Security and Proprietary Software Leftovers

By Roy Schestowitz
Created 21/03/2020 - 12:00pm
Submitted by Roy Schestowitz on Saturday 21st of March 2020 12:00:32 PM Filed under Security [1]

---

Security updates have been issued by Arch Linux (bluez and chromium), Debian (icu, rails, thunderbird, and twisted), Fedora (chromium and webkit2gtk3), Gentoo (bsdiff, cacti, clamav, fribidi, libgit2, pecl-imagick, phpmyadmin, pyyaml, and tomcat), openSUSE (wireshark), Oracle (firefox, icu, python-imaging, thunderbird, and zsh), Scientific Linux (thunderbird), SUSE (firefox, nghttp2, thunderbird, and tomcat), and Ubuntu (twisted).

---


For malicious people, preying on collective fear and misinformation is nothing new. Mentioning national headlines can lend a veneer of credibility to scams. We’ve seen this tactic time and again, so it's no surprise that COVID-19 themed social media and email campaigns have been popping up online. This blogpost provides an overview to help you fight against phishing attacks and malware, examples of phishing messages we’ve seen in the wild related to coronavirus and COVID-19, and specific scenarios to look out for (such as if you work in a hospital, are examining maps of the spread of the virus, or are using your phone to stay informed).

The COVID-19 themed scam messages are examples of "phishing," or when an attacker sends a message, email, or link that looks innocent, but is actually malicious and designed to prey on fears about the virus. Phishing often involves impersonating someone you know or impersonating a platform that you trust. Your day-to-day diligence is the best preventative measure. Consider these points before you click: Is it an enticing offer? Is there a sense of urgency? Have you interacted with the sender before over this platform?
Librem Hardware and the Intel CSME Vulnerability [4]

Whenever a security vulnerability comes out one of the first questions that come to many people's minds is: am I affected? The last couple of years in particular have seen a lot of hardware-based vulnerabilities in Intel processors and in those cases generally it's a matter of looking at the affected list of hardware and comparing it against your own hardware.

More recently a vulnerability (CVE-2019-0090) was announced in the Intel CSME that can allow an attacker with local access to potentially extract secret Intel hardware signing keys from a system. There are a number of different analyses out there on this vulnerability from the very dry CVE report itself to 'sky is falling' reports that contain a lot more hype. If you want more technical details on the vulnerability itself, I've found this report to have a good balance of measured technical information on impact without the hype.

Hackers leak internal documents showing the FSB's quest for a cyber-weapon that can take whole nations offline [5]

The hacker group Digital Revolution? has released documents describing a procurement order from a division of Russia's Federal Security Service (FSB) for the development of Fronton? software that would enable cyberattacks using infected Internet-of-Things (IoT) devices. The BBC's Russian-language service was the first media outlet to report this story.

[...]

In total, according to the hackers' data, there are three versions of the software: Fronton, Fronton-3D, and Fronton-18. The programs can infect any smart device (from digital assistants to 'smart' homes), connecting them into a network and then attacking the servers responsible for the stability of online services and the Internet itself in entire countries.

Based on the documents, FSB contractors recommended creating botnets 95-percent comprising IP cameras and digital video recorders (cameras that receive control data and send image data via the Internet). If they transmit video, the leaked materials state, they have a big enough communication channel to perform DDoS attacks effectively. The project suggests hacking these devices by using a dictionary of typical passwords used for IoT devices.

Windows, Ubuntu, macOS, VirtualBox fall at Pwn2Own hacking contest [6]

The 2020 spring edition of the Pwn2Own hacking contest has come to a close today.

This year's winner is Team Fluoroacetate -- made up of security researchers Amat Cama and Richard Zhu -- who won the contest after accumulating nine points across the two-day competition, which was just enough to extend their dominance and win their fourth tournament in a row.
But this year's edition was a notable event for another reason. While the spring edition of the Pwn2Own hacking contest takes place at the CanSecWest cyber-security conference, held each spring in Vancouver, Canada, this year was different.

- **Once upon a time there was a WebSocket** [7]

  This is the story from one of our recent penetration testing engagements. Still, the story is a familiar one for those who are testing newer web applications that use one of the multitudes of evolving web app platforms built on a poorly understood technology stack. In this case, we ran into a WebSocket-based application that was thought to be relatively secure; however, the use of web sockets in the application was misunderstood, resulting in a significant set of authentication and authorization flaws.

- **ESET Releases Latest Version of ESET Endpoint Antivirus for Linux** [8]

  ESET has launched the latest version of ESET Endpoint Antivirus for Linux, ensuring all organizations are protected to the highest standard, no matter the operating system. Endpoint Antivirus for Linux joins ESET's extensive product range, which already caters extensively to Windows and MacOS.

  ESET Endpoint Antivirus for Linux is designed to provide advanced protection from threats to organizations’ general desktops. Powered by the advanced ESET LiveGrid technology, the solution combines speed, accuracy and minimal system impact, leaving more system resources for the desktops' vital tasks in order to maintain business continuity.

- **Zoom bombing?: When Video Conferences Go Wrong** [9]

  Zoom has become the default social platform for millions of people looking to connect with friends, family, students and colleagues while practicing social distancing during the new coronavirus pandemic.

  But the trolls of the internet are under quarantine, too, and they're looking for Zooms to disrupt.
They are jumping into public Zoom calls and using the platform’s screen-sharing feature to project graphic content to unwitting conference participants, forcing hosts to shut down their events.

Zyxel Flaw Powers New Mirai IoT Botnet Strain [10]

A joint advisory on CVE-2020-9054 from the U.S. Department of Homeland Security and the CERT Coordination Center rates this vulnerability at a ?10? — the most severe kind of flaw. The DHS/CERT advisory also includes sample code to test if a Zyxel product is vulnerable to the flaw.

My advice? If you can’t patch it, pitch it, as Mukashi is not the only thing interested in this Zyxel bug: Recent activity suggests attackers known for deploying ransomware have been actively working to test it for use against targets.

Discord says it’s banning millions of accounts to tackle spam [11]

Discord banned 5.2 million accounts between April and December last year, the company revealed today in its second transparency report. The most common reasons for account bans were spam and exploitative content, which includes nonconsensual pornography (so-called “revenge porn”) as well as sexual content related to minors.

The report reveals a stark difference in the kinds of violations that most users are likely to report, versus the actions that are most likely to get people and servers banned. The most common reports Discord receives from users relate to harassment, however only a relatively small proportion of these reports actually result in action being taken. Discord says that in many cases it will teach people how to block the offending user without taking any further
Server Outages and Increased API Errors: Incident Report for Discord

Discord was unavailable for most users for a period of an hour. The root cause is well understood and fixed. The bug was in our service discovery system, which is used by services within our infrastructure to discover one another. In this instance, service discovery is used by our real time chat services services in order to discover the RPC endpoint that they use to load data from our databases when you connect to Discord, or when a Discord server (or "guild") is created for the first time, or needs to be re-loaded from the database.

Google suspends Chrome upgrades as COVID-19 impacts software schedules

According to a now-outdated Chrome release schedule, Google was supposed to upgrade the browser to version 81 on Tuesday, March 17. Chrome OS was to shift to version 81 on March 24. Google had both on a metronomic schedule that delivered new features every six to eight weeks.

Also on Wednesday, Google updated Chrome 80 ? the version that debuted Feb. 4 ? to build 80.0.3987.149, which contained fixes for 13 security vulnerabilities. The nine that Google called out in a separate post were all rated as "High," the second-most-serious threat ranking in a four-step scoring system. Only one of the nine noted a bug bounty amount ? $8,500 ? and five other bug listings said that a cash reward would be determined later.

Apple Briefly Dips Below $1 Trillion Level It Held Since October
Coronavirus-related weakness has already evicted two names from the thirteen-digit club: Amazon.com Inc. and Google-parent Alphabet Inc. Both rose above the threshold earlier this year but fell back below $1 trillion in late February.

**Source URL:** [http://www.tuxmachines.org/node/135438](http://www.tuxmachines.org/node/135438)

**Links:**
1. [http://www.tuxmachines.org/taxonomy/term/59](http://www.tuxmachines.org/taxonomy/term/59)
2. [https://lwn.net/Articles/815591/rss](https://lwn.net/Articles/815591/rss)
7. [https://blog.secureideas.com/2020/03/once-upon-a-time-there-was-a-websocket.html](https://blog.secureideas.com/2020/03/once-upon-a-time-there-was-a-websocket.html)
12. [https://status.discordapp.com/incidents/62gt9cgjwdgf](https://status.discordapp.com/incidents/62gt9cgjwdgf)