Security Newsletter

15 February 2021

Subscribe to this newsletter

10 SIM Swappers Arrested for Stealing $100M in Crypto from Celebrities

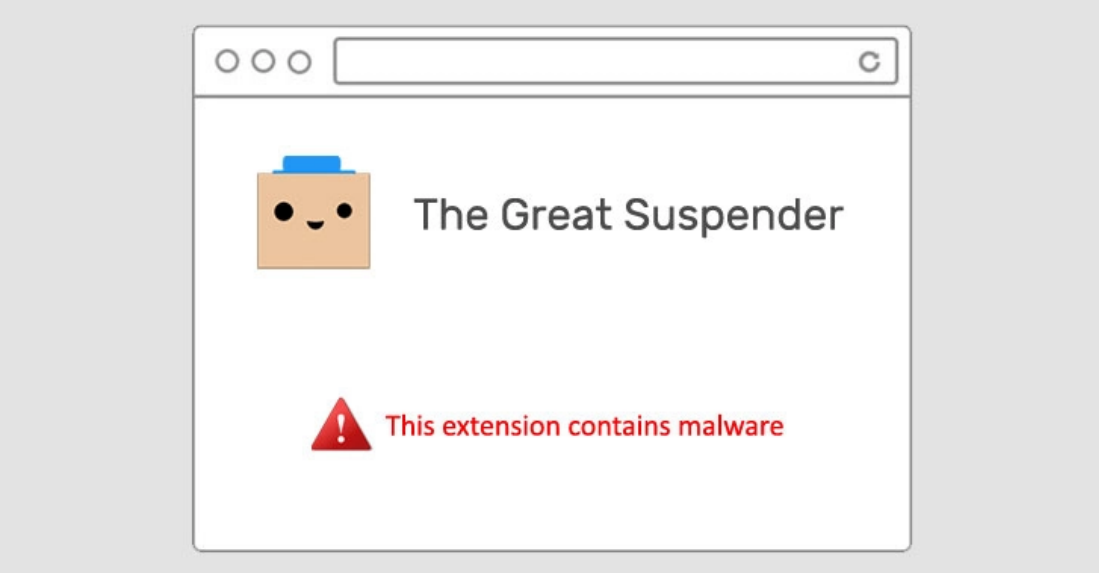
Ten people belonging to a criminal network have been arrested in connection with a series of SIM-swapping attacks that resulted in the theft of more than $100 million by hijacking the mobile phone accounts of high-profile individuals in the U.S.

Typically achieved with the help of a corrupt insider or using social engineering lures, SIM swapping refers to the technique adopted by cybercriminals to persuade phone carriers into porting their victims' cell services to a SIM card under their control. The SIM swap then grants attackers access to incoming phone calls, text messages, and one-time verification codes (or one-time passwords) that various websites send via SMS messages as part of the two-factor authentication (2FA) process.

Once in control of the target's mobile phone, the authorities noted that the criminals accessed personal information, including contacts synced with online accounts, and stole money, with cryptocurrency losses exceeding $100 million in 2020. "They also hijacked social media accounts to post content and send messages masquerading as the victim," the U.S. Secret Service said. To avoid SIM swapping attacks, it's recommended that users keep their device's software up to date, limit data-sharing online, and enable 2FA via apps instead of having an authentication code sent over SMS.

Read More on TheHackerNews

Hugely Popular 'The Great Suspender' Chrome Extension Contains Malware



Google on Thursday removed The Great Suspender, a popular Chrome extension used by millions of users, from its Chrome Web Store for containing malware. It also took the unusual step of deactivating it from users' computers. "This extension contains malware," read a terse notification from Google, but it has since emerged that the add-on stealthily added features that could be exploited to execute arbitrary code from a remote server, including tracking users online and committing advertising fraud.

The extension, which had more than two million installs before it was disabled, would suspend tabs that aren't in use, replacing them with a blank gray screen until they were reloaded upon returning to the tabs in question. According to The Register, Dean Oemcke, the extension's original developer, is said to have sold the extension in June 2020 to an unknown entity, following which two new versions were released directly to users via the Chrome Web Store (7.1.8 and 7.1.9).

