Attack Signal Intelligence vs. Hybrid-cloud Attack

Cyberattack progression from on-premises to cloud evades common defense strategies leading to critical threat prioritization in real-time.

Incident background:

- Leading R&D company
- Hybrid-cloud infrastructure
- Uses advanced security measures
- Attackers target zero-day exploit
- Gain path from on-prem to cloud

Hybrid-Cloud Attack

Simulated Incident: One SOC analyst and Vectra stopped a hybrid cloud compromise just before a hacker was able to access high value cloud data

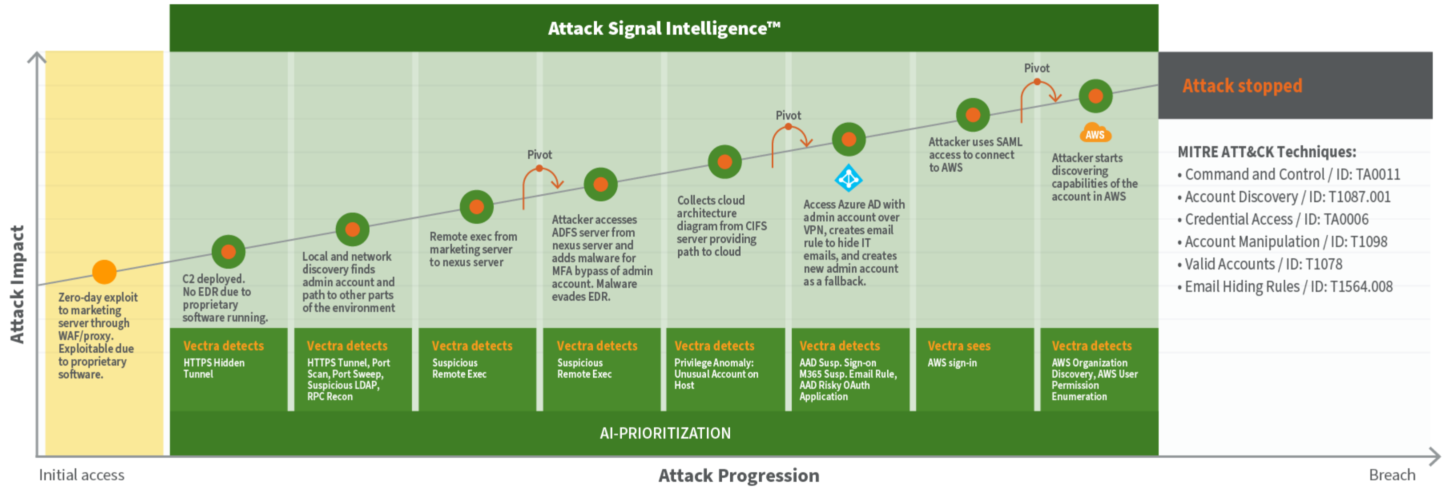
The target: FictoTech

- Leading R&D company
- High-value intellectual property (IP)
- Hybrid cloud

The attacker: ThunderJaw

- State-sponsored hacker group
- Focused on cyber espionage and IP theft
- Targets private organizations

Response time	First Vectra alert	Attack stopped
	5:02a.m	5:22a.m



Attack Signal Intelligence™

Attack Impact

Zero-day exploit to marketing server through WAF/proxy. Exploitable due to proprietary software.

C2 deployed. No EDR due to proprietary software running.

Vectra detects HTTPS Hidden Tunnel

Local and network discovery finds admin account and path to other parts of the environment

Vectra detects HTTPS Tunnel, Port Scan, Port Sweep, Suspicious LDAP, RPC Recon

Remote exec from marketing server to nexus server

Vectra detects Suspicious Remote Exec

Pivot

Attacker accesses ADFS server from nexus server and adds malware for MFA bypass of admin account. Malware evades EDR.

Vectra detects Suspicious Remote Exec

Collects cloud architecture diagram from CIFS server providing path to cloud

Vectra detects Privilege Anomaly: Unusual Account on Host

Pivot

Access Azure AD with admin account over VPN, creates email rule to hide IT emails, and creates new admin account as a fallback.

