kindred

Security Newsletter

13 Sep 2021

Subscribe to this newsletter

Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role

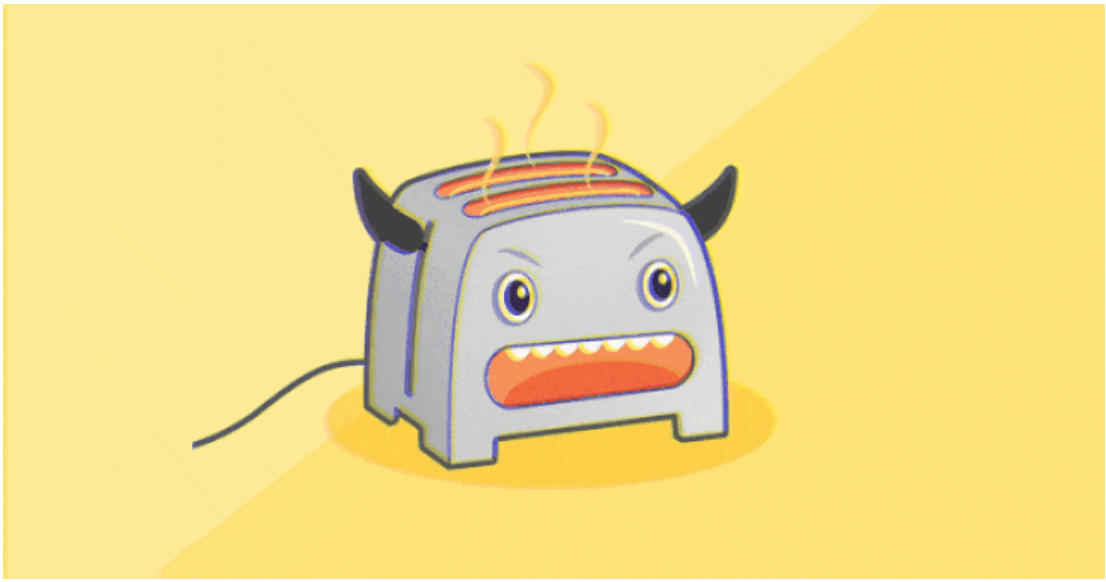
Days before Christmas in 2015, Juniper Networks Inc. alerted users that it had been breached. In a brief statement, the company said it had discovered “unauthorized code” in one of its network security products, allowing hackers to decipher encrypted communications and gain high-level access to customers’ computer systems.

More than five years later, the breach of Juniper’s network remains an enduring mystery in computer security, an attack on America’s software supply chain that potentially exposed highly sensitive customers including telecommunications companies and U.S. military agencies to years of spying before the company issued a patch.

Those intruders haven’t yet been publicly identified, and if there were any victims other than Juniper, they haven’t surfaced to date. But one crucial detail about the incident has long been known — uncovered by independent researchers days after Juniper’s alert in 2015 — and continues to raise questions about the methods U.S. intelligence agencies use to monitor foreign adversaries.

Read More on Bloomberg

Fighting the Rogue Toaster Army: Why Secure Coding in Embedded Systems is Our Defensive Edge



There are plenty of pop culture references to rogue AI and robots, and appliances turning on their human masters. It is the stuff of science fiction, fun, and fantasy, but with IoT and connected devices becoming more prevalent in our homes, we need more discussion around cybersecurity and safety.

Software is all around us, and it's very easy to forget just how much we're relying on lines of code to do all those clever things that provide us so much innovation and convenience. Much like web-based software, APIs, and mobile devices, vulnerable code in embedded systems can be exploited if it is uncovered by an attacker.

While it's unlikely that an army of toasters is coming to enslave the human race (although, the Tesla bot is a bit concerning) as the result of a cyberattack, malicious cyber events are still possible. Some of our cars, planes, and medical devices also rely on intricate embedded systems code to perform key tasks, and the prospect of these objects being compromised is potentially life-threatening.

Read More on The Hacker News

More #News

- Ransomware gangs target companies using these criteria
- REvil ransomware's servers mysteriously come back online
- Ukrainian extradited for selling 2,000 stolen logins per week
- Yandex is battling the largest DDoS in Russian Internet history
- Windows MSHTML zero-day exploits shared on hacking forums
- WhatsApp to Finally Let Users Encrypt Their Chat Backups in the Cloud
- New SpookJS Attack Bypasses Google Chrome's Site Isolation Protection
- SOVA: New Android Banking Trojan Emerges With Growing Capabilities
- You Don't Need to Burn off Your Fingertips (and Other Biometric Authentication Myths)

#Breach Log

- McDonald's leaks password for Monopoly VIP database to winners
- Jenkins project's Confluence server hacked to mine Monero
- Howard University shuts down network after ransomware attack
- Hackers leak passwords for 500,000 Fortinet VPN accounts
- MyRepublic discloses data breach exposing government ID cards
- BlackMatter ransomware hits medical technology giant Olympus

#Patch Time!

- Netgear fixes severe security bugs in over a dozen smart switches
- Zoho patches actively exploited critical ADSelfService Plus bug

#Tech and #Tools

- GitHub finds 7 code execution vulnerabilities in 'tar' and npm CLI
- Microsoft MSHTML Remote Code Execution Vulnerability
- CertPortal: Building Self-Service Secure S/MIME Provisioning Portal
- IAM Vulnerable - An AWS IAM Privilege Escalation Playground
- CVE-2021-40444 PoC
- Finding Azurescape – Cross-Account Container Takeover in Azure Container Instances
- Mēris botnet, climbing to the record

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