VECTRA

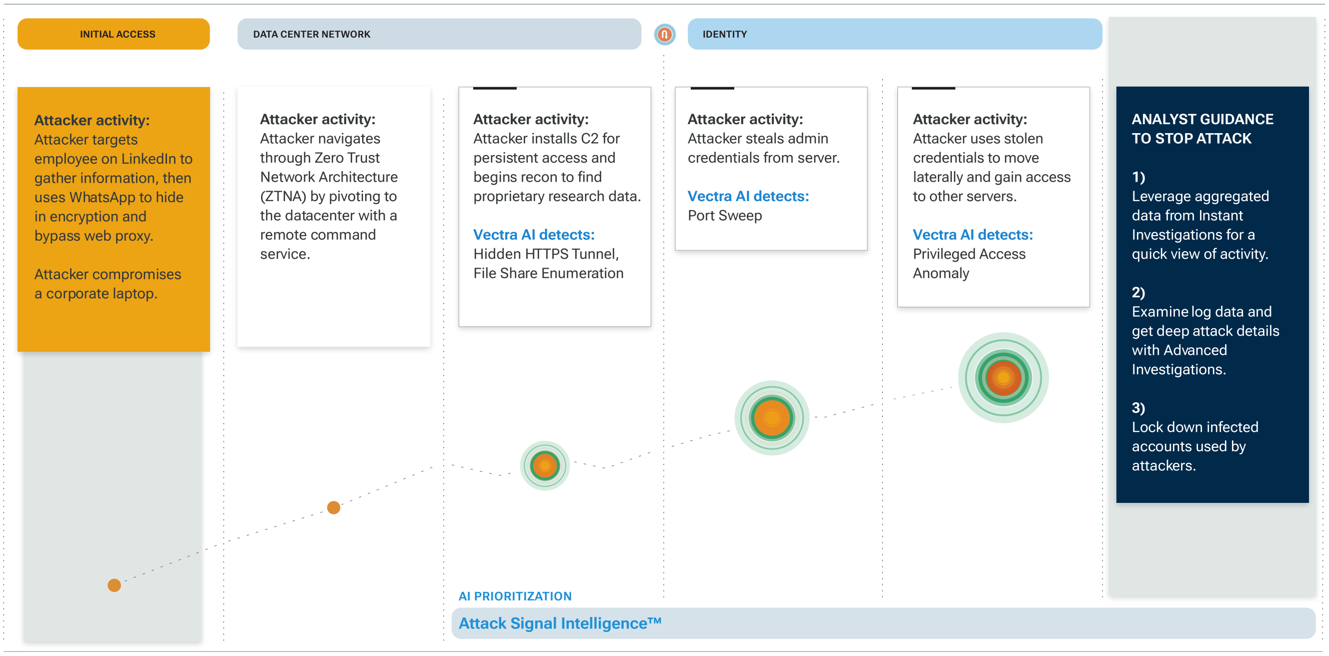
Attack Signal Intelligence vs. Lazarus Cybercrime Group

State sponsored cyber threat group Lazarus initiates cyberattack at a Global 500 company by compromising employee credentials to gain access.

Incident background:

- Lazarus Group
- Global 500 Pharmaceutical company
- Employee targeted on LinkedIn
- Prevention controls failed

Spear Phishing
(simulated attack)



Attacker activity:
Attacker targets employee on LinkedIn to gather information, then uses WhatsApp to hide in encryption and bypass web proxy.

Attacker compromises a corporate laptop.

Attacker activity:
Attacker navigates through Zero Trust Network Architecture (ZTNA) by pivoting to the datacenter with a remote command service.

Attacker activity:
Attacker installs C2 for persistent access and begins recon to find proprietary research data.

Vectra AI detects:
Hidden HTTPS Tunnel, File Share Enumeration

Attacker activity:
Attacker steals admin credentials from server.

Vectra AI detects:
Port Sweep

Attacker activity:
Attacker uses stolen credentials to move laterally and gain access to other servers.

Vectra AI detects:
Privileged Access Anomaly

ANALYST GUIDANCE TO STOP ATTACK

1) Leverage aggregated data from Instant Investigations for a quick view of activity.

2) Examine log data and get deep attack details with Advanced Investigations.

3) Lock down infected accounts used by attackers.

Attack Implications:

- Loss of patent
- Delayed time to market
- Revenue loss
- Reputation damage
- Customer trust concerns

Lazarus Group uses spear-phishing tactics to target employees at pharmaceutical companies — a common theme throughout the pandemic in an attempt to steal proprietary patent information. This attack highlights that trend where an employee at a Global 500 company was targeted through social media to ultimately gain initial access.

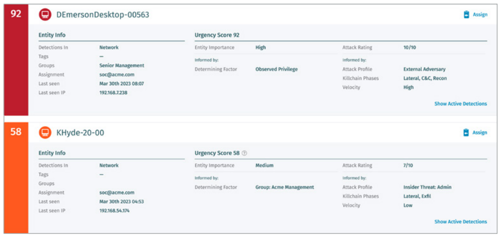
- Employee targeted on LinkedIn
- Encrypts WhatsApp to bypass web proxy
- Compromises corporate laptop
- Moves to data center via remote command

Prioritizing Tactics

Upon gaining access, attackers set up command and control (C2) for persistent access and started recon activities to locate research data. The actors were able to swipe admin credentials and then move laterally to other servers.

Attack Signal Intelligence™ detects and prioritizes:

- Hidden TTPS Tunnel
- File Share Enumeration
- Port Sweep
- Azure AD Privilege Operation Anomaly



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:
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

Clarity into attacker movement with detections mapped to their specific tactics, makes it possible to efficiently prioritize and stop the attack.

A history of exploits

Lazarus is a North Korean state-sponsored cybercrime group that in addition to targeting pharmaceutical companies has been reportedly associated with high-profile attacks such as the one on Sony Pictures in 2014. Recent reports also cite Lazarus for attempting to exploit the Log4J remote code execution vulnerability.

Prioritization beyond prevention

This attack by Lazarus highlights the ability of sophisticated attackers to successfully bypass security controls. Secure web gateway, email security, anti-virus, firewalls, IPS and other tools didn't stop the actors from gaining access.

Once the attackers gained a foothold, detection and prioritization of the attacker activity inside the environment is key for the security team to stop the attack from progressing.

About Vectra AI

Vectra AI 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 MXDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

VECTRA®

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