Vectra detects AAD Susp. Sign-on M365 Susp. Email Rule, AAD Risky OAuth Application

Attacker uses SAML access to connect to AWS

Vectra sees AWS sign-in

Pivot

AWS

Attacker starts discovering capabilities of the account in AWS

Vectra detects AWS Organization Discovery, AWS User Permission Enumeration

AI-PRIORITIZATION

Attack stopped

MITRE ATT&CK Techniques:

- Command and Control / ID: TA0011
- Account Discovery / ID: T1087.001
- Credential Access / ID: TA0006
- Account Manipulation / ID: T1098
- Valid Accounts / ID: T1078
- Email Hiding Rules / ID: T1564.008

Initial access

Attack Progression

Breach

Attack implications:

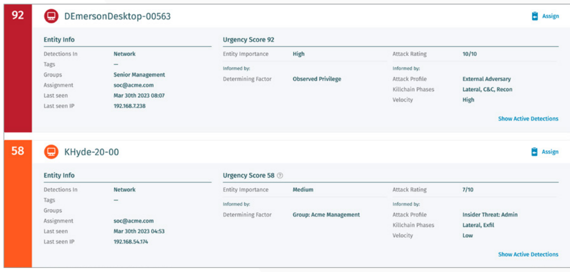
- Data exfiltration
- Loss of intellectual property
- Business disruption
- Reputation damage

As a leading R&D company specializing in advanced materials, FictoTech's high-value intellectual property makes them a prime target for cyberattacks. This attack was initiated through a zero-day exploit that was left unpatched in an on-premises marketing server, where IT does not control software updates.

- Zero-day exploit exposed
- Prevention security not in play
- Actors seeking admin access
- Possible attempt to expose cloud

Prioritizing Tactics

Progressing towards the cloud, attackers navigated the environment with an abundance of tactics starting with command and control (C2) to conduct recon upon access. The attackers were then able to locate admin accounts, add malware to evade MFA and ultimately locate a cloud architecture diagram along with gaining access to Azure AD and AWS. During the process, the actors claimed possession of high-privileged credentials with the potential to enable access critical to parts of the network.



92 DEmersonDesktop-00563

Entity Info		Urgency Score 92			
Detections In	Network	Entity Importance	High	Attack Rating	10/10
Tags	—	Informed by:		Informed by:	
Groups	Senior Management	Determining Factor	Observed Privilege	Attack Profile	External Adversary
Assignment	soc@acme.com			Killchain Phases	Lateral, C&C, Recon
Last seen	Mar 30th 2023 08:07			Velocity	High
Last seen IP	192.168.7.238				

58 KHyde-20-00

Entity Info		Urgency Score 58			
Detections In	Network	Entity Importance	Medium	Attack Rating	7/10
Tags	—	Informed by:		Informed by:	
Groups		Determining Factor	Group: Acme Management	Attack Profile	Insider Threat: Admin
Assignment	soc@acme.com			Killchain Phases	Lateral, Exfil
Last seen	Mar 30th 2023 04:53			Velocity	Low
Last seen IP	192.168.54.174				

Attack Signal Intelligence™ detects and prioritizes:

- HTTPS Hidden Tunnel
- HTTPS Tunnel, Port Scan, Port Sweep, Suspicious LDAP, RPC Recon
- Suspicious Remote Execution
- Privilege Anomaly: Unusual Account on Host
- Azure AD Suspicious Sign-on
- M365 Suspicious Email Rule
- Azure AD Risky OAuth Application
- AWS sign-in
- AWS Organization Discovery
- AWS User Permission Enumeration

With an accurate timestamp of the incident and clear threat detections, the analyst was able to catch up to the attacker in real-time and quickly disable the infected account and lock down the host.

Cloud cyberattacks are the new normal

45% of all data breaches in 2022 were cloud based[1].

Source[1]: IBM – Cost of a Data Breach 2022 report

50% of data breaches involve stolen credentials.[2]

Source [2]: Verizon – Data Breach Investigations report 2022

Attackers keep EDR out of play

The initial exploit posed a detection challenge since IT wasn't in control of the server. This kept EDR out of play as the proprietary software had drivers installed that would interfere with the agent. This incident was the first time that Vectra detected activity on this host, which indicated potential attacker progression. Further into the progression, EDR didn't alert due to the actions involving native tools, while MFA was also bypassed — validating the need for detection functionality capable of alerting on active attacker motions.

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