kindred

Security Newsletter

14 December 2020

Subscribe to this newsletter

US Agencies and FireEye Were Hacked Using SolarWinds Software Backdoor

State-sponsored actors allegedly working for Russia have targeted the US Treasury, the Commerce Department's National Telecommunications and Information Administration (NTIA), and other government agencies to monitor internal email traffic as part of a widespread cyberespionage campaign. The Washington Post, citing unnamed sources, said the latest attacks were the work of APT29 or Cozy Bear, the same hacking group that's believed to have orchestrated a breach of US-based cybersecurity firm FireEye a few days ago leading to the theft of its Red Team penetration testing tools.

The motive and the full scope of what intelligence was compromised remains unclear, but signs are that adversaries tampered with a software update released by Texas-based IT infrastructure provider SolarWinds earlier this year to infiltrate the systems of government agencies as well as FireEye and mount a highly-sophisticated supply chain attack. SolarWinds' networking and

security products are used by more than 300,000 customers worldwide, including Fortune 500 companies, government agencies, and education institutions.

The campaign, ultimately, appears to be a supply chain attack on a global scale, for FireEye said it detected this activity across several entities worldwide, spanning government, consulting, technology, telecom, and extractive firms in North America, Europe, Asia, and the Middle East. The hack was the biggest known theft of cybersecurity tools since those of the National Security Agency were purloined in 2016 by a still-unidentified group that calls itself the ShadowBrokers. That group dumped the N.S.A.'s hacking tools online over several months, handing nation-states and hackers the "keys to the digital kingdom," as one former N.S.A. operator put it. North Korea and Russia ultimately used the N.S.A.'s stolen weaponry in destructive attacks on government agencies, hospitals and the world's biggest conglomerates - at a cost of more than $10 billion.

In a security advisory published by SolarWinds, the company said the attack targets versions 2019.4 through 2020.2.1 of the SolarWinds Orion Platform software that was released between March and June 2020, while recommending users to upgrade to Orion Platform release 2020.2.1 HF 1 immediately.

Read More on TheHackerNews

Even more on 'Schneier On Security'

Microsoft: Important steps to protect themselves from recent nation-state cyberattacks

EU Vaccine Approval Agency Investigating Cyberattack

The European Medicines Agency, which helps evaluate and authorize medicines and vaccines - including those for COVID-19 - in the EU acknowledges it has been hit with a cyberattack. The EMA is a decentralized agency for the European Union responsible for evaluating, monitoring, and supervising new medicines introduced to the EU.

In a joint statement issued Thursday by pharmaceutical makers BioNTech and Pfizer, which are partnering on their COVID vaccine, the two companies said "some documents relating to the regulatory submission for Pfizer and BioNTech's COVID-19 vaccine candidate, BNT162b2, which has been stored on an EMA server, had been unlawfully accessed. ... No BioNTech or Pfizer systems have been breached in connection with this incident, and we are unaware that any study participants have been identified through the data being accessed."

Europol and Interpol last week issued notifications warning of a potential surge in organized crime activity tied to COVID-19 vaccines. In the U.S., the DHS' Cybersecurity and Infrastructure Security Agency last week also issued an advisory citing a new report by IBM warning organizations involved in COVID-19 vaccine production and distribution of a global phishing campaign targeting the cold storage and transport supply chain. In November, cold storage giant Americold was hit by a ransomware attack that forced them to shut down their systems and caused significant disruption in food delivery services.

Read More on BankInfoSecurity

Even More on BleepingComputer

More #News

- Massive Subway UK phishing attack is pushing TrickBot malware
- Watch Out! Adrozek Malware Hijacking Chrome, Firefox, Edge, Yandex Browsers
- France Fines Google, Amazon 135 Mn Euros
- Mastercard, Visa cut card payment ties with Pornhub over child abuse, illegal content allegations
- Critical CSRF vulnerability found on Glassdoor company review platform
- Pwnie Awards 2020 winners include Zerologon, CurveBall, Checkm8, BraveStarr attacks
- Hackers are selling more than 85,000 MySQL databases on a dark web portal
- Adobe to block Flash content from running on January 12, 2021
- Four sentenced to prison for planting malware on 20 million Gionee smartphones
- Payment Card Skimming Group Deployed Raccoon Infostealer
- Accounts with default creds found in 100+ GE medical device models
- Credit card stealing malware bundles backdoor for easy reinstall
- How DMARC Can Stop Criminals Sending Fake Emails on Behalf of Your Domain
- Teen who shook the Internet in 2016 pleads guilty to DDoS attacks
- Ex-Cisco engineer who nuked 16k WebEx accounts goes to prison

#Breach Log

- Spotify Informs Users of Personal Information Exposure
- Panasonic India's Data Released in Extortion Plot
- Vendor to Dental Practices Hacked; 1 Million Affected
- Foxconn electronics giant hit by ransomware, $34 million ransom
- HR Giant Randstad Hit by Egregor Ransomware

#Patch Time!

- Patch Tuesday, Good Riddance 2020 Edition
- Windows Kerberos Bronze Bit attack gets public exploit, patch now
- Cisco Patches Wormable, Zero-Click Vulnerability in Jabber
- 4 security bugs discovered in games on Valve's Steam platform
- DHS-CISA urges admins to patch OpenSSL DoS vulnerability
- 'AMNESIA:33' Vulnerabilities in TCP/IP Stacks Expose Millions of Devices to Attacks
- Adobe security update squashes critical vulnerabilities in Lightroom, Prelude
- WARNING — Critical Remote Hacking Flaws Affect D-Link VPN Routers
- All Kubernetes versions affected by unpatched MiTM vulnerability
- QNAP patches QTS vulnerabilities allowing NAS device takeover
- VMware Patches Workspace ONE Access Vulnerability Reported by NSA
- Vulnerability in NI Controller Can Allow Hackers to Remotely Disrupt Production
- Microsoft Office security updates fix critical SharePoint RCE bugs

#Tech and #Tools

- A survey of nearly 1,200 FOSS contributors found security to be low on developers' list of priorities.

- Tactics, Techniques and Procedures (TTPs) Utilized by FireEye's Red Team Tools
- Google open-sources Atheris, a tool for finding security bugs in Python code
- OpenSSF Launches Open Source Tool for Evaluating SAST Products
- Improving DNS Privacy with Oblivious DoH in 1.1.1.1
- Good-bye ESNI, hello ECH!
- Abusing AirWatch MDM Services to Bypass MFA
- Whitelisting Processes on Kubernetes Pods Using AppArmor (Part 1)
- Rizin: Open Source Reverse Engineering Framework
- It is Time to Take Action - How to Defend Against FireEye's Red Team Tools
- Depi: recovering passwords from pixelized screenshots.
- Fibratus: exploration and tracing of the Windows kernel.

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