Security Newsletter

11 January 2021

Subscribe to this newsletter

SolarWinds: The more we learn, the worse it looks

In March of 2020, Americans began to realize that the coronavirus was deadly and going to be a real problem. What no Americans knew then was that at about the same time, the Russian government's hack of SolarWinds's proprietary software Orion network monitoring program was destroying the security of top American government agencies and tech companies. There were no explosions, no deaths, but it was the Pearl Harbor of American IT.

Russia, we now know, used SolarWinds' hacked program to infiltrate at least 18,000 government and private networks. The data within these networks, user IDs, passwords, financial records, source code, you name it, can be presumed now to be in the hands of Russian intelligence agents.

The Russians may even have the crown-jewels of Microsoft software stack: Windows and Office. In a twist, which would be hilarious if it weren't so serious, Microsoft claims it's no big deal. As time goes by more and more government agencies and companies have been shown to have been hacked. This includes the Department of State; Department of Homeland Security; National Institutes of Health; the Pentagon; Department of the Treasury; Department of Commerce; and the Department of Energy, including the National Nuclear Security Administration. How much bigger will it get? We don't know. Personally, I'd assume that if my company had been using SolarWinds Orion software during 2020, I've been hacked

Read More on ZDNet

Ticketmaster To Pay $10 Million Fine For Hacking A Rival Company

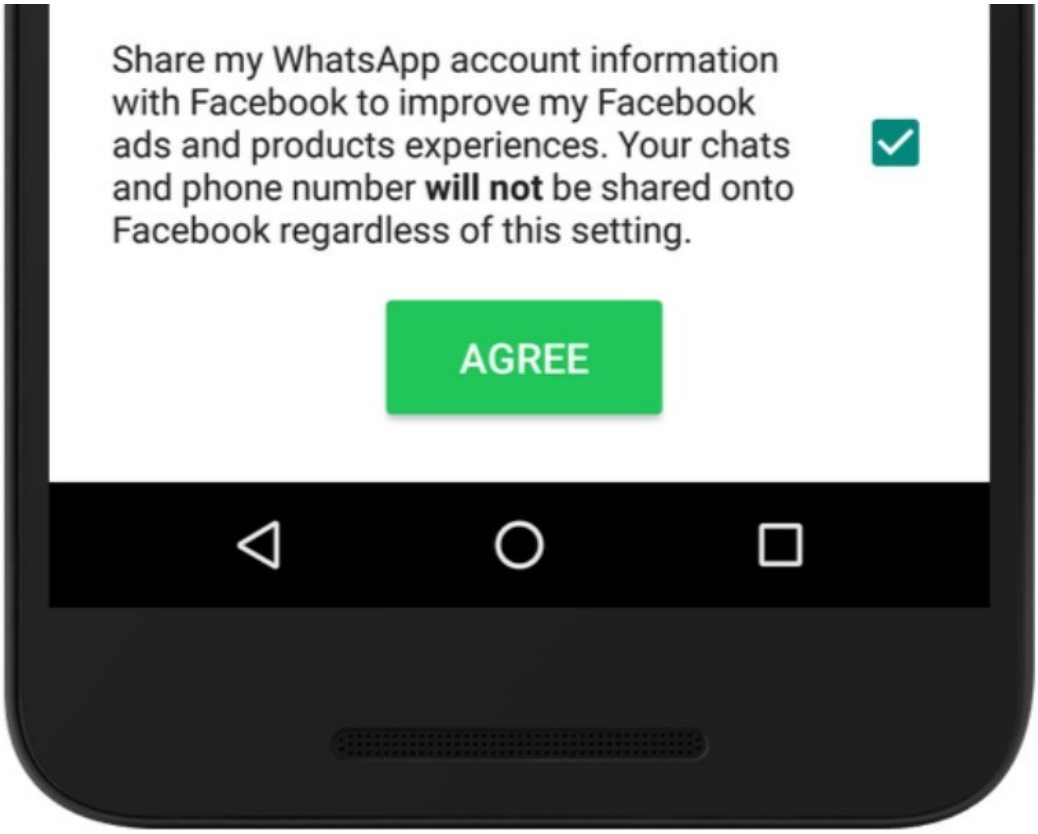
Ticketmaster has agreed to pay a $10 million fine after being charged with illegally accessing computer systems of a competitor repeatedly between 2013 and 2015 in an attempt to "cut [the company] off at the knees." A subsidiary of Live Nation, the California-based ticket sales and distribution company used the stolen information to gain an advantage over CrowdSurge — which merged with Songkick in 2015 and later acquired by Warner Music Group (WMG) in 2017 — by hiring a former employee to break into its tools and gain insight into the firm's operations.

The allegations were first reported in 2017 after CrowdSurge sued Live Nation for antitrust violations, accusing Ticketmaster of accessing confidential business plans, contracts, client lists, and credentials of CrowdSurge tools. According to court documents released on December 30, after being hired by Live Nation in 2013, Stephen Mead, who was CrowdSurge's general manager of U.S. operations, shared with Zeeshan Zaidi, the former head of Ticketmaster's artist services division, and another Ticketmaster employee the passwords to Artist Toolbox, an app that provided real-time data about tickets sold through the victim company. Besides password theft, Mead is also accused of providing "internal and confidential financial documents" retained from his former employer, as well as URLs for draft ticketing web pages so as to learn which artists planned to use CrowdSurge to sell tickets and "dissuade" them from doing so.

Ticketmaster previously settled a lawsuit brought by Songkick in 2018 by agreeing to pay the company's owners $110 million and acquire its remaining intellectual property not sold to WMG for an undisclosed amount. Besides paying the $10 million penalties, Ticketmaster is expected to maintain a compliance and ethics program to detect and prevent such unauthorized acquisition of confidential information belonging to its rivals.The company will also be required to make an annual report to the U.S. Attorney's Office over the next three years to ensure compliance.

Read More on TheHackerNews

WhatsApp updates privacy policy to enable sharing more data with Facebook



In a major update to its Privacy Policy and Terms of Service, WhatsApp is notifying users in many parts of the world that as of February 8 it will share some of their data with Facebook, the chat app's parent company. Importantly, users who won't agree to the new terms will need to stop using the app or delete their accounts.

Note, however, that users in Europe will be exempt from the service's new data-sharing practices and are only shown the first two of the three points in the notice. WhatsApp's director of policy for Europe, the Middle East and Africa (EMEA). How about the rest of the world, though? Here's an important part of the platform's updated ToS as it will apply to those users: "As part of the Facebook Companies, WhatsApp receives information from, and shares information with, the Facebook Companies as described in WhatsApp's Privacy Policy, including to provide integrations which enable you to connect your WhatsApp experience with other Facebook Company Products; to ensure security, safety, and integrity across the Facebook Company Products; and to improve your ads and products experience across the Facebook Company Products,"

At this point it is important to remember some of the key information that WhatsApp collects:

- Your phone number that you used to create an account
- Your profile picture and profile information
- The phone numbers of your WhatsApp contacts
- Transaction and payments data
- Location information
- Information about your device such as the model, operating system, and mobile network
- Other information, including your IP address, device operations information, and identifiers

By agreeing with new terms and policy you will be effectively agreeing to Facebook and its subsidiaries having access to at least some of your data.

Read More on WeLiveSecurity

Even More on BBC news

More #News

- Rioters Open Capitol's Doors to Potential Cyberthreats
- Chrome browser has a New Year's resolution: HTTPS by default
- Healthcare Industry Witnessed 45% Spike in Cyber Attacks Since Nov 20
- The dynamic duo: How to build a red and blue team to strengthen your cybersecurity, Part 1
- Indian government sites leaking patient COVID-19 test results
- $2.4 Million Settlement in 2017 Sabre Data Breach
- Whirlpool Hit With Ransomware Attack
- New AutoHotkey-Based Malware Targets US, Canadian Banks
- https://www.bleepingcomputer.com/news/security/multi-platform-card-skimmer-found-on-shopify-bigcommerce-stores/
- US Treasury warns of ransomware targeting COVID-19 vaccine research
- A Google Docs Bug Could Have Allowed Hackers See Your Private Documents
- EU Launches Decryption Tool for Law Enforcement
- Trucking giant Forward Air hit by new Hades ransomware gang
- New side-channel attack can recover encryption keys from Google Titan security keys
- Scammer extorts site owners using porn backlinks threat

#SolarWinds saga

- JetBrains denies being involved in SolarWinds hack
- SolarWinds hackers had access to over 3,000 US DOJ email accounts
- FBI, CISA, NSA Officially Blame Russia for SolarWinds Cyber Attack
- Severe SolarWinds Hacking: 250 Organizations Affected?
- SolarWinds hackers accessed Microsoft source code

#Breach Log

- Vodafone's ho. Mobile admits data breach, 2.5m users impacted
- Stolen employee credentials put leading gaming firms at risk
- T-Mobile discloses its fourth data breach in three years
- Kawasaki: Cyber Incident May Have Resulted in Data Loss
- VMware latest to confirm breach in SolarWinds hacking campaign
- New SUPERNOVA backdoor found in SolarWinds cyberattack analysis
- Shareholder Sues SolarWinds for Alleged Security Failures

#Patch Time!

- Google Discloses Poorly-Patched, Now Unpatched, Windows 0-Day Bug
- Vulnerabilities in Fortinet WAF Can Expose Corporate Networks to Attacks
- Zyxel hardcoded admin password found – patch now!
- Zend Framework disputes RCE vulnerability, issues patch
- Critical Flaws Put Dell Wyse Thin Client Devices at Risk
- Nissan NA source code leaked due to default admin:admin credentials

#Tech and #Tools

- Threat Intel tool Intel Owl v2.0.0 release
- Steam's login method is kinda interesting
- Machine Learning security course
- Lesser Known Techniques for Attacking AWS Environments
- Hacking with Haskell
- Hardening Docker with CIS
- Harden Docker with CIS – Part 1; 2; 3; 4; 5
- Gossamer: Supply Chain Security for the PHP Ecosystem
- The Mac Malware of 2020: A comprehensive analysis of the year's new malware
- State of Pentesting 2020
- Exploring Nmap #1
- Pentest - Everything SMTP
- Shifting Cloud Security Left — Scanning Infrastructure as Code for Security Issues
- Adversary Infrastructure Report 2020: A Defender's View
- Defences against Cobalt Strike
- Awesome CobaltStrike resource list
- Watcher - Open Source Cybersecurity Threat Hunting Platform

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