REDSTRIKE

# ASSESSMENT REPORT

## GLOBAL FINANCE CORPORATION

MAR 2024

# Executive Summary

Financial Corporation underwent a red team assessment from February 1-18, 2024 simulating APT41 tactics, techniques, and procedures (TTPs). The assessment successfully achieved all primary objectives, revealing significant security vulnerabilities in database access controls, password management, and incident response procedures.

## Goals

- Evaluate security posture against APT41-style attacks.
- Test database access controls and privilege escalation paths.
- Assess password security and incident response effectiveness.

## Strengths

- Incident response team successfully detected malware deployment.
- Network segmentation effectively limited the scope of initial system access.
- Endpoint protection controls (evasion detection & response) software demonstrated partial effectiveness.

## Improvements

- Severe weaknesses in database access controls.
- Inadequate password complexity and strength requirements.
- Slow detection and response to privilege escalation attempts.

## Recommendations

- Implement strict database access controls with comprehensive monitoring.
- Strengthen password policies and implement multi-factor authentication.
- Deploy advanced endpoint detection and response (EDR) solutions for workstations and servers.
- Implement ongoing security awareness training and education.

# Table of Contents

# 01

# Methodology

## Scenario

The red team emulated APT41, a sophisticated threat actor known for financial theft and cyber espionage. The operation focused on database compromise, credential theft, and targeted malware deployment.

## 1.1 Scope

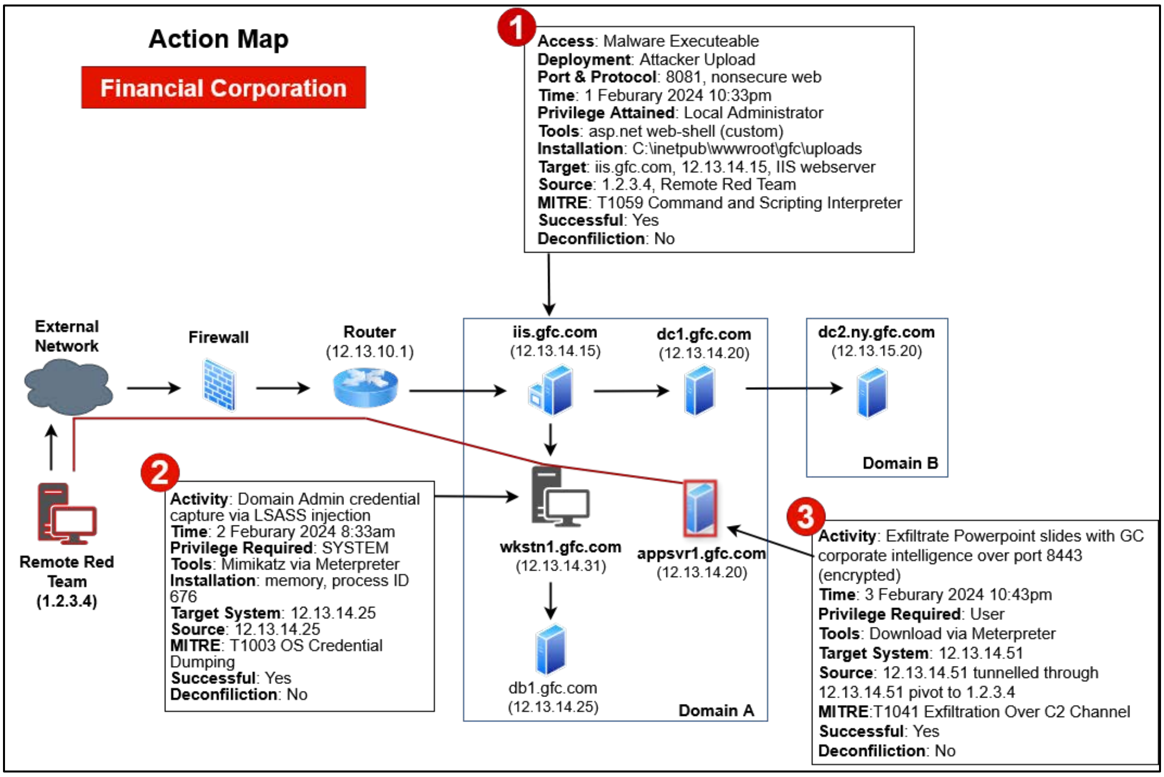
- Target: Financial database infrastructure.
- System: IIS, WKSTN1, APPSVR1
- Duration: 2 weeks (February 1-18 2024).
- Restrictions: WKSTN1 D: drive encryption only.