Read More TheHackerNews

Researcher hacks over 35 tech firms in novel supply chain attack

A researcher managed to breach over 35 major companies' internal systems, including Microsoft, Apple, PayPal, Shopify, Netflix, Yelp, Tesla, and Uber, in a novel software supply chain attack. The attack comprised uploading malware to open source repositories including PyPI, npm, and RubyGems, which then got distributed downstream automatically into the company's internal applications.

Unlike traditional typosquatting attacks that rely on social engineering tactics or the victim misspelling a package name, this particular supply chain attack is more sophisticated as it needed no action by the victim, who automatically received the malicious packages. This is because the attack leveraged a unique design flaw of the open-source ecosystems called dependency confusion. For his ethical research efforts, the researcher has earned well over $130,000 in bug bounties.

Birsan noticed some of the manifest file packages were not present on the public npm repository but were instead PayPal's privately created npm packages, used and stored internally by the company. Birsan soon realized, should a dependency package used by an application exist in both a public open-source repository and your private build, the public package would get priority and be pulled instead -- without needing any action from the developer. In some cases, as with PyPI packages, the researcher noticed that the package with the higher version would be prioritized regardless of wherever it was located. Using this technique, Birsan executed a successful supply chain attack against Microsoft, Apple, PayPal, Shopify, Netflix, Tesla, Yelp, and Uber simply by publishing public packages using the same name as the company's internal ones.

Read More on BleepingComputer

More #News

- New research reveals who's targeted by email attacks

- Web hosting provider shuts down after cyberattack
- Hacker Tried Poisoning Water Supply After Breaking Into Florida's Treatment System
- Led by Hydra, Darknet Markets Logged Record Revenue
- SitePoint discloses data breach after stolen info used in attacks
- Proofpoint sues Facebook to get permission to use lookalike domains for phishing tests
- Ukrainian Police Arrest Author of World's Largest Phishing Service U-Admin
- Top 5 reasons not to use fear to encourage security compliance
- How much is your info worth on the Dark Web? For Americans, it's just $8
- Google Launches Database for Open Source Vulnerabilities
- Ransomware gangs made at least $350 million in 2020

#Breach Log

- CD Projekt Red gaming studio hit by ransomware attack
- Webdev tutorials site SitePoint discloses data breach
- Antivirus Firm Emsisoft Discloses Data Breach
- Experian: No Evidence of System Compromise in Brazil

#Patch Time!

- Microsoft Patch Tuesday, February 2021 Edition
- Adobe patches wave of critical bugs in Magento, Acrobat, Reader
- Intel fixes vulnerabilities in Windows, Linux graphics drivers
- WordPress plugin "Responsive Menu" exposes 100K sites to takeover attacks
- Siemens Patches 21 More File Parsing Vulnerabilities in PLM Products
- Critical Vulnerability Patched in SAP Commerce Product
- Apple Patches 10-Year-Old macOS SUDO Root Privilege Escalation Bug
- Plex patches media server bug potentially exploited by DDoS attackers
- Critical vulnerability in WordPress plugin "NextGen Gallery" with 800K installs
- Cyberpunk 2077 bug fixed that let malicious mods take over PCs
- Fortinet fixes critical vulnerabilities in SSL VPN and web firewall

#Tech and #Tools

- Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies
- Language Agnostic Security Code Review
- The 10 most common bugs of 2021 so far, and how to find them!
- How SecureBoot works
- MSSQL Link Crawl - OpenQuery Quotes Calculator
- Know, Prevent, Fix: A framework for shifting the discussion around vulnerabilities in open source
- cut1
- Getting started with Kubernetes audit logs and Falco
- The "P" in Telegram stands for Privacy

- A playbook for modernizing security operations
- How to use the Vault command line tool to store your code secrets
- Cloud Security Table Top Exercises

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