Attack Signal Intelligence vs. Microsoft Cloud Attack

Cyber attacker targets Microsoft SaaS with stolen credentials.

Incident background:

- Credential theft in play
- Targeting SaaS systems
- Multiple sign-on attempts

¶ Common TTPs used to progress

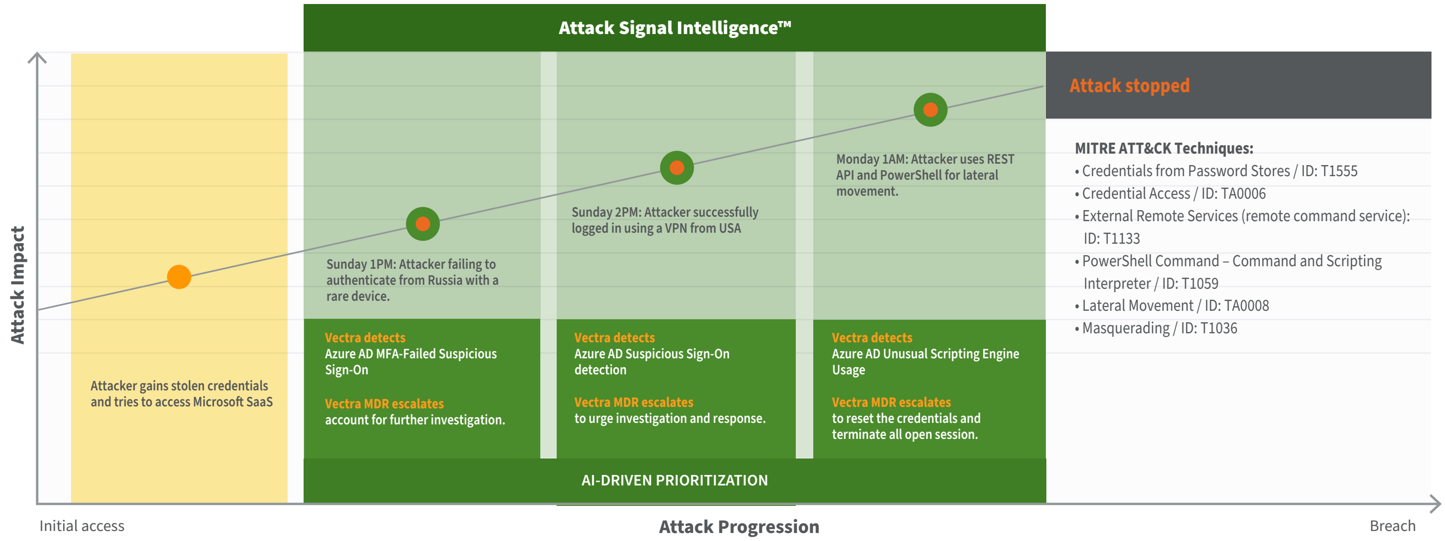
Microsoft Cloud Attack

Actual incident: Vectra AI MDR Analysts prevented M365 attack

Industry: Tech Enterprises

Impact Avoided:
Intellectual Property (IP) theft, sabotage, loss of competitive advantage, damage to customer trust and brand reputation

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



Attacker gains stolen credentials and tries to access Microsoft SaaS

Sunday 1PM: Attacker failing to authenticate from Russia with a rare device.

Vectra detects Azure AD MFA-Failed Suspicious Sign-On

Vectra MDR escalates account for further investigation.

Sunday 2PM: Attacker successfully logged in using a VPN from USA

Vectra detects Azure AD Suspicious Sign-On detection

Vectra MDR escalates to urge investigation and response.

Monday 1AM: Attacker uses REST API and PowerShell for lateral movement.

Vectra detects Azure AD Unusual Scripting Engine Usage

Vectra MDR escalates to reset the credentials and terminate all open session.

MITRE ATT&CK Techniques:

- Credentials from Password Stores / ID: T1555
- Credential Access / ID: TA0006
- External Remote Services (remote command service): ID: T1133
- PowerShell Command – Command and Scripting Interpreter / ID: T1059
- Lateral Movement / ID: TA0008
- Masquerading / ID: T1036

Attack implications:

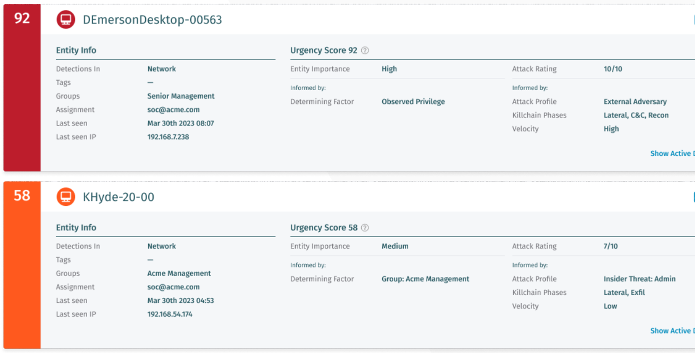
- Intellectual Property (IP) theft
- Sabotage
- Loss of competitive advantage
- Reputation damage
- Loss of customer trust

Credential theft gives cyber attackers the keys to move about an organization and progress towards other objectives. In this instance, an actor gained stolen credentials and headed straight for Microsoft SaaS and attempted to log in.

- Attacker steals admin credentials
- Attempts to access Microsoft SaaS accounts

Prioritizing Tactics

Acting quickly after gaining credentials, the threat actor attempted to authenticate from Russia through an unusual device. With the first attempt failing, they found an alternate route and successfully logged in using a VPN located in the U.S. Once inside, the attackers discovered an opportunity to move laterally through REST API and PowerShell techniques.



92 DEmersonDesktop-00563

Entity Info
Detections In Network
Tags —
Groups Senior Management
Assignment soc@acme.com
Last seen Mar 30th 2023 08:07
Last seen IP 192.168.7.238

Urgency Score 92
Entity Importance High
Informed by:
Determining Factor Observed Privilege

Attack Rating 10/10
Informed by:
Attack Profile External Adversary
Killchain Phases Lateral, C&C, Recon
Velocity High

58 KHyde-20-00

Entity Info
Detections In Network
Tags —
Groups Acme Management
Assignment soc@acme.com
Last seen Mar 30th 2023 04:53
Last seen IP 192.168.54.174

Urgency Score 58
Entity Importance Medium
Informed by:
Determining Factor Group: Acme Management

Attack Rating 7/10
Informed by:
Attack Profile Insider Threat: Admin
Killchain Phases Lateral, Exfil
Velocity Low

Attack Signal Intelligence™ detects and prioritizes:

- Azure AD MFA-Failed Suspicious Sign-On
- Azure AD Suspicious Sign-On detection
- Azure AD Unusual Scripting Engine Usage

After the initial compromise, multiple Vectra AI threat detections were triggered as the attacker progressed. In this case, the customer uses Vectra Managed Detection and Response (MDR) for analyst reinforcement where the team escalated and ultimately stopped the incident as the attacker took action. Whether the response comes from an MDR analyst or an internal member of the security team, the key factor to stopping the attack is having a clear threat signal to detect and prioritize attacker behaviors post compromise.

Integrated signal to detect attacks beyond alert noise

Security analysts are unable to deal with over two-thirds (67%) of the daily alerts they receive.[1] Attackers use this to their advantage to blend in with normal activity and move laterally towards a target. Defenders can adjust by ensuring they have an integrated attack signal to prioritize the most urgent threats and with 24/7 analyst reinforcements by way of an MDR service.

Credential theft enables attackers to fly under the radar

When the attackers gained possession of user credentials, it was only a matter of time before they would find a way into the environment. Tools such as MFA are taken out of play when attackers possess credentials, which was the case during this incident. While the initial attempt failed, the attackers remained persistent and ultimately found a way in. Once inside, having behavioral detection capabilities gave defenders the ability to detect and prioritize tactics that ultimately exposed the attack so the analyst could stop it.

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.

Source[1]: Global Report: *2023 State of Threat Detection, The Defender's Dilemma*

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