## 1.2 Action & Event Map

1. Initial Access: Phishing campaign targeting database users.

2. Privilege Escalation: Lateral movement to get DA rights from WKSTN1.

3. Malware Deployment: Targeted encryption and data exfiltration APPSVR1.



1

**Access**: Malware Executeable
**Deployment**: Attacker Upload
**Port & Protocol**: 8081, nonsecure web
**Time**: 1 Feburary 2024 10:33pm
**Privilege Attained**: Local Administrator
**Tools**: asp.net web-shell (custom)
**Installation**: C:\inetpub\wwwroot\gfc\uploads
**Target**: iis.gfc.com, 12.13.14.15, IIS webserver
**Source**: 1.2.3.4, Remote Red Team
**MITRE**: T1059 Command and Scripting Interpreter
**Successful**: Yes
**Deconfiliction**: No

2

**Activity**: Domain Admin credential capture via LSASS injection
**Time**: 2 Feburary 2024 8:33am
**Privilege Required**: SYSTEM
**Tools**: Mimikatz via Meterpreter
**Installation**: memory, process ID 676
**Target System**: 12.13.14.25
**Source**: 12.13.14.25
**MITRE**: T1003 OS Credential Dumping
**Successful**: Yes
**Deconfiliction**: No

3

**Activity**: Exfiltrate Powerpoint slides with GC corporate intelligence over port 8443 (encrypted)
**Time**: 3 Feburary 2024 10:43pm
**Privilege Required**: User
**Tools**: Download via Meterpreter
**Target System**: 12.13.14.51
**Source**: 12.13.14.51 tunnelled through 12.13.14.51 pivot to 1.2.3.4
**MITRE**:T1041 Exfiltration Over C2 Channel
**Successful**: Yes
**Deconfiliction**: No

## 1.3 Technical Attack Summary

- Used spear-phishing with malicious attachments.
- Exploited unpatched vulnerabilities for privilege escalation.
- Leveraged PowerShell for credential harvesting.
- Deployed custom encryption malware.
- Exfiltrated sensitive database records.

# 02

# Assessment Timeline & Narrative

Team Delta conducted a red team assessment against Global Financial Corporation (GFC), simulating APT41's tactics through real-world adversarial techniques. The assessment began on February 1, 2024, at 0900 CST with an Open-Source Intelligence (OSINT) campaign. By targeting GFC's company website, social media, and job postings, Team Delta gathered extensive intelligence, including user profiles, email addresses, phone numbers, and technology details—all critical preparation for the planned spear-phishing campaign.

## 2.1 Initial Access Phase

The red team began by launching a targeted spear-phishing campaign using malicious CHM file attachments. Within hours, they established their first foothold across multiple network segments. Using a customized version of Cobalt Strike for command and control, the campaign successfully compromised several systems. The team secured user persistence through Startup Folders and Windows Services. After establishing initial access and persistence, they shifted to system and network enumeration, using BloodHound to map Active Directory objects and network infrastructure.

## 2.2 Lateral Movement & Privilege Escalation

By February 6, the team had identified and compromised key intermediary systems that provided access to segmented parts of the network. Using a combination of Remote Desktop Protocol, stolen credentials, and administrative group manipulation, the red team moved laterally across two network segments. The team used Mimikatz for credential dumping and Snaffler to crawl network shares, successfully getting elevated credentials and privileges.

## 2.3 Database Targeting Phase

In the second week, the operation targeted the database infrastructure. The team employed SQL injection techniques along with specialized tools like Sqlmap and JexBoss to breach database environments. They established persistence by modifying the MSSQL database dbo.My_Procedure script to create a user with system privileges upon execution.

## 2.4 Data Exfiltration & Encryption

The final phase took place on February 6-18, during which the team created RAR archives to simulate data exfiltration. Following APT41's typical patterns, the team conducted operations during UTC+8 business hours (9:00 AM to 9:00 PM). The assessment concluded with a targeted encryption demonstration on WKSTN1, with the impact carefully contained on the D: drive per engagement parameters.

## 2.5 Evasion Techniques

Throughout the engagement, the team demonstrated APT41's characteristic agility by quickly adapting to defensive measures. When security teams blocked access, the red team responded within hours by re-compiling backdoors with new command-and-control domains. The team maintained persistent access by using six malware obfuscation techniques: string encryption, code packing, control flow obfuscation, dead code insertion, variable renaming, and arithmetic manipulation—all to evade detection.

## 2.6 Assessment Conclusion

Within the two-week timeframe, the red team successfully compromised 11 systems across two network segments, achieving all objectives. The operation proved the effectiveness of APT41's sophisticated TTPs while maintaining strict operational security and following engagement parameters. The assessment uncovered critical vulnerabilities in database access controls and incident response procedures, yielding valuable insights for improving Global Financial Corporation's security posture.

# 03

# Technical Findings & Recommendations

### Risk Ratings & Factors

The risk rating system employed is used to prioritize and categorize security issues discovered during the assessment. The system uses three distinct severity levels - high, medium, and low - allowing for clear differentiation between critical security concerns and less urgent matters that require attention.

### Risk Ratings

| Score | Description |
|---|---|
| **High** | Adversaries may disrupt, destroy, or intrude upon critical systems, information processes, and information sources. |
| **Medium** | The compromise or corruption of sensitive data, loss of service across systems or information processes, manipulation of data, or degradation of logistical support—all of which could impair operations indefinitely. |
| **Low** | The impact on information operations, processes, or sources is minimal or nonexistent. |

## 3.1 Technical Findings

| **Observation Findings** | |
|---|---|
| **Active Directory Enumeration** | **High** |
| **Description & Observations**<br>Active Directory enumeration was successful using a combination of Bloodhound and SharpHound tools without detection, indicating weak monitoring of AD reconnaissance activities. | |
| **Operational Impact**<br>Attackers can map entire network infrastructure and identify high-value targets. | |
| **Affected Assets**<br>Domain Controllers, Active Directory Services. | |
| **Recommendation**<br>Implement robust Active Directory auditing, deploy advanced endpoint detection and response (EDR) solutions to monitor enumeration activities, and establish baseline behavioral analytics. | |

| **Observation Findings** | |
|---|---|
| **Spear-phishing** | **High** |
| **Description & Observations**<br>Spear-phishing campaign using CHM files successfully bypassed email security controls. | |
| **Operational Impact**<br>Compromised HR workstations provide initial access points for further network penetration. | |
| **Affected Assets**<br>HR Department Workstations, Email Servers | |
| **Recommendation**<br>Deploy advanced email filtering solutions, implement CHM file blocking policies, conduct regular phishing awareness training. | |

| **Observation Findings** | |
|---|---|
| **SQL Injection Vulnerabilities** | **High** |
| **Description & Observations**<br>SQL injection vulnerabilities in database infrastructure allowed unauthorized access. | |
| **Operational Impact**<br>Sensitive financial data is directly accessible, increasing the potential for manipulation. | |
| **Affected Assets**<br>Database Servers, Financial Applications | |
| **Recommendation**<br>Implement WAF solutions, conduct regular penetration testing, enforce prepared statements in application code, deploy database activity monitoring. | |

| Observation Findings | |
|---|---|
| **Lateral Movement** | **Medium** |
| **Description & Observations**<br>Lateral movement using RDP and stolen credentials went undetected for extended periods. | |
| **Operational Impact**<br>Unrestricted internal network movement allows attackers to access critical systems. | |
| **Affected Assets**<br>Network Infrastructure, Windows Servers | |
| **Recommendation**<br>Implement network segmentation, deploy privileged access management (PAM) solutions, enable RDP logging and monitoring. | |

| Observation Findings | |
|---|---|
| **Malware persistence** | **Medium** |
| **Description & Observations**<br>Malware persistence achieved through multiple backdoors remained undetected. | |
| **Operational Impact**<br>The potential for future attacks exists because of long-term unauthorized system access. | |
| **Affected Assets**<br>Enterprise Workstations, WKSTN1, Servers | |
| **Recommendation**<br>Deploy advanced malware detection systems, implement application whitelisting, establish robust incident response procedures. | |

# 04

# Conclusion

The red team assessment revealed significant security gaps in the Financial Corporation's defensive cybersecurity posture. Although some security controls proved effective, Financial Corporation critically needs improvements in database access controls, password management, and malware detection capabilities. Implementing the recommended security measures will significantly enhance the organization's security posture against APT41-style attacks.

REDSTRIKE