kindred

Security Newsletter

6 Sep 2021

Subscribe to this newsletter

SolarWinds and the Holiday Bear Campaign: A Case Study for the Classroom

Southwest Parkway is a wide and winding road that leads away from Austin towards the Texas Hill Country. Along its length are neighborhoods, schools, and long stretches of open landscape. It is not where one might expect to find the epicenter of a major cybersecurity episode. But Southwest Parkways also is where one can find the unassuming headquarters of SolarWinds, a name that burst into the headlines in December 2020.

SolarWinds specializes in network-management tools—that is, software that large enterprises use to monitor and control conditions throughout their information technology environment. Its products are in widespread use around the world, including a wide array of prominent private sector entities and government agencies.

What follows is a detailed account of the complex sequence of operations SVR conducted as part of the Holiday Bear campaign. As we shall see, exploiting SolarWinds was a central part of the campaign, but there is far more to the story than that

Read More on Lawfare blog

Gift Card Gang Extracts Cash From 100k Inboxes Daily

Some of the most successful and lucrative online scams employ a “low-and-slow” approach — avoiding detection or interference from researchers and law enforcement agencies by stealing small bits of cash from many people over an extended period.

Here’s the story of a cybercrime group that compromises up to 100,000 email inboxes per day, and apparently does little else with this access except siphon gift card and customer loyalty program data that can be resold online.

The data in this story come from a trusted source in the security industry who has visibility into a network of hacked machines that fraudsters in just about every corner of the Internet are using to anonymize their malicious Web traffic. For the past three years, the source — we’ll call him “Bill” to preserve his requested anonymity — has been watching one group of threat actors that is mass-testing millions of usernames and passwords against the world’s major email providers each day.

Read More on Krebs on Security

More #News

- Proofpoint lawsuits underscore risk of employee offboarding
- Apple Delays Plans to Scan Devices for Child Abuse Images After Privacy Backlash
- U.S. Cyber Command Warns of Ongoing Attacks Exploiting Atlassian Confluence Flaw

- WhatsApp Photo Filter Bug Could Have Exposed Your Data to Remote Attackers
- New BrakTooth Flaws Leave Millions of Bluetooth-enabled Devices Vulnerable
- CISA Adds Single-Factor Authentication to the List of Bad Practices
- Attackers Can Remotely Disable Fortress Wi-Fi Home Security Alarms
- China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying
- Google's TensorFlow drops YAML support due to code execution flaw
- FBI: Spike in sextortion attacks cost victims $8 million this year
- WhatsApp to appeal $266 million fine for violating EU privacy laws
- FTC bans stalkerware maker Spyfone from surveillance business
- Cybercriminal sells tool to hide malware in AMD, NVIDIA GPUs
- Germany reportedly pushing EU to require 7 years of updates on Android, iOS devices

#Breach Log

- Autodesk reveals it was targeted by Russian SolarWinds hackers
- Fired NY credit union employee nukes 21GB of data in revenge
- LockBit gang leaks Bangkok Airways data, hits Accenture customers
- DuPage Medical Group hit with data breach that may affect 600,000 patients

#Patch Time!

- NPM package with 3 million weekly downloads had a severe vulnerability
- Cisco Issues Patch for Critical Enterprise NFVIS Flaw
- QNAP Working on Patches for OpenSSL Flaws Affecting its NAS Devices
- Atlassian Confluence remote code execution vulnerability actively exploited
- Patched Vulnerability in WhatsApp could have led to data exposure of users

#Tech and #Tools

- Analysis of the Human-Operated Ransomware Targeting Healthcare
- The ABCs of NFC chip security
- Protecting SSH keys with TPM 2.0
- A deep-dive into the SolarWinds Serv-U SSH vulnerability
- Patched Vulnerability in WhatsApp could have led to data exposure of users
- CVE-2021-26084 Remote Code Execution on Confluence Servers
- From RpcView to PetitPotam
- A review of the implementation of electronic driver's licenses in Iceland

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us