CONFIDENTIAL

CS

CloudShield
Managed IT

Security Risk Assessment

Credential Exposure Analysis

example-corp.com

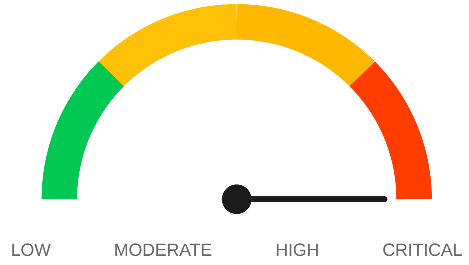
Prepared exclusively for

CloudShield Managed IT

December 12, 2025

CloudShield Managed IT

Executive Summary



100

CRITICAL

👤

4

COMPROMISED IDENTITIES

🔓

17

STOLEN PASSWORDS

🦠

4

MALWARE INFECTIONS

The 100/100 CRITICAL risk score signals an immediate, severe security breach. Active infections with Lumma and RedLine Stealers currently grant attackers direct access to corporate bank accounts, sensitive data, and system sessions. Seventeen recent findings confirm ongoing, active compromise.

Four compromised identities and seventeen stolen passwords, often from private accounts on company devices, create direct ransomware entry points. Critical email security failures (SPF/DMARC) enable widespread phishing, demanding immediate, decisive action.

🦠 Critical Malware Findings (Stealer Logs)

This data originates from infected devices. The affected computers were compromised by infostealer malware that extracted passwords, browser cookies, and session tokens. The risk of ransomware attack or account takeover is immediate.

Email	Password	Source	Date	Logins
ce***@example-corp.com	••••***	Lumma Stealer	Oct 15, 2025 58 DAYS AGO	example-corp.com linkedin.com ... 4x
in***@example-corp.com	••••***	Generic Stealer	Oct 1, 2025 72 DAYS AGO	example-corp.com mailchimp.com ... 4x
ac***@example-corp.com	••••***	RedLine Stealer	Sep 20, 2025 83 DAYS AGO	example-corp.com quickbooks.com ... 5x
in***@example-corp.com	••••***	Generic Stealer	Sep 15, 2025 88 DAYS AGO	example-corp.com github.com ... 4x

* **Lumma Stealer**: Steals online banking credentials and browser sessions. Attackers can impersonate your employee.

* **Generic Stealer**: Passwords were stolen from an infected device. The device must be identified and remediated.

* **RedLine Stealer**: Most widespread malware in 2024. Steals VPN credentials – attackers can infiltrate your corporate network.

Email Security

External Attack Surface

❌ CEO Fraud Risk

HIGH

Currently, any criminal can send an email that technically appears to come from @example-corp.com. Your accounts payable department could be deceived.

❌ SPF (Sender Policy Framework)

Critical

No SPF record. Domain is vulnerable to email spoofing.

❌ DMARC (Domain-based Message Authentication)

Critical

No DMARC record. No protection against phishing attacks.

Threat Index

No email authentication

Recommended Actions

Immediate Steps

⚠️ **IMPORTANT QUESTION**

"Did your current IT provider inform you about these security gaps?"

If not: Why not?

Identified Gap	Recommended Action
⚠ Malware Infections	✅ EDR Solution + 24/7 Threat Monitoring
⚠ Compromised Passwords	✅ Enterprise Password Manager + Auto-Rotation
⚠ Missing MFA	✅ MFA Rollout for All Critical Systems
⚠ Phishing Susceptibility	✅ Security Awareness Training

Next Step

📧 info@cloudshield-it.com 📞 +1 (555) 234-5678

Schedule Your Security Assessment

This report contains confidential information regarding the security posture of example-corp.com. Generated by CloudShield Managed IT.

Immediate Action Checklist

Prioritized tasks based on your risk analysis

IMMEDIATE (0-4 hours)

- □ Identify infected device: `ce***@example-corp.com`
- □ Identify infected device: `in***@example-corp.com`
- □ Identify infected device: `ac***@example-corp.com`
- □ Identify infected device: `in***@example-corp.com`

URGENT (24-48 hours)

- □ Enable MFA: `ce***@example-corp.com`
- □ Reset password: `ce***@example-corp.com`
  `for linkedin.com, microsoft365.com, zoom.us`
- □ Enable MFA: `in***@example-corp.com`
- □ Reset password: `in***@example-corp.com`
  `for mailchimp.com, hubspot.com, dropbox.com`
- □ Enable MFA: `ac***@example-corp.com`
- □ Reset password: `ac***@example-corp.com`
  `for quickbooks.com, stripe.com, paypal.com, chase.com`
- □ Enable MFA: `in***@example-corp.com`
- □ Reset password: `in***@example-corp.com`
  `for github.com, figma.com, notion.so`

This Week

- □ Configure SPF record: `example-corp.com`
- □ Configure DMARC record: `example-corp.com`