Security Leftovers

By Roy Schestowitz
Created 29/04/2020 - 5:59pm
Submitted by Roy Schestowitz on Wednesday 29th of April 2020 05:59:09 PM Filed under Security [1]

- **Security updates for Wednesday** [2]


- **Massive & Unprecedented Security Breach Takes Usenet Providers Offline** [3]

  A massive security breach has taken at least one major Usenet provider offline. UseNext says that a "security hole in a partner company" could have revealed names and bank account information, exposing customers to fraud and identity theft. The precise nature of the breach isn't clear but reports that a Usenet client has been stealing login credentials is being linked to the security disaster.
How to avoid Coronavirus scam websites, calls, and texts

The COVID-19 pandemic has brought out the best and worst in human society. While people around the world have come together in solidarity to try and flatten the curve and frontline essential workers are still keeping everyone fed, the scammers of the world have taken this as a golden opportunity to try and steal from people just when they need their money the most.

Endangered users of Windows, macOS and Linux. Critical vulnerability detected in all popular antiviruses

Vulnerability experts tested and found a "hole" in 28 popular antivirus programs, including Microsoft Defender (Windows Defender), Avast, Kaspersky, and many others. Moreover, it acts not only on Windows but macOS with Linux.

According to experts, antivirus packages have errors that allow hackers to delete files, cause serious system crashes, and install malware. Depending on the operating system, vulnerabilities can be exploited in various ways. It is based on the already known type of vulnerability called Symlink, which originates in the unsafe creation of files by a program.

Rack911 Labs notes: During testing on Windows, macOS, and Linux, we were able to easily delete important files related to antivirus software, which resulted in the loss of efficiency or even deletion of key files of the operating system, which could cause significant damage requiring a complete reinstallation of the OS.

We're going on a vuln hunt. We're going to catch a big one: Researchers find Windows bugs dominate — but fixes are fast

A study of vulnerabilities - bugs that can be a gateway for malware or allow privilege escalation by an intruder - shows that Windows platforms have the most by far, but that they also tend to be fixed quickly, compared to Linux systems or appliances like routers, printers and scanners.

Kenna Security has published a report based on "vulnerability data culled from more than 9 million active assets across nearly 450 organizations," gathered by its cybersecurity research partner Cyentia Institute and based in part on data from automated vulnerability scanners.

Why voting online is not the way to hold an election in a pandemic

Yet online voting faces serious, possibly insurmountable obstacles. Even its keenest cheerleaders acknowledge that it should complement, not replace, other methods. The
The consensus among experts is that the technology remains vulnerable to security breaches and cyber-attacks. Malware can tamper with votes before they reach government servers. Hackers can create mirror versions of an election portal, steal voter credentials, or attack computers that count and store online ballots. A recent paper by the International Foundation for Electoral Systems, a non-profit group, concludes that countries without experience of online voting should not contemplate rolling it out in response to the covid-19 crisis. The cure would be worse than the disease.

Several people [attacking]: Feds turn to civilian Slack groups for help during coronavirus

The Cyber Threat Coalition is one of two Slack groups ? the CTI League is the other ? created in recent weeks by civilian cybersecurity professionals who wanted to put their heads together and try to stem the rising tide of cybercrime that?s flooded the [Internet] amid the coronavirus pandemic.

Both groups vet each new member and have still quickly swelled to thousands of users worldwide. And notably, each quickly saw an influx of government agents, leading to an unprecedented situation in which technology employees regularly find themselves chatting in [Internet] chat rooms with cyber cops around the world, each identified by their real name and agency.

[Old] Your Slack DMs aren?t as private as you think

It?s also possible that your employer has invested in a higher-level plan, like Enterprise Grid. Those plans work with third-party apps like Hanzo that allow employers to store messages and other information. Companies may need to consistently preserve electronic communications for review by regulatory agencies, such as the Securities and Exchange Commission (SEC) and the Financial Industry Regulation Authority.

[Old] Slack updates privacy policy: Employers can read 'private' DMs without telling workers

Under the updated policy, which starts on April 20, compliance reports are being discontinued and the downloading options expanded. According to the Slack website: [...]
[2] https://lwn.net/Articles/818950/rss