www.cpomagazine.com /cyber-security/lapsus-hackers-breached-t-mobile-repeatedly-and-download…

Lapsus$ Hackers Breached T-Mobile Repeatedly and Downloaded Thousands of Source Code Repositories, Leaked Chats Show - CPO Magazine

Cyber SecurityNews·4 min read ⋮ 6-8 minutes ⋮ 4/28/2022

Leaked chats between Lapsus$ hackers revealed that the gang breached T-Mobile multiple times in March and copied thousands of source code repositories.

The chats originated from the hacking group's private Telegram channel.

Unlike their public Telegram channel with over 40,000 followers, the private group is exclusive to seven core members.

A career cybercriminal and DoxBin doxxing website owner "KT" leaked the chats to KrebsOnSecurity's researcher Brian Krebs.

The chats exposed the group plotting another heist before authorities detained seven suspected Lapsus$ members aged 15-21 years, and two unnamed suspects, 16 and 17 years old, face multiple charges related to unauthorized access.

Lapsus$ extortion group operates by stealing and threatening to publish it, usually without encrypting the victim's devices.

Lapsus$ hackers frequently bought access credentials from Russian underground markets

Krebs says that Lapsus$ hackers bought stolen credentials from the Russian Market that regularly stocked these details.

Whenever T-Mobile employees would inadvertently disrupt Lapsus$ hackers by changing passwords, the threat actors would procure another set of credentials from Russian underground markets.

"You typically can't completely prevent adversaries from getting into your network – especially if they purchase stolen credentials from Russian cybercrime forums, as the Lapsus$ gang does – so the best strategy is to deploy monitoring with the right detection rules in your SOC so you can quickly contain attacks before they have a major business impact," says Phil Neray, Vice President of Cyber Defense Strategy at CardinalOps.

Lapsus$ hackers also stole credentials by luring employees into disclosing these details and authorizing or enrolling devices onto the company's virtual private network.

"When it comes to internal breaches where networks are compromised, identity is still the number one challenge," Gal Helemski, CTO and co-founder of PlainID, said. "Organizations must adopt a 'Zero Trust' approach, which means trusting no one – not even known users or devices – until they have been verified and validated."

According to the leaked chats, Lapsus$ hackers gained access to internal tools, including T-Mobile's Atlas customer accounts management systems. This access allowed the hackers to perform SIM swaps and take ownership of the victims' cell phone numbers for fraud and two-factor authentication.

Lapsus$ hackers intended to SIM swap wealthy clients for money. Additionally, one gang member identified as White targeted the FBI and the Department of Defense.

However, the government accounts required additional authorizations, and other members advised him against it to preserve their access.

Lapsus$ hackers compromised T-Mobile's Slack and BitBucket and downloaded source code repos

Lapsus$ hacker White informed others that he had successfully breached T-Mobile's Slack and Bitbucket. Additionally, he allegedly discovered how to upload scripts to the company's virtual machine. Within 12 hours, White reported downloading 30,000 source code repositories from T-Mobile.

However, T-Mobile downplayed the incident claiming that Lapsus$ hackers did not gain access to "anything of value."

"Several weeks ago, our monitoring tools detected a bad actor using stolen credentials to access internal systems that house operational tools software," T-Mobile said.

According to the company, "the system accessed contained no customer or government information or other similarly sensitive information."

T-Mobile added that its response team quickly contained the intrusion and kicked out the unauthorized parties from the system.

"Our systems and processes worked as designed, the intrusion was rapidly shut down and closed off, and the compromised credentials used were rendered obsolete."

"T-Mobile's confirmation that the Lapsus$ extortion gang breached its network shows how much more damaging and complex cyberattacks have become as extortion attempts rise in popularity," Arti Raman, CEO & Founder at Titaniam, said. "This highlights the importance of technologies like encryption-in-use (also known as data-in-use encryption) which specifically protect against data extortion."

Krebs noted that Lapsus$ hackers tried to steal and delete any source code it accessed on compromised systems. He suggested that the source code assisted the group in discovering more vulnerabilities, or there was high demand for leaked source code in the underground markets.

“Knowing how vulnerable you are to ransomware attacks, as well as reviewing your security posture through continuous vulnerability management and proactive penetration testing, is crucial to establishing better defenses as hacker organizations such as Lapsus$ continue to rise. “- Aaron Sandeen, CEO and co-founder, Cyber Security Works.

Within four years, Lapsus$ has carried at least ten data breaches, stealing source code from Nvidia (1 terabyte), Samsung (200 GB including internal data), Globant (70 GB), and Microsoft (37 GB). Other Lapsus$ victims include Vodafone, Impresa, Okta, Ubisoft, and Brazil’s Ministry of Health.

“Recent attacks and extortion attempts on large enterprises are clear examples of the damage that can be done when compromised credentials are used to carry out account takeover (ATO) attacks,” said Gunnar Peterson, CISO at Forter. “The Lapsus$ ransomware group is conducting all of their ATO activity using stolen usernames and passwords that were obtained using unconventional and sophisticated means.”

Peterson advised organizations to invest in building learning systems that evolve and keep up with attackers’ tactics.

Leaked chats show Lapsus$ #hackers had access to T-Mobile's internal systems capable of SIM swapping and downloaded thousands of source code repositories. #databreach #cybersecurity #respectdata

“Because Lapsus$ is clearly capable of breaking through perimeter security measures, companies must focus on detection and response to minimize the damage of the infiltration. It’s important to invest in solutions that establish a baseline of user and entity behavior and are capable of flagging potentially malicious or suspicious activity as soon as it occurs,” said Tyler Farrar, CISO at Exabeam.