LAPSUS$

THE LATEST THREAT TO YOUR DIGITAL SUPPLY CHAIN

Modern threat groups are well-oiled machines that function like real-world businesses.

Lapsus$ doesn't follow this model — arguably, this makes them even more dangerous.

Who is Lapsus$?

- Emerged in late 2021
- First appeared in S. America
- Prioritizes notoriety and publicity
- Operates a public Telegram channel
- Caused several high profile breaches
- Frequently recruits insiders for hacks

WHO HAS LAPSUS$ TARGETED SO FAR?

Ministry of Health (Brazil)
Dumped 50 TB of data

Confina/Impresa
Offline for over a month

Microsoft
Stole Bing & Cortana source code

Localiza
Redirected users to a porn site

Claro
Dumped over 10K TB of data

Vodafone Portugal
Disrupted 4G/5G Network, SMS, TV services

NVIDIA
Leaked credentials & source code incl. signing certs.

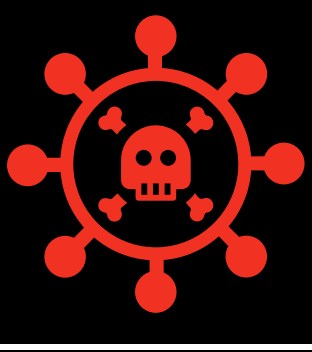
Samsung
Stole over 190gb of internal source code

Okta
Reset credentials for ~375 business clients

HOISTED BY THEIR OWN PETARD

Microsoft used Lapsus$'s Telegram channel to cut off an attack, then publicly disclosed the group's TTPs:

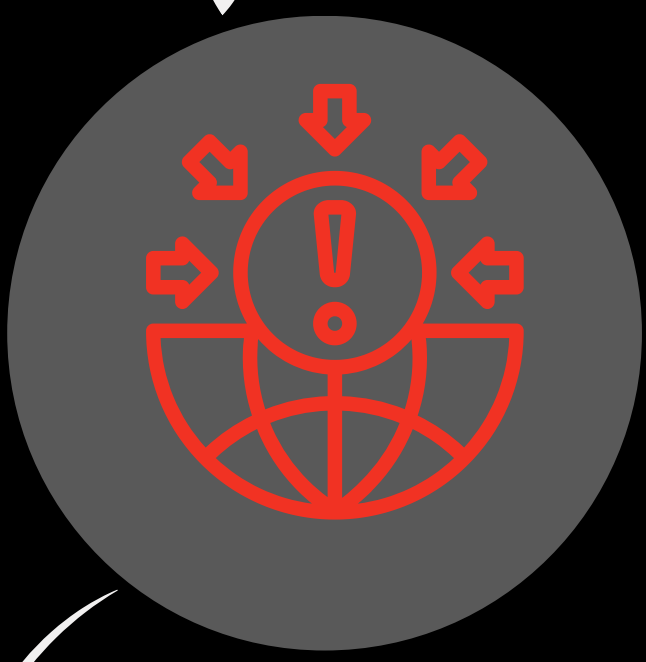
- Phishing
- Purchased/stolen credentials
- Public code repositories
- Bribing insiders
- Targeting personal accounts
- SIM-swapping



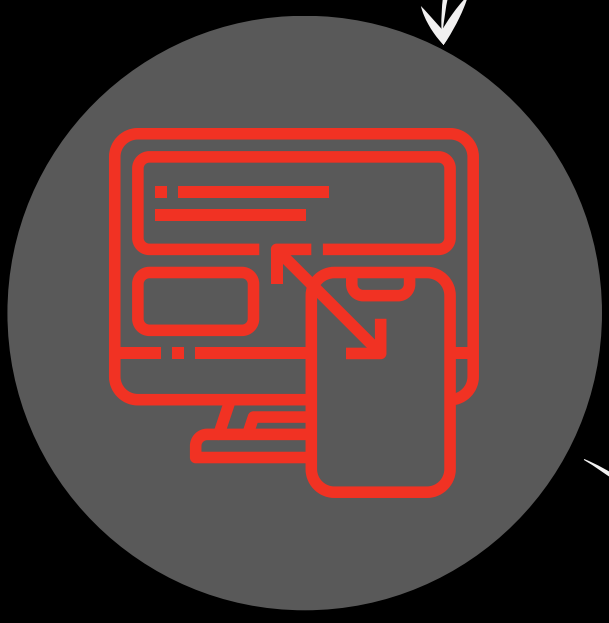
Protecting Yourself Against Lapsus$

<u>Basic Best Practices</u>

- Authentication
- Auditing
- Authorization
- Patching
- Secure access points



Use IOCs for active threat hunting across your entire supply chain



Improve your hiring process, security awareness training, and incident response

Leverage DLP and User and Entity Behavior Analysis (UEBA)