Security Leftovers

By Roy Schestowitz
Created 23/03/2020 - 4:05pm
Submitted by Roy Schestowitz on Monday 23rd of March 2020 04:05:40 PM Filed under Security [1]

- Security updates for Monday [2]

Security updates have been issued by Debian (amd64-microcode, chromium, graphicsmagick, jackson-databind, phpmyadmin, python-bleach, and tor), Gentoo (exim and nodejs), openSUSE (chromium and thunderbird), Oracle (tomcat), Red Hat (devtoolset-8-gcc, libvncserver, runc, samba, thunderbird, and tomcat6), and SUSE (ruby2.5).

- No, the head of the World Health Organization has not emailed you? it's a message laced with malware [3]

As happens every time there is a major news event, scumbags exploit the public's interest to spread malware. This time, criminals have picked on the World Health Organization's handling of the global COVID-19 coronavirus pandemic. Researchers at IBM X-Force report the HawkEye malware is being spread under the guise of an email alert from WHO director general Tedros Adhanom Ghebreyesus.

Victims are asked to open an attachment, launching the password-and-Bitcoin-harvesting Windows malware.

"One thing worth mentioning is that the attackers put some effort in hiding the real intention of it," X-Force said. "The environmental awareness of our sample was quite good and average users would most likely not notice an info-stealer being installed."

- Security 101: Virtual Private Networks (VPNs) [4]
I'm trying something new - a Security 101 series. I hope to make these topics readable for those with no security background. I'm going to pick topics that are either related to my other posts (such as foundational knowledge) or just things that I think are relevant or misunderstood.

Today, I want to cover Virtual Private Networks, commonly known as VPNs. First I want to talk about what they are and how they work, then about commercial VPN providers, and finally about common misconceptions.

Pwn2Own contest yields 13 bugs, as virtual format expands talent pool[5]

Research teams at the Pwn2Own 2020 competition successfully exploited 13 software vulnerabilities this past week, including bugs found in products from Adobe, Apple, Microsoft, Oracle and Ubuntu. Participants earned $270,000 over the two-day event - the first Pwn2Own ever to be held virtually, as a measure to combat the rapid spread of the novel coronavirus.

Richard Zhu and Amat Cama of Fluoroacetate repeated from last year and were once again crowned Masters of Pwn. On day one, the team demonstrated a use-after-free (UAF) bug in Microsoft Windows and exploited it to escalate privileges to SYSTEM. The next day, they paired UAF bugs in Windows and Adobe Reader to once again elevate to SYSTEM.

Other highlights included the chaining of six bugs to produce a macOS kernel escalation of privilege in Apple Safari, another Windows UAF flaw allowing the escalation of privileges to SYSTEM, a local privilege escalation in Ubuntu Desktop, and a two-bug combination in Oracle VirtualBox that enabled code execution on the host OS from the guest OS. Unofficially, the event also featured one additional flaw in VMware Workstation and another in Oracle VirtualBox, although they did not count toward the competition.