Security Newsletter

1 March 2021

Subscribe to this newsletter

SolarWinds Supply Chain Attacks: Blames Intern for 'solarwinds123' Password Lapse

As cybersecurity researchers continue to piece together the sprawling SolarWinds supply chain attack, top executives of the Texas-based software services firm blamed an intern for a critical password lapse that went unnoticed for several years. To date, at least nine government agencies and 100 private sector companies have been breached in what's being described as one of the most sophisticated and well-planned operations that involved injecting the malicious implant into the Orion Software Platform with the goal of compromising its customers.

The said password "solarwinds123" was originally believed to have been publicly accessible via a GitHub repository since June 17, 2018, before the misconfiguration was addressed on November 22, 2019. "I've got a stronger password than 'solarwinds123' to stop my kids from watching too much YouTube on their iPad," Representative Katie Porter of California said. "You and your company were supposed to be preventing the Russians from reading Defense Department emails."

In the weeks following the revelation, SolarWinds was hit with a class-action lawsuit in January 2021 that alleged the company failed to disclose that "since mid-2020, SolarWinds Orion monitoring products had a vulnerability that allowed hackers to compromise the server upon which the products ran," and that "SolarWinds' update server had an easily accessible password of 'solarwinds123'," as a result of which the company "would suffer significant reputational harm." While it's still not clear as to the extent the leaked password may have enabled the hack, a third-party spokesperson for the company claimed to the contrary. Likening the SolarWinds cyberattack to a "large-scale series of home invasions," Smith urged the need for strengthening the tech sector's software and hardware supply chains, and promoting broader sharing of threat intelligence for real-time responses during such incidents. SolarWinds, for its part, said it's implementing the knowledge gained from the incident to evolve into a company that is "Secure by Design" and that it's deploying additional threat protection and threat hunting software across all its network endpoints including measures to safeguard its development environments.

Read More on TheHackerNews

New 'Silver Sparrow' Malware Infected Nearly 30,000 Apple Macs

Days after the first malware targeting Apple M1 chips was discovered in the wild, researchers have disclosed yet another previously undetected piece of malicious software that was found in about 30,000 Macs running Intel x86_64 and the iPhone maker's M1 processors.

However, the ultimate goal of the operation remains something of a conundrum, what with the lack of a next-stage or final payload leaving researchers unsure of its distribution timeline and whether the threat is just under active development.

"Though we haven't observed Silver Sparrow delivering additional malicious payloads yet, its forward-looking M1 chip compatibility, global reach, relatively high infection rate, and operational maturity suggest Silver Sparrow is a reasonably serious threat, uniquely positioned to deliver a potentially impactful payload at a moment's notice," Lambert said.

Read More on TheHackerNews

Judge approves $650m settlement for Facebook users in privacy, biometrics lawsuit

A $650 million settlement to close a class-action lawsuit alleging that Facebook violated user privacy has been approved. The case, a class-action lawsuit filed against the social media giant six years ago, alleged that Facebook violated the Illinois Biometric Information Privacy Act (BIPA), which prevents companies from gathering or using biometric information from users without consent.

The lawsuit claimed that the Facebook Tag Suggestions feature, which used facial markers to suggest people in image tagging, violated BIPA by scanning, storing, and using user biometrics to create "face templates" without written permission. In total, close to 1.6 million Facebook users in Illinois could receive as much as $345 each within months, on the assumption that no appeal is filed, as reported by the Chicago Tribune.

In a statement, Facebook said, "we are pleased to have reached a settlement so we can move past this matter, which is in the best interest of our community and our shareholders." In related news over the past week, video content-sharing platform TikTok has agreed to a $92 million settlement to resolve claims that the company harvested and shared data belonging to minors.

Read More on ZDNet

More #News

- Microsoft Teams is getting end-to-end encryption support
- Xerox legal threat reportedly silences researcher at Infiltrate security conference
- Hackers abuse Google Apps Script to steal credit cards, bypass CSP
- Chrome will soon try HTTPS first when you type an incomplete URL
- Ransomware: Beware of 13 Tactics, Tools and Procedures
- Brussels Okays EU-UK Personal Data Flows
- New Hack Lets Attackers Bypass MasterCard PIN by Using Them As Visa Card
- Warning: Google Alerts abused to push fake Adobe Flash updater
- Fraudsters Using Telegram API to Harvest Credentials
- SolarWinds Hackers Stole Some Source Code for Microsoft Azure, Exchange, Intune
- Shadow Attacks Let Attackers Replace Content in Digitally Signed PDFs

- Checkout Skimmers Powered by Chip Cards
- Online Trackers Increasingly Switching to Invasive CNAME Cloaking Technique
- New 'unc0ver' Tool Can Jailbreak All iPhone Models Running iOS 11.0 - 14.3
- Working Windows and Linux Spectre exploits found on VirusTotal
- NSA Publishes Guidance on Adoption of Zero Trust Security
- Google's Password Checkup tool rolling out to Android devices
- Businessman charged with intent to steal General Electric's secret silicon technology

#Breach Log

- VC giant Sequoia Capital discloses data breach after failed BEC attack
- Ransomware gang hacks Ecuador's largest private bank, Ministry of Finance
- TD Bank suffered systemwide banking outage, services now recovered
- US cities disclose data breaches after vendor's ransomware attack
- Kroger data breach exposes pharmacy and employee data
- Malicious NPM packages target Amazon, Slack with new dependency attacks
- Oxfam Australia supporters embroiled in new data breach
- NASA and the FAA were also breached by the SolarWinds hackers
- European e-ticketing platform Ticketcounter extorted in data breach
- US Right-Wing Platform Gab Acknowledges it Was Hacked
- World's leading dairy group Lactalis hit by cyberattack
- Asian Food Distribution Giant JFC International Hit by Ransomware
- Universal Health Services lost $67 million due to Ryuk ransomware attack
- Minion privilege escalation exploit patched in SaltStack Salt project

#Patch Time!

- Keybase secure messaging fixes photo-leaking bug
- SonicWall releases additional update for SMA 100 vulnerability
- 6,000 VMware vCenter Devices Vulnerable to Remote Attacks
- Cisco Releases Security Patches for Critical Flaws Affecting its Products
- SHAREit fixes security bugs in app with 1 billion downloads
- IBM issues patches for Java Runtime, Planning Analytics Workspace, Kenexa LMS
- Critical VMware vCenter Server Flaw Can Expose Organizations to Remote Attacks
- "systeminformation" Node.js package has a code injection vulnerability
- Cisco fixes maximum severity MSO auth bypass vulnerability

#Tech and #Tools

- Defences against Cobalt Strike
- ECountering Cyber Proliferation: Zeroing in on Access-as-a-Service
- HAFNIUM targeting Exchange Servers with 0-day exploits
- ALchemist: Fusing Application and Audit Logs forPrecise Attack Provenance without Instrumentation
- Yarlx: Scalable YARA-based Malware Intelligence

- What I wish someone had told me when I started learning about File System Forensics
- How To Export LAPS Passwords from Active Directory with Powershell
- mubeng: An incredibly fast proxy checker & IP rotator with ease.
- Endgame: An AWS Pentesting tool
- teler: real-time intrusion detection and threat alert based on web log
- OWASP Top 10 for API explained interactively
- An Exploration of JSON Interoperability Vulnerabilities
- Server Side Request Forgery — Attack and Defense
- The little bug that couldn't: Securing OpenSSL
- Offensive Wifi Toolkit (owt)
- Anti-Debug and Anti-Memory Dump for Android
- Red Team Stories: The Gordian Lock
- Security Logging in Cloud Environments - AWS
- Crowdstrike 2021 Global Threat Report

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