Security Newsletter

18 May 2020

Subscribe to this newsletter

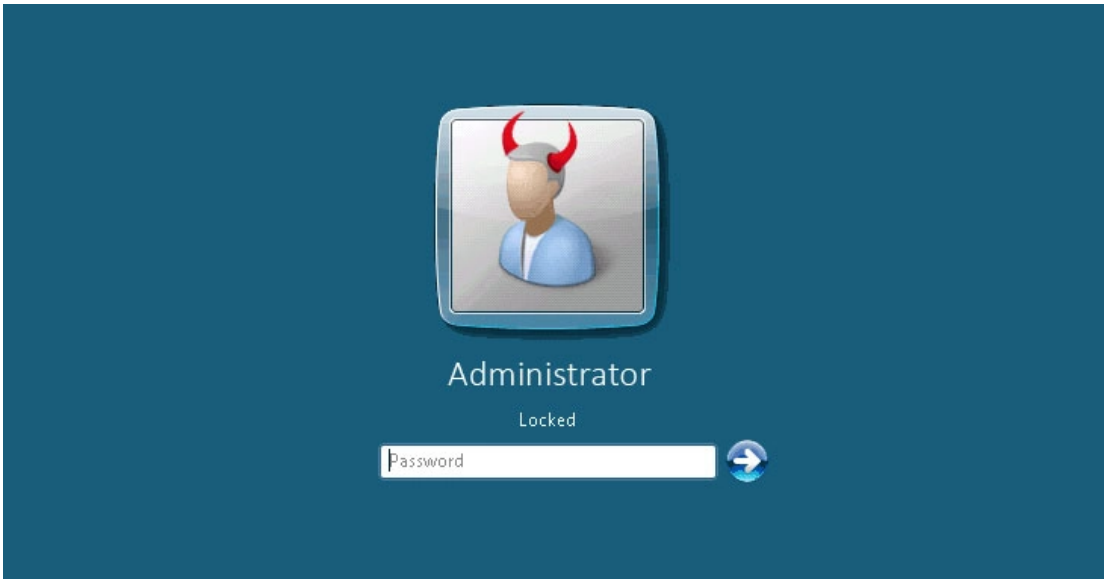
The Confessions of Marcus Hutchins, the Hacker Who "Saved" the Internet

At 22, he single-handedly put a stop to the worst cyberattack the world had ever seen. Then he was arrested by the FBI. This is his untold story.

At around 7 am on a quiet Wednesday in August 2017, Marcus Hutchins walked out the front door of the Airbnb mansion in Las Vegas where he had been partying for the past week and a half. A gangly, 6'4", 23-year-old hacker with an explosion of blond-brown curls, Hutchins had emerged to retrieve his order of a Big Mac and fries from an Uber Eats deliveryman. But as he stood barefoot on the mansion's driveway wearing only a T-shirt and jeans, Hutchins noticed a black SUV parked on the street—one that looked very much like an FBI stakeout. He stared at the vehicle blankly, his mind still hazed from sleep deprivation and stoned from the legalized Nevada weed he'd been smoking all night. For a fleeting moment, he wondered: Is this finally it?

Read More on Wired

Improper Microsoft Patch for Reverse RDP Attacks Leaves 3rd-Party RDP Clients Vulnerable



Remember the Reverse RDP Attack—wherein a client system vulnerable to a path traversal vulnerability could get compromised when remotely accessing a server over Microsoft's Remote Desktop Protocol? Though Microsoft had patched the vulnerability (CVE-2019-0887) as part of its July 2019 Patch Tuesday update, it turns out researchers were able to bypass the patch just by replacing the backward slashes in paths with forward slashes. Microsoft acknowledged the improper fix and re-patched the flaw in its February 2020 Patch Tuesday update earlier this year, now tracked as CVE-2020-0655.

Apparently, the workaround works fine for the built-in RDP client in Windows operating systems, but the patch is not fool-proof enough to protect other third-party RDP clients against the same attack that relies on the vulnerable sanitization function developed by Microsoft. "We want developers to be aware of this threat so that they could go over their programs and manually apply a patch against it."

Read More on Bleeping Computer

New Thunderbolt security flaws affect systems shipped before 2019

Attackers who gain physical access to Windows, Linux, or macOS devices can access and steal data from their hard drives by exploiting 7 vulnerabilities found in Intel's Thunderbolt hardware interface and collectively known as Thunderspy.

Thunderbolt is a hardware interface designed by Intel and Apple in collaboration to help connect external peripherals that need high-speed connections (RAID arrays, network interface, video capture devices, and others) to a computer. The new attack, discovered by Eindhoven University of Technology researcher Björn Ruytenberg, is designed to break Thunderbolt's security, making it possible for attackers to steal information from any vulnerable Thunderbolt-enabled device.

For Linux and Windows users, all systems purchased before 2019 are vulnerable to Thunderspy attacks according to Ruytenberg, while devices bought during and after 2019 might come with support for Kernel DMA Protection which protects against drive-by Direct Memory Access attacks. Similarly, Macs from 2011 and older, except for Retina MacBooks, are all impacted by Thunderspy as they all provide users with Thunderbolt connectivity. Intel confirmed that the vulnerabilities are valid but will not mitigate the Thunderspy vulnerabilities by issuing a patch to already sold and known to be vulnerable devices as they would require a silicon redesign.

Read More on BleepingComputer

More #News

- Researcher finds 1,236 websites infected with credit card stealers
- Empowering your remote workforce with end-user security awareness
- A cybercrime store is selling access to more than 43,000 hacked servers
- Microsoft Office 365 ATP getting malware campaign analysis
- Ransomware Reminder: Paying Ransoms Doesn't Pay
- Ransomware now demands extra payment to delete stolen files
- Windows 10 to get PUA/PUP protection feature
- Over 4000 Android Apps Expose Users' Data via Misconfigured Firebase Databases
- DigitalOcean Inadvertently Exposed Customer Data
- Microsoft and Intel project converts malware into images before analyzing it
- ChatBooks discloses data breach after data sold on dark web
- The Confessions of Marcus Hutchins, the Hacker Who "Saved" the Internet

#Patch Time!

- SAP May 2020 Security Patch Day delivers critical updates
- Adobe issues patches for 36 vulnerabilities in DNG, Reader, Acrobat
- Huawei denies involvement in buggy Linux kernel patch proposal
- Microsoft Patch Tuesday, May 2020 Edition
- An Undisclosed Critical Vulnerability Affect vBulletin Forums — Patch Now

#Tech and #Tools

- Using SharePoint as a Phishing Platform
- The Unattributable "db8151dd" Data Breach
- Security Flaws in Adobe Acrobat Reader Allow Malicious Program to Gain Root on macOS Silently
- Reg1c1de: Registry permission scanner for finding potential privesc avenues
- Introduction: Cloudgoat to Learn Cloud Security
- Web Security 101: An Interactive Cross-Site Request Forgery (CSRF) Demo
- Bypass Instagram SSL Certificate Pinning for iOS
- Attacking NFC and RFID
- Putting the “Fun” in “Hash Function”
- Stormspotter: Azure Red Team tool for graphing Azure and Azure Active Directory objects
- Open-sourcing new COVID-19 threat intelligence
- Breaking typical Windows hardening implementations
- Introducing C2concealer: a C2 Malleable Profile Generator for Cobalt Strike
- Powerob - An On-The-Fly Powershell Script Obfuscator Meant For Red Team Engagements

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us