Security Newsletter

18 January 2021

Subscribe to this newsletter

'SolarLeaks' Site Claims to Offer Attack Victims' Data

A new leaks site claims to be selling data from Cisco, FireEye, Microsoft and SolarWinds that was stolen via the SolarWinds supply chain attack. The appearance of the leaks website comes just four weeks after cybersecurity firm FireEye discovered and issued a public alert, warning that Texas-based SolarWinds' Orion network monitoring software had been backdoored as part of a sophisticated, monthslong campaign.

The new leaks website, solarleaks.net, contains a single text file, via which the operator claims to be selling four batches of stolen data from Cisco, FireEye, Microsoft and SolarWinds, with each victim's batch retailing for between $50,000 and $600,000. The site also offers to sell "all leaked data for $1 million," as well as to include an unnamed bonus. Would-be buyers are directed to email "solarleaks@protonmail.com" - an email address registered with ProtonMail, a free, encrypted email service. Emails sent to that address, however, bounced back as being undeliverable.

As of Wednesday, Mega had removed all four files from its service. But they're likely already circulating via BitTorrent sites for posterity. Additional information posted to the leaks site states that the site isn't including information from any additional victims, but will do so in the future. "We aren't fully done yet and we want to preserve the most of our current access," the site reads. "Consider this a first batch."

Read More on BankInfoSecurity

More #News

- Finding the Location of Telegram Users
- SolarWinds defense: How to stop similar attacks
- Facebook sues two Chrome extension devs for scraping user data
- How Conti Ransomware Works

- NSA advises companies to avoid third party DNS resolvers
- TikTok Harvested MAC Addresses By Exploiting Android Loophole
- Apple removes feature that allowed its apps to bypass macOS firewalls and VPNs
- Scam-as-a-Service operation made more than $6.5 million in 2020
- WhatsApp Stresses Privacy as Users Flock to Rivals
- Google reveals sophisticated Windows and Android hacking operation
- New Sunspot malware found while investigating SolarWinds hack

#Breach Log

- COVID-19 Vaccine Documents, Personal Data Leaked
- Ubiquiti tells customers to change passwords after security breach
- Mimecast Says Hackers Compromised Digital Certificate
- Capcom: 390,000 people may be affected by ransomware data breach
- Reserve Bank of New Zealand Investigates Data Breach
- How to review App Privacy data on your iPhone, iPad, or Mac

#Patch Time!

- It's finally over! Time to uninstall Adobe Flash Player
- Microsoft Patch Tuesday, January 2021 Edition
- Office January security updates fix remote code execution bugs
- Vulnerability Exposes F5 BIG-IP Systems to Remote DoS Attacks
- Cisco says it won't patch 74 security bugs in older RV routers that reached EOL
- Adobe fixes critical code execution vulnerabilities in 2021's first major patch round
- Microsoft Issues Patches for Defender Zero-Day and 82 Other Windows Flaws
- SAP Patches Serious Code Injection, DoS Vulnerabilities
- Chrome, Firefox updates fix severe security bugs
- Nvidia releases security update for high-severity graphics driver vulnerabilities

#Tech and #Tools

- Robust Indicators of Compromise for SUNBURST
- HackTricks - Free webbook of hacking tips and tricks
- Splunk - A Golden SAML Journey: SolarWinds Continued
- Best practices and advanced patterns for Lambda code signing
- Running my own DoH relay and getting Pi-hole protection away from home!
- Trickbot Still Alive and Well
- Project Zero: Introducing the In-the-Wild Series
- Everything (you need to know) about TTPs
- Research Paper: Understanding and Exploiting Zerologon
- Lil Pwny - Offline auditing of AD accounts' password using Python
- Microsoft Defender Attack Surface Reduction recommendations
- Universal Deserialisation Gadget for Ruby 2.x-3.x
- Leonardo S.p.A. Data Breach Analysis

- A Side Journey to Google Titan security key
- Abusing cloud services to fly under the radar

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