kindred

Security Newsletter

28 Mar 2022

Subscribe to this newsletter

Authentication Giant Okta Breached Through Customer Support

Cybersecurity giant Okta, which provides authentication services for private and government clients and handles how hundreds of millions of users are able to securely log into their employer's networks, itself was targeted by an extortion-focused hacking group.

In a statement, Okta said the breach was brief and took place in January. But the method the hackers used to gain access still highlights a weakness in giant companies: the hackers targeted a third-party customer support worker.

"In late January 2022, Okta detected an attempt to compromise the account of a third party customer support engineer working for one of our subprocessors," Okta told Motherboard in a statement. "The matter was investigated and contained by the subprocessor."

Read More on Vice

LAPSUS$: How a Sloppy Extortion Gang Became One of the Most Prolific Hacking Groups

The U.S. government has said it is paying close attention to LAPSUS$, the group that breached Okta, Microsoft, and Nvidia. The answers for the group's motivations are hiding in plain sight.

The group has confounded and captivated some in the cybersecurity industry, with some even speculating that LAPSUS$ may be a front for a government-backed hacking group. But a review of LAPSUS$'s public statements, their breaches, technical analysis by security experts, and indications of who a main member might be, paints a picture of a crew that bears much more resemblance to the sort of free-wheeling gangs that have become a staple in the world of SIM-swapping and other relatively low level hacking techniques. Only this time, people are paying much more attention, in part because of the sorts of targets that LAPSUS$ managed to compromise. On Thursday shortly after the publication of this story, British police said they had arrested seven teenagers suspected of being part of the gang.

Read More on Vice

More #News

- A Closer Look at the LAPSUS$ Data Extortion Group
- Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison
- Spyware dubbed Facestealer infects 100,000+ Google Play users
- Okta: "We made a mistake" delaying the Lapsus$ hack disclosure
- Lapsus$ suspects arrested for Microsoft, Nvidia, Okta hacks
- South Africa wants to fight SIM swapping with biometric checks
- GitHub explains the cause behind the past week's outages
- New Mustang Panda hacking campaign targets diplomats, ISPs
- Hackers exploit new WPS Office flaw to breach betting firms
- The top 5 things the 2022 Weak Password Report means for IT security
- Crypto malware in patched wallets targeting Android and iOS devices
- US, EU reach preliminary data privacy agreement

#Breach Log

- Social Engineering Attacks Resulted in Compromise of Morgan Stanley Client Accounts
- Greece's public postal service offline due to ransomware attack
- Top Russian meat producer hit with Windows BitLocker encryption attack

#Patch Time!

- Western Digital fixes critical bug giving root on My Cloud NAS devices
- Emergency Google Chrome update fixes zero-day used in attacks
- Western Digital My Cloud OS update fixes critical vulnerability

#Tech and #Tools

- Chinese Threat Actor Scarab Targeting Ukraine
- Remote Code Execution on Western Digital PR4100 NAS (CVE-2022-23121)
- Mining data from Cobalt Strike beacons
- Reports from the Field: Part 3
- Crypto malware in patched wallets targeting Android and iOS devices
- Racing against the clock -- hitting a tiny kernel race window

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 more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 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