HostBreach

Lead Qualification Report

Cybersecurity Sales Enablement Intelligence

Apex Manufacturing Corp.

Manufacturing | 850 Employees | Phoenix, AZ

78

RISK SCORE

HIGH PRIORITY

143	8	WEAK	$2.4M
EXPOSED CREDENTIALS	INFOSTEALER INFECTIONS	SECURITY MATURITY	EST. BREACH EXPOSURE

IDENTIFIED PAIN POINTS

5 Critical Findings

- ! **143 employee credentials** found in breach databases and infostealer logs
- ! **8 active infostealer infections** with session tokens that bypass MFA
- ! **DMARC not enforcing** (p=none) - vulnerable to email spoofing
- ! **Ransomware incident** reported in Q3 2024 (BlackCat affiliate)
- ! **12 CVEs identified** on external infrastructure including 3 critical
- ! **Shadow IT detected** - unauthorized cloud storage and remote access tools

CREDENTIAL EXPOSURE INTELLIGENCE

143 Records

SOURCE TYPE	COUNT	SEVERITY	DETAILS
Infostealer Logs	8	CRITICAL	Active infections with session cookies for M365, Salesforce, AWS. MFA bypass possible.
Breach Databases	89	HIGH	LinkedIn (2021), Dropbox (2012), Adobe (2013) - includes plaintext and hashed passwords
Combolist Exposure	46	MEDIUM	Credentials appearing in aggregated credential lists used for credential stuffing attacks

EXTERNAL ATTACK SURFACE

24 Assets

ASSET TYPE	COUNT	RISK LEVEL	NOTABLE FINDINGS
Web Applications	12	HIGH	Exposed admin panels, outdated WordPress instances, staging environments
Remote Access	4	CRITICAL	RDP exposed on 2 hosts, VPN gateway with known CVE, SSH on non-standard port
Mail Servers	3	MEDIUM	Exchange server with outdated patches, open relay detected on dev server
Cloud Infrastructure	5	MEDIUM	AWS S3 buckets enumerable, Azure blob with weak permissions

EMAIL SECURITY POSTURE

⚠	✔	✗
SPF	**DKIM**	**DMARC**
Too permissive (+all)	Configured	p=none (not enforcing)

Risk: Email spoofing attacks possible. Attackers can send emails appearing to come from @apexmfg.com without detection.

BREACH HISTORY

DATE	TYPE	DETAILS
Q3 2024	Ransomware	BlackCat affiliate, data exfiltration confirmed
2022	Phishing	BEC incident, wire fraud attempt

SAAS & SHADOW IT DISCOVERY

18 Services Detected

CATEGORY	SERVICES DETECTED	RISK	NOTES
Cloud Storage	Dropbox, Google Drive, Box	HIGH	Personal accounts detected alongside corporate - potential data leakage
Remote Access	TeamViewer, AnyDesk	CRITICAL	Unauthorized remote access tools on corporate network
Productivity	Slack, Notion, Trello	MEDIUM	Potential sensitive data in unmanaged collaboration tools
Dev/Staging	staging.apexmfg.com, dev.apexmfg.com	HIGH	Development environments exposed to internet with test credentials

SALES RECOMMENDATION

PURSUE - HIGH PRIORITY

This account shows clear signs of security pain and recent incident history. The ransomware attack in Q3 2024 indicates budget allocation for security investments. Active infostealer infections with MFA-bypassing session tokens create urgency. The weak email security posture and exposed remote access infrastructure provide multiple entry points for discussion.

Recommended approach: Lead with the infostealer findings and session token exposure. Reference the ransomware incident as evidence that their current controls aren't sufficient. The DMARC gap is a quick win that demonstrates immediate value.

This report contains intelligence gathered from publicly available sources and commercial threat intelligence feeds. Data is provided for sales enablement purposes. Findings should be verified before customer communication.

HostBreach | Security Intelligence
Generated: January 2026