Report CTI Example

This is a CTI report

Your Company

March 27, 2025

acme

Summary

1 Evil Company Data Leak - Cyber Threat Intelligence Report

2 Introduction

The Cyber Threat Intelligence (CTI) team is responsible for monitoring the Deep & Dark Web to protect brand integrity and prevent the exposure of sensitive information. This proactive monitoring aims to identify Zero-Day threats, data leaks, credential leaks, new vulnerabilities, and ransomware activities that may affect the organization, manufacturers, or partners.

3 Executive Summary

A threat actor known as “DarkPhantom” claimed on a notorious underground forum to have access to approximately **10 million** customer records from Evil Company’s authentication systems. This includes compromised credentials from the company’s Single Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP) systems.

4 Threat Details

According to the forum post, the attacker allegedly breached Evil Company’s authentication servers (auth.evilcompany.com), leading to the exfiltration of millions of user credentials and sensitive information. The attacker claims to have obtained the following data:

- Encrypted passwords (SSO & LDAP)
- API keys
- Authentication tokens
- Private encryption keys
- Internal employee directory information

While the SSO passwords are encrypted, the attacker asserts that they can be decrypted using the available key files. Similarly, the hashed LDAP passwords may be cracked. The attacker, however, admitted their lack of computational resources to conduct brute-force decryption and is seeking assistance from other cybercriminals in exchange for a portion of the stolen data.

The attacker has shared the following samples as proof:

- **Sample File 1:** A list containing 250,000 affected email addresses and domains.
- **Sample File 2:** A database dump with sensitive authentication information, including:
  - User IDs
  - Encrypted passwords

  - User roles and permissions
  - API access logs
  - Multi-Factor Authentication (MFA) statuses

- **Sample File 3:** Encrypted private keys allegedly linked to Evil Company's internal services.

5 Threat Actor Profile

The threat actor "DarkPhantom" is a relatively new member of the cybercrime community, registered on the dark web forum in March 2025. They have no significant reputation but have made several posts related to credential leaks and database breaches. In addition to their forum activity, they also operate on encrypted messaging platforms, where they offer stolen data for sale or trade.

6 Forum Post by the Attacker

Message from the attacker.

```
Evil Company authentication servers breached (auth.evilcompany.com)

Hey,
I have successfully breached Evil Company's authentication servers, affecting their SSO and LDAP systems.
Over 10 million user records have been stolen, including encrypted passwords, API keys, and internal authentication data.

The encrypted passwords **can be decrypted**, but I need assistance to brute-force them. In exchange, I will share part of the stolen data.

Companies can pay to have their employee data removed before the full database is sold.

I'm also willing to trade for 0-day exploits.

PM me for offers.

Sample Data > []
Company List > []
Encryption Keys > []
```

7 Image of the Post

Figure 1: Extracted from Underground Forum

8 Shodan Information

```
Remote Desktop Protocol NTLM Info:
  OS: Windows Server 2019
  OS Build: 10.0.17763
  Target Name: EVILCOMPANY
  NetBIOS Domain Name: EVILCOMPANY
  NetBIOS Computer Name: EVILSRV001
  DNS Domain: evilcompany.com
```

9 Mitigation Recommendations

1. **Immediate Password Resets**: Force password resets for all affected users.
2. **MFA Enforcement**: Ensure multi-factor authentication is mandatory for all accounts.
3. **Network Segmentation**: Isolate critical authentication servers to prevent lateral movement.
4. **Log Analysis**: Review access logs for unusual login attempts or unauthorized access.
5. **Threat Hunting**: Proactively search for indicators of compromise (IOCs) related to this breach.
6. **Dark Web Monitoring**: Continue monitoring underground forums for further leaks or activity related to this incident.

10 Conclusion

This breach highlights the growing threats posed by cybercriminals targeting enterprise authentication systems. Evil Company must take immediate action to mitigate potential damages and strengthen its security posture to prevent future incidents.