kindred

Security Newsletter

30 July 2018

Subscribe to this newsletter

Google: Security Keys Neutralized Employee Phishing

Google has not had any of its 85,000+ employees successfully phished on their work-related accounts since early 2017, when it began requiring all employees to use physical Security Keys in place of passwords and one-time codes.

Security Keys are inexpensive USB devices that offer an alternative approach to two-factor authentication (2FA). The most common forms of 2FA require the user to supplement a password with a one-time code sent to their mobile device via text message or an app. In contrast, a Security Key implements a form of multi-factor authentication known as Universal 2nd Factor (U2F), which allows the user to complete the login process simply by inserting the USB device and pressing a button on the device. U2F is the only technology resisting to the most advanced Phishing techniques to date.

Google took its efforts to protect online accounts up a notch this week, announcing its own hardware-based security key, dubbed the Titan key. There will be two versions of Google's key: a USB one that plugs into your computer, and a Bluetooth one that must be paired with a device before use, aimed at users of mobile devices. They will both meet the Fast IDentity Online (FIDO) authentication standard, making them compatible with a range of other sites beyond Google's own.

Read More

Google takes on Yubico with its own security key, Titan

Google Advanced Protection Program

NetSpectre — New Remote Spectre Attack Steals Data Over the Network

Scientists have published a paper today detailing a new Spectre-class CPU attack that can be carried out via network connections and does not require the attacker to host code on a targeted machine.

This new attack —codenamed NetSpectre— is a major evolution for Spectre attacks, which until now have required the attacker to trick a victim into downloading and running malicious code on his machine, or at least accessing a website that runs malicious JavaScript in the user's browser. With NetSpectre, an attacker can simply bombard a computer's network ports and achieve the same results.

The biggest is the attack's woefully slow exfiltration speed, which is 15 bits/hour for attacks carried out via a network connection and targeting data stored in the CPU's cache. Both NetSpectre variations are too slow to be considered valuable for an attacker. This makes NetSpectre just a theoretical threat, and not something that users and companies should be planning for with immediate urgency.

Under the hood, this new NetSpectre attack is related to the Spectre v1 vulnerability (CVE-2017-5753) that Google researchers and academics have revealed at the start of the year. As such, all CPUs previously affected by Spectre v1 are believed to also be affected by NetSpectre, although academics said that existing vendor mitigations should stop NetSpectre, if they've been deployed with our OS and CPU's firmware.

TheHackerNews

ArsTechnica

Cutting room floor

- Under GDPR, Data Breach Reports in UK Have Quadrupled
- Hackers Hiding Web Shell Logins in Fake HTTP Error Pages
- US Government to Remove Adobe Flash Contents From Federal Agency Sites and Computers
- Half a Billion Enterprise Devices Exposed by DNS Rebinding
- LifeLock Bug Exposed Millions of Customer Email Addresses
- Researchers Detail New CPU Side-Channel Attack Named SpectreRSB
- Apache OpenWhisk Flaws Allowed Attackers to Overwrite Code in IBM Cloud
- Software Supply Chain Increasingly Targeted in Attacks: Survey
- The Bluetooth “device snooping bug” – what you need to know
- Apache Tomcat Patches Important Security Vulnerabilities
- Rapid7 penetration tests reveal multitude of software flaws, network misconfigurations
- How website filtering affects workplace productivity
- Exposed: 157 GB of sensitive data from Tesla, GM, Toyota & others
- “Simple trick” floors home security camera, gives anyone access
- 364 Idaho Inmates Hacked Their Prison Tablets for Free Credits

#Tech and #Tools

- Evilginx 2 - Next Generation of Phishing 2FA Tokens
- XSS on etherscan.io
- Attack inception: Compromised supply chain within a supply chain poses new risks
- Announcing GhostPack - C# implementations of previous PowerShell red team functionality
- The Road to QUIC
- Malicious.life podcast
- Shortcomings of blacklisting in Adobe Reader and what you can do about it
- Vulnerability Spotlight: Multiple Vulnerabilities in Samsung SmartThings Hub
- The Philosophy of ATT&CK
- Oracle Privilege Escalation via Deserialization
- Vulnerability in Hangouts Chat a.k.a. how Electron makes open redirect great again
- Into the Borg – SSRF inside Google production network

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 over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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 as an innovation driven company that builds on trust.

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