyone inside the network.
- They are sold as appliances, but they are sophisticated publicly exposed computers.

https://www.broadbandgenie.co.uk/blog/20180409-wifi-router-security-survey

UK based Broadband Genie surveyed 2,205 age >18, asking whether they had carried out simple tasks like changing their Wi-Fi password, changing their router admin password or updating the router's firmware. Unsurprisingly, they discovered that very few had:



Google "Chat" for Android
Google (successfully) pushes the entire sprawling cellular industry to support RCS "Universal Profile"
https://www.gsma.com/futurenetworks/rcs/universal-profile/
https://www.theverge.com/2018/4/19/17252486/google-android-messages-chat-rcs-anil-sabharwal-imessage-texting

But... Whoops!... since it's carrier-to-carrier, enhanced SMS/MMS -- =NO= Encryption.

"Universal Profile for Rich Communication Services."

Announced today: Amazon will deliver packages to the trunk of your car
https://www.theverge.com/2018/4/24/17261744/amazon-package-delivery-car-trunk-gm-volvo

Amazon announced today a new service that gives its couriers access to a person's vehicle for the purpose of leaving package deliveries inside.

GM (General Motors) and Volvo

Rolling out in 37 cities in the US starting today.

Not eligible for in-car delivery are packages:

- Weighing 50 pounds
- Larger than 26 x 21 x 16 inches
- Requiring a signature
- Valued over $1,300
- From a third-party seller.

To access the new delivery service, you:

- Add your car to your Amazon Key app
- Include a description of the vehicle so Amazon's couriers will be able to locate it

The car must be parked within a certain distance of an address normally used for Amazon deliveries (so not some other state) -- i.e. home or work.

Driveways, parking lots, parking garages, and street parking are all eligible locations, just as long as it's not at some random address across town.

Miscellany

Previous hits:

- Infinite Loop - engaging and relaxing
- The Sequence - visual programming
- Blockwick - a terrific take on the sliding block puzzle

Steve's first puzzle pick in a long time:
$3 / "Dissembler" / Feb 21, 2018

- A brand new, original, simple and clean concept.
- No timer. No ads. No annoyances.
- Easy "whoops" undo without limit.
- Nice background music (mutable).

Azure Sphere

Microsoft proposes a secure solution for IoT

- https://www.microsoft.com/en-us/azure-sphere/
- https://azure.microsoft.com/en-us/blog/introducing-microsoft-azure-sphere-secure-and-power-the-intelligent-edge/
- https://www.microsoft.com/en-us/research/publication/seven-properties-highly-secure-devices/
- https://www.microsoft.com/en-us/research/project/sopris/
- https://www.microsoft.com/en-us/research/blog/from-research-idea-to-research-powered-product-behind-the-scenes-with-azure-sphere/

Azure Sphere is:

- A custom chip design - "MediaTek MT3620"
- A Linux Distro - "Azure Sphere OS"
- A cloud-based service
- All the for sole purpose of securing IoT.
- … and =ALL= completely open and freely available without licensing.

The Linux distro is open source and the chip's design is 100% free for anyone to make.

The first chips will be available later this year from the Taiwanese MediaTek (not the ASMedia who produced the AMD backdoored chipsets!) ⇒ MediaTek MT3620

Microsoft has also released the Azure Sphere Security Service, a cloud service that continually scans Azure Sphere devices for security anomalies.

https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf

Hardware-based Root of Trust

- Unforgeable cryptographic keys generated and protected by hardware. Physical countermeasures resist side-channel attacks.
- Does the device have a unique, unforgeable identity that is inseparable from the hardware?

Small Trusted Computing Base

- Private keys stored in a hardware-protected vault, inaccessible to software. Division of software into self-protecting layers.
- Is most of the device's software outside the device's trusted computing base?

Defense in Depth

- Multiple mitigations applied against each threat. Countermeasures mitigate the consequences of a successful attack on any one vector.
- Is the device still protected if the security of one layer of device software is breached?

Compartmentalization

- Hardware-enforced barriers between software components prevent a breach in one from propagating to others.
- Does a failure in one component of the device require a reboot of the entire device to return to operation?

Certificate-based Authentication

- Signed certificate, proven by unforgeable cryptographic key, proves the device identity and authenticity.
- Does the device use certificates instead of passwords for authentication?

Renewable Security

- Renewal brings the device forward to a secure state and revokes compromised assets for known vulnerabilities or security breaches.
- Is the device's software updated automatically?

Failure Reporting

- A software failure, such as a buffer overrun induced by an attacker probing security, is reported to cloud-based failure analysis system.
- Does the device report failures to its manufacturer?

Azure Sphere Open Cloud
The Azure Sphere Security Service guards every Azure Sphere device. It renews security, identifies emerging threats, and brokers trust between device, cloud, and other endpoints.

Protecting devices with certificate-based authentication

- Guaranteeing device authenticity and running only your genuine software
- Getting insight into device and application failure and visibility into emerging threats
- Deploys app updates to your Azure Sphere powered devices

Azure Sphere gives you choice. You can connect data from any cloud, proprietary or public, or even to your on-prem infrastructure to the Azure Sphere Security Service.

- Informing your app with data
- Storing telemetry and insights
- Providing customer information
- Housing commerce and other transactions