rubrik

8 MODERN ADVERSARY TACTICS

The modern adversary group, Scattered Spider, active since 2022, employs eight sophisticated tactics, ranging from social engineering and MFA bypass to ransomware deployment, to compromise organizations and exfiltrate data.

Social Engineering

(Phishing, Smishing, Impersonation)

Average cost of a data breach that originated from phishing is a staggering $4.88 Million.

IBM Cost of a Data Breach 2025

Data Exfiltration

In 2024, National Public Data suffered a massive data breach with 2.9 billion records impacted, including Social Security numbers and other personal data of millions of Americans.

USA Today

MFA Bypass

(Push Bombing, SIM Swap, Session Proxy Interception)

While 87% of leaders believe phishing-resistant MFA is critical to their security strategies, only 30% are highly confident in their phishing controls.

Duo

Ransomware Deployment

Ransomware as a Service (RaaS) group ALPHV/BlackCat extorted over $300 Million in ransomware payments, derived from over 1,000 victim organizations, according to the FBI.

Bleeping Computer

Initial Access via Compromised Credentials

1.8 billion credentials were stolen in the first half of 2025.

Flashpoint Global Threat Intelligence

Lateral Movement

The global median dwell time for cyberattacks has risen to 11 days, providing adversaries a significant opportunity to engage in lateral movement.

Google Cloud Security M-Trends 2025 Report

Living off the Land (LotL) and Cloud (LotC)

In 2024, malware-free activity accounted for 79% of all detections.

CrowdStrike 2025 Global Threat Report

Bring-Your-Own-Vulnerable-Driver (BYOVD)

Nearly 1 in 4 ransomware attacks featured some sort of anti-EDR (evasion or tampering) or privilege escalation powered by BYOVD techniques.

Huntress

5 Steps to be Cyber Resilient

Understanding attack methods is the first step toward building a robust cyber resilience and recovery plan that incorporates five key steps to protect your critical data and identities. If an attack is inevitable, then a focus on reducing risk, minimizing impact, and optimizing recovery is critical.

1. 

Future-proof your data with an air-gapped and immutable architecture.

2. 

Prepare by running cyber recovery attack simulations.

3. 

Reduce blast radius of a compromised identity and identify abnormal patterns of hypervisor-based encryption of files on VMs.

4. 

Monitor backups for malware, hunt for threats, and recover without reinfection.

5. 

Restore identity services to combat the threat actor's lateral movement and persistence tactics.

To learn more about how to build a cyber resilience and recovery plan for protection from modern adversaries like Scattered Spider that target data and identities, download this white paper.