Incident Report: APT52 Attack on Apex Financial

Incident ID: INC250306_5689

Course: Incident Handling BFOR 643

Faculty: Premila Melvin, John Griffin

Team Members:

Leela Pavan Kumar K
Shalem Raju M
Sriram R
SriVarsha A
Junaid M
Phanindhar Reddy K

Department of Cyber Security and Digital Forensics

Date: April 1, 2025

Contents

1 Background Information

- **Organization:** Apex Financial (online banking, investment management, and financial consulting)
- **Target:** Sensitive customer financial data and proprietary trading algorithm
- **Threat Actor:** APT52 (Advanced Persistent Threat group specializing in financial espionage)
- **Initial Vector:** Spear-phishing campaign targeting finance/IT employees
- **Objective:** Data exfiltration and long-term persistence establishment

2 Executive Summary

On **March 6, 2025**, Apex Financial was compromised by APT52 through:

- **Initial Vector:** Spear-phishing email delivering malicious PDF macro
- **Compromised Host:** WORKSTATION-01 (`apexfinancial\analyst1`)
- **Tactics:** Execution (T1204.002), Persistence (T1053)
- **Final Payload:** ShadowCrypt ransomware on `192.168.1.200`

3 Incident Notification

- **Severity:** Critical
- **Detection Time:** 2025-03-06T16:45:32 EST
- **EDR Alert:** Malicious macro execution on WORKSTATION-01
- **Response:** Immediate containment and recovery actions initiated

4 Attack Timeline

- **16:59:36 UTC:** Spear-phishing email delivered
- **17:04:36 UTC:** Malicious macro executed (T1204.002)
- **17:29-17:34 UTC:** Credential compromise (`analyst1`)
- **18:04:36 UTC:** Pass-the-hash attack
- **18:14-18:19 UTC:** WMI/PsExec lateral movement
- **19:59:36 UTC:** Ransomware deployed
- **20:04:36 UTC:** Persistence established (T1053)

5 Detailed Analysis

5.1 Phase 1: Initial Compromise (Spear-Phishing)

Evidence: Splunk Query: `sourcetype="email_gateway" "Spear-phishing"` **MITRE ATT&CK:** T1566.001 - Phishing: Spearphishing Attachment

Analysis: The attacker sent a targeted email with malicious PDF attachment to `user@apexfinancial.com`, bypassing email filters through social engineering tactics.

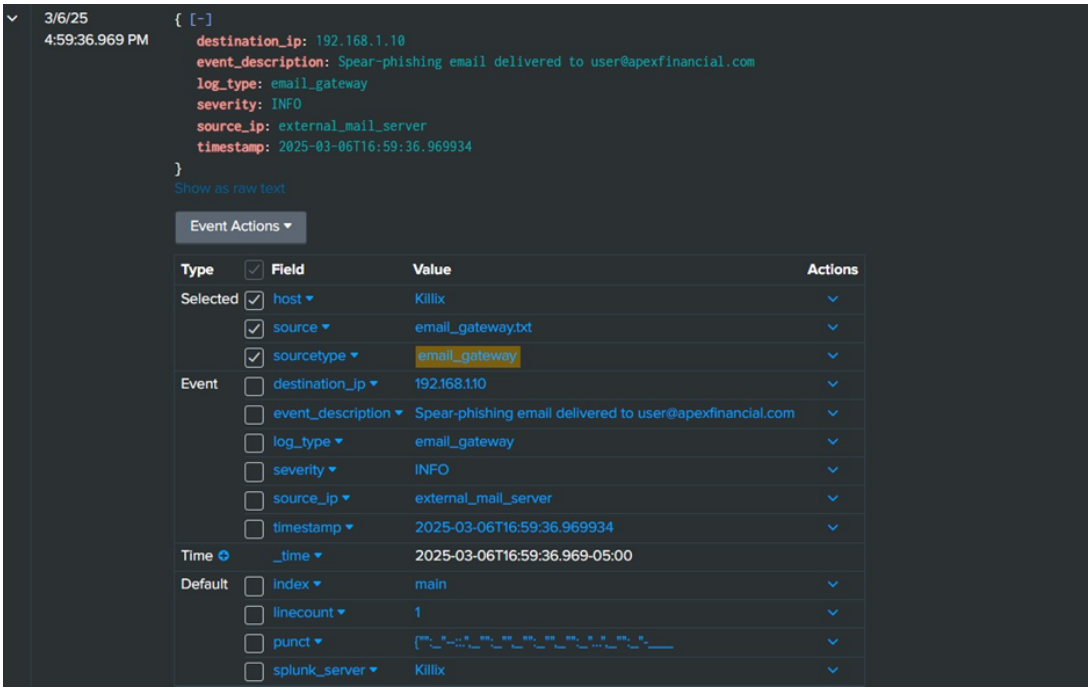

Figure 1: Spear-phishing email delivery log

5.2 Phase 2: Malicious Macro Execution

Evidence: Splunk Query: `sourcetype="endpoint_security" "malicious macro"` **MITRE ATT&CK:** T1204.002 - User Execution: Malicious File

Analysis: The macro from `Q1_Performance_Review.pdf` executed on WORKSTATION-01 (`192.168.1.10`), leading to:

- C2 communication establishment
- Credential dumping via Mimikatz
- Initial persistence mechanisms

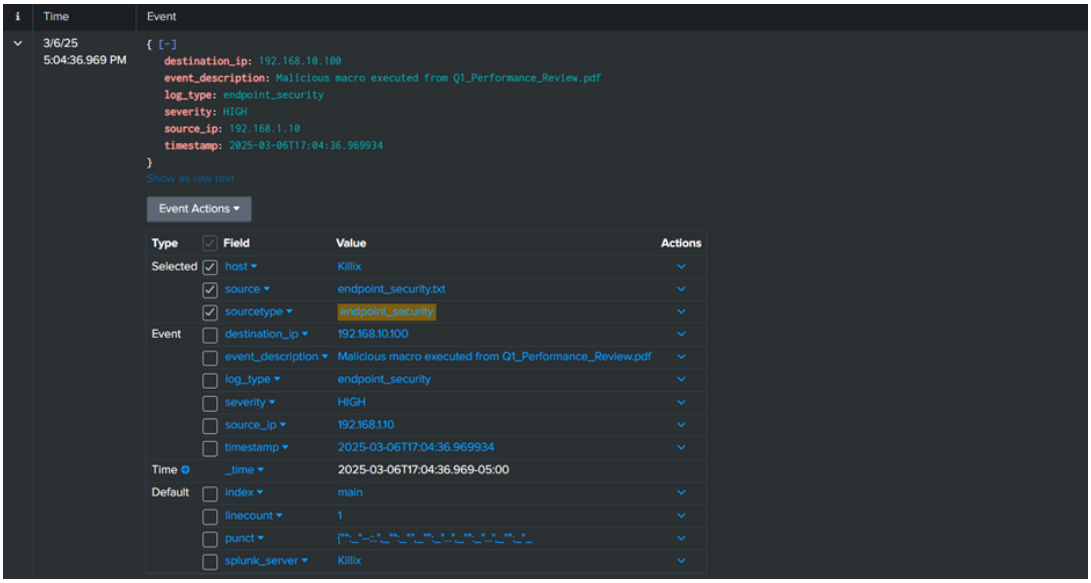

Figure 2: EDR alert for macro execution

5.3 Phase 3: Credential Access

5.3.1 Brute-Force Attempt

Evidence: Splunk Query: `sourcetype="authentication" "Failed login"` **MITRE ATT&CK:** T1110 - Brute Force

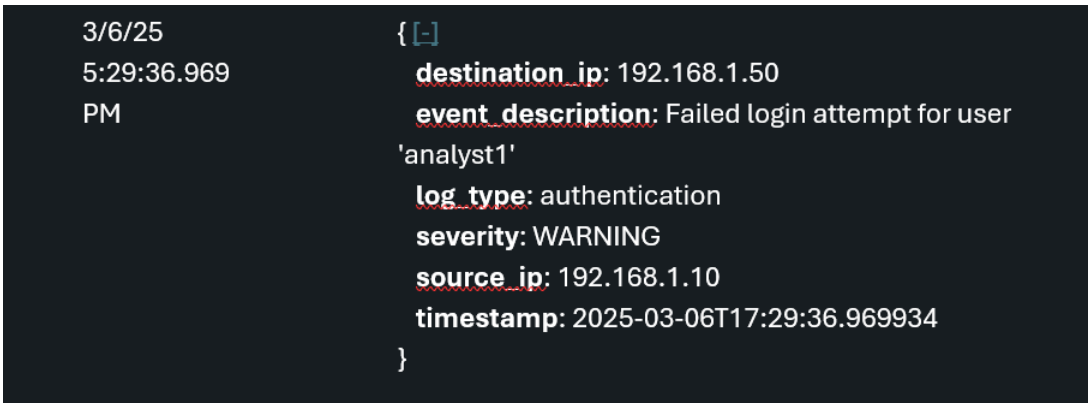

Figure 3: Failed login for `analyst1`

5.3.2 Credential Compromise

Evidence: Splunk Query: `sourcetype="authentication" "Successful login" user="analyst1"` **MITRE ATT&CK:** T1078 - Valid Accounts

Figure 4: Successful authentication as `analyst1`

5.3.3 Pass-the-Hash Attack

Evidence: Splunk Query: `sourcetype="authentication" "Pass-the-hash"` **MITRE ATT&CK:** T1550.002 - Use Alternate Authentication Material: Pass the Hash

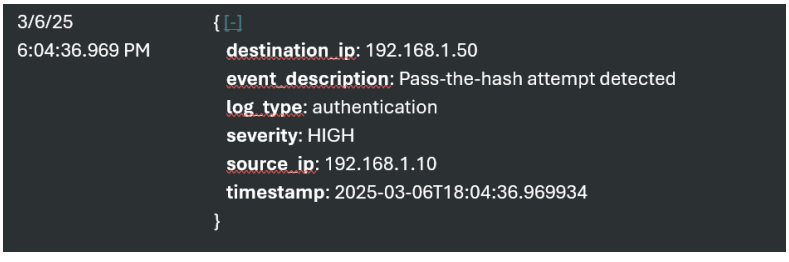

Figure 5: Pass-the-hash detection

5.4 Phase 4: Lateral Movement

5.4.1 WMI Execution

Evidence: Splunk Query: `sourcetype="endpoint_security" "WMI"` **MITRE ATT&CK:** T1047 - Windows Management Instrumentation

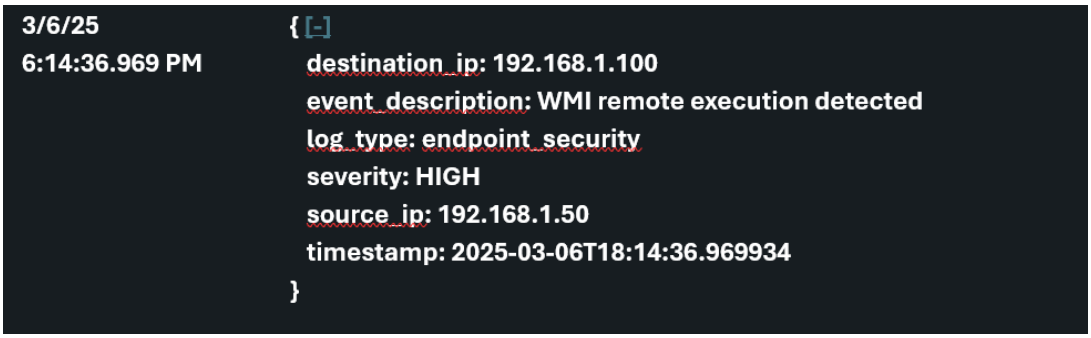

Figure 6: WMI remote execution

5.4.2 PsExec Execution

Evidence: Splunk Query: `sourcetype="endpoint_security" "PsExec"` **MITRE ATT&CK:** T1569.002 - System Services: Service Execution

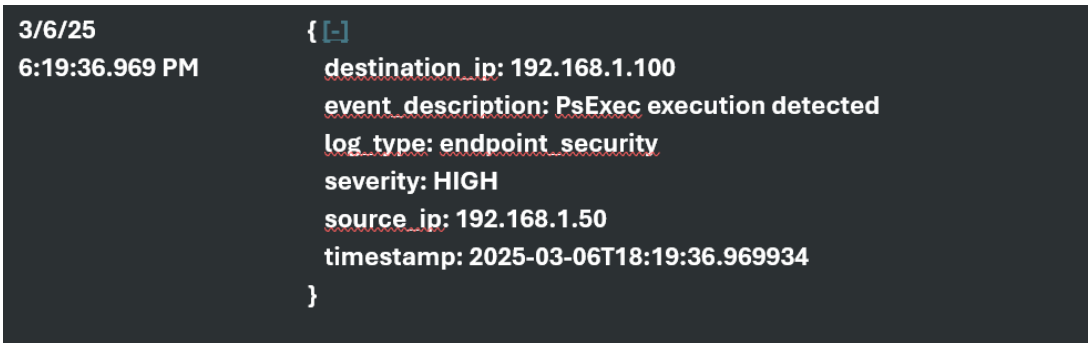

Figure 7: PsExec activity

5.5 Phase 5: Impact (Ransomware)

Evidence: Splunk Query: `sourcetype="endpoint_security" "Ransomware"` **MITRE ATT&CK:** T1486 - Data Encrypted for Impact

