Poll Question

The webinar will begin momentarily.
Please answer the following poll question before we start:

How prepared is your firm to deal with a potential Scattered Spider attack?

A. Very prepared
B. Somewhat prepared
C. Not prepared
D. Unsure how prepared

abacus group llc

A Leader in Managed IT, Multi-Cloud and Cybersecurity Services for the Global Financial Services Industry

Inside Scattered Spider:

Safeguarding Highly-Regulated Industries from Emerging Cyber Threats

LIVE WEBINAR

AUGUST 11TH, 2025



Our Speakers



Moderator

Jonathan Bohrer

President

abacus groupllc



Panelist

Travis DeForge

Director of Cybersecurity

abacus groupllc

Cybersecurity Unit



Panelist

Michael Brunetti

Senior Director of Incident Response

abacus groupllc

Incident Response Unit



Panelist

Andi Ursry

Senior Threat Intelligence Analyst

blackpoint

Agenda

1. Who is Scattered Spider?
2. Scattered Spider Tactics
3. Post-Breach Incident Response
4. Defensive Strategies
5. Q&A

- **Webinar Duration:** 30-45 minutes
- **Recording:** Webinar will be recorded and emailed
- **Q&A:** Please use Q&A function in GoToWebinar to ask questions

Who is Scattered Spider?

Scattered Spider is a sophisticated cybercriminal group known for **targeting large enterprises with social engineering and ransomware attacks**, often exploiting identity and access management systems. Despite several arrests, the group's decentralized structure has made it remarkably resilient to law enforcement efforts.

Also Known As: UNC3944, Octo Tempest, Muddled Libra

Notable Attacks:

Cartier

Aflac

HAWAIIAN AIRLINES

unfi united natural foods

Industries Attacked:

May 2025 - Present

1. Retail
2. Insurance
3. Airlines
4. Finance / Healthcare

Why is Scattered Spider Targeting?

Target Characteristics:

High-Value Data

PII
Trading Strategies
Transaction Systems
Etc.

Complex IT Infrastructure

Complex Systems to Gain Entry and Move Laterally

Help Desk

Outsourced or Vulnerable Help Desk Operations

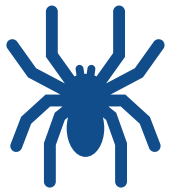
Total Losses to Victims: ~ $9.5 - $25M *since May 2025*

Impacts on Victims:

- Double Extortion: Ransomware + Data Exfiltration
- Operational Downtime
- SEC Disclosure Obligations + Enforcement
- Cyber Insurance Costs + Coverage Implications
- Reputational Damage

Scattered Spider Tactics

Scattered Spider is best known for its highly targeted social engineering attacks, which often serve as the entry point for more destructive campaigns. They rely on legitimate features and tools on devices to execute attacks, as well as utilizing off-the-shelf ransomware.



Phishing and Smishing:
Sending deceptive emails, SMS messages, or chats to trick users into revealing credentials.

Helpdesk Impersonation and Vishing:
Impersonating employees to manipulate IT staff into resetting passwords or bypassing MFA protections or posing as Helpdesk staff to deceive employees into sharing confidential information or installing malicious software.

SIM Swapping:
Hijacking phone numbers to intercept MFA codes.

Deep-fake Voice Calls:
Using AI-generated audio, or even live voice cloning, to impersonate executives or IT personnel.

Case Study of a Scattered Spider Incident

1. Apply social engineering tactics to contact victim's help desk for a password reset and to change MFA settings.
2. Deploy persistent "remote rats" tools to establish access in the environment.
3. Audit victim's infrastructure to identify sensitive and proprietary information and strategic targets, like hypervisors and backups.

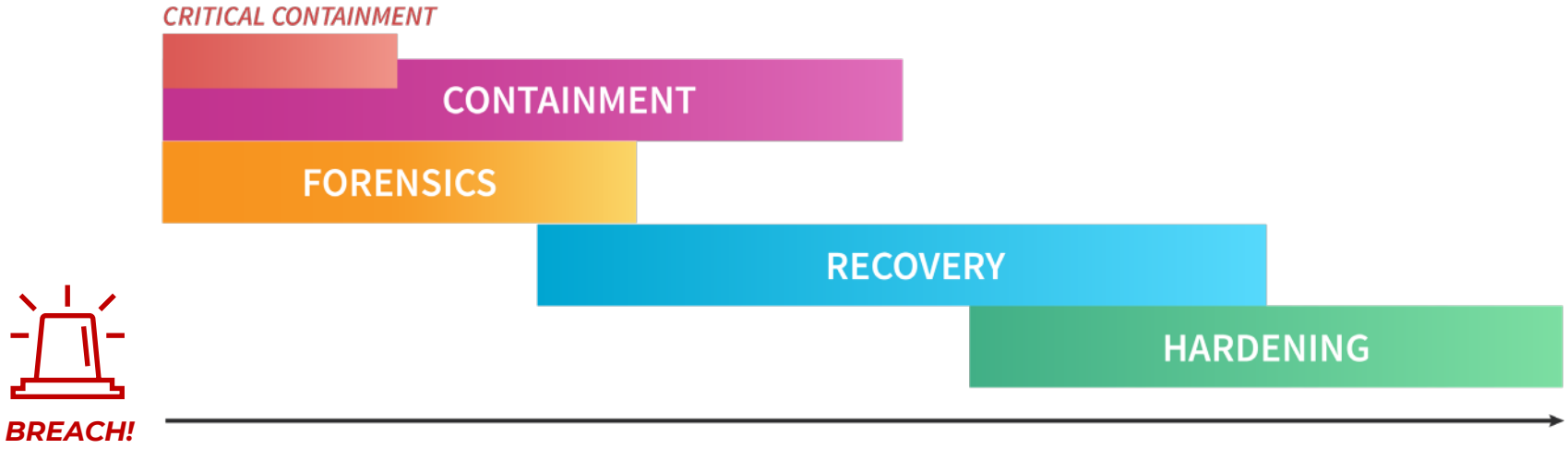
⊘ Abacus Incident Response team disrupts Scattered Spider attack and immediately **contains the threat actor and eradicates them from the environment**.

4. Exfiltrate data.
5. Encrypt systems.
6. Send ransom demand.

MISTAKES COMPANIES MAKE IN THE FIRST 48 HOURS OF A SECURITY INCIDENT

- Letting backups and snapshots roll over
- Restoring over-infected systems
- Not following or not having an incident response plan
- Not bringing in vendors/experts
- Purchasing of additional hardware

Incident Response Recovery Process



- **Critical Containment (24 Hours):** Shutdown all external access in and out of the environment at all sites
- **Containment (2-4 Weeks):** Establish control of the infrastructure to allow internet and systems to be brought back online
- **Forensics (2-4 Weeks):** Identify what the Threat Actor took, how they got in, and what they impacted
- **Recovery (2-6 Weeks):** Restore the environment to the state it was before the incident
- **Hardening (Ongoing):** Strengthen the organization's security posture to ensure the Threat Actor can't get back in

Defensive Strategies



Initial Access	Execution	Persistence & Privilege Escalation	Discovery	Lateral Movement	Post Compromise Activity
• Email Security • Phishing Resistant MFA • Ongoing Security Awareness • Strengthened Help Desk Protocol • Zero Trust	• Endpoint MDR + Cloud MDR • Application Controls	• Phishing Resistant MFA • Endpoint MDR + Cloud MDR • Zero Trust • Strengthened Help Desk Protocols	• Endpoint MDR + Cloud MDR	• Endpoint MDR + Cloud MDR • Zero Trust	• Critical to have an Incident Response partner in place already

Questions?

Use the Q&A Function



Jonathan Bohrer

President,
Abacus Group

jbohrer@abacusgroupllc.com



Travis DeForge

Director of Cybersecurity,
Abacus Group

tdeforge@abacusgroupllc.com



Michael Brunetti

Senior Director of Incident Response,
Abacus Group

michael.brunetti@entaracorp.com



Andi Ursry

Senior Threat Intelligence Analyst,
Blackpoint

aursry@blackpointcyber.com

The recording of this webinar will be shared within 24 hours.
For more updates, follow us on LinkedIn.

LEARN MORE

abacusgroupllc.com