Attack Signal Intelligence vs. Lapsus$ Cybercrime Group

Notorious cybercrime group bypasses prevention security to target cloud environments, making AI-driven prioritization is key to successful defense.

Incident background:

- Lapsus$ cybercrime group
- Attacks targeting tech enterprises
- Exploiting prevention tool weakness
- Lateral movement throughout cloud

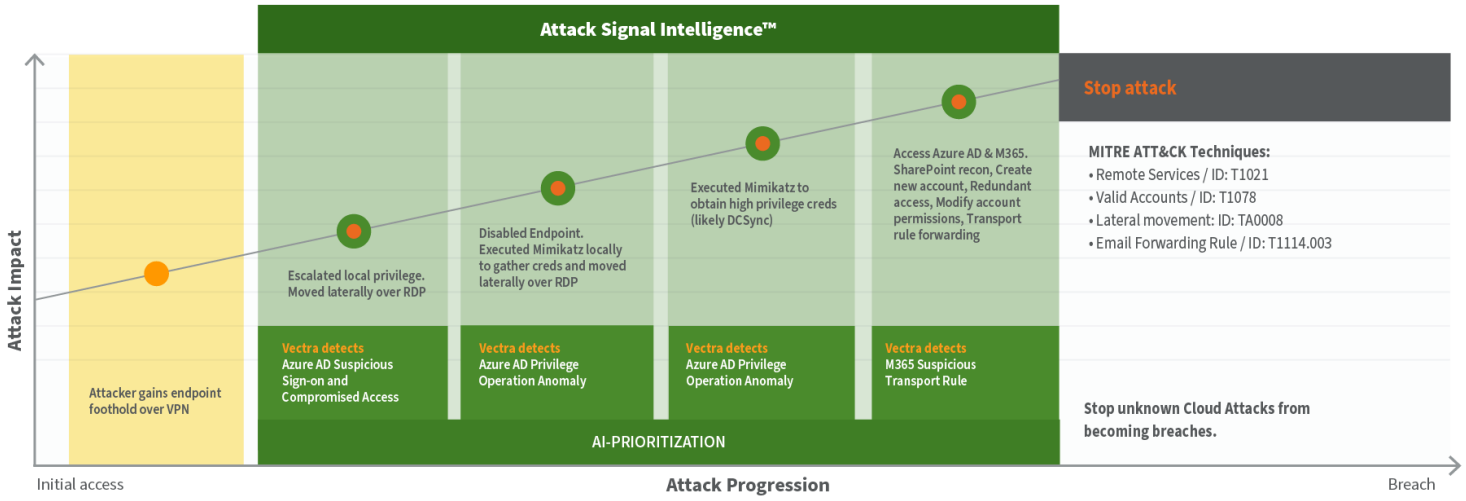
Cloud Attack

Simulated Incident: Attack Signal Intelligence™ vs Lapsus$

Industry: Tech Enterprises

Targets:
Exploiting prevention tool weaknesses
Lateral movement throughout cloud

Response time	First Vectra alert	Attack stopped
	00:00	**00:20**



Attack implications:

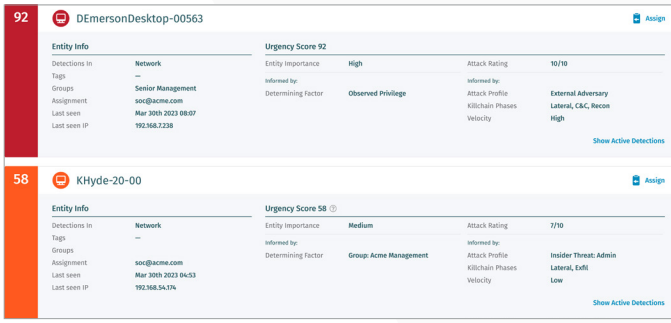
- Mass exfiltration
- Ransomware
- Reputation damage
- Business disruption

Lapsus$ has shown the ability to exploit weaknesses in prevention security (including MFA) to gain access to enterprise environments. This simulated example highlights their ability to use compromised credentials to access and progress across a cloud environment.

- VPN access bypasses EDR
- Credentials compromised
- Azure AD sign-in with stolen credentials
- Use remote desktop to move laterally

Prioritizing Tactics

Once attackers gain access, it's critical that any tactics they use to advance are prioritized. Here, the attackers moved laterally by using a remote desktop and were able to disable an endpoint and gather credentials to progress — ultimately gaining access to Azure AD and M365.



Attack Signal Intelligence™ prioritizes:

- AD Suspicious Sign-on and Compromised Access
- Azure AD Privilege Operation Anomaly
- Azure AD Privilege Operation Anomaly
- M365 Suspicious Transport Rule

Lapsus$ shows no shortage of techniques

Lapsus$ is a well-funded cybercrime group that has been active since 2019 with a track record of using encryption, malware, phishing and other techniques to execute attacks. They are believed to be behind the Uber breach as well as other attacks on high-profile tech companies.

Attack prioritization beyond the endpoint

Reports show Lapsus$ using compromised credentials to gain access and progress attacks, even with multifactor authentication (MFA) in place. Detection beyond EDR would be required to prioritize and stop a similar attack once actors gain a foothold inside a cloud environment.

About Vectra AI

Vectra® is the leader in hybrid cloud threat detection and response. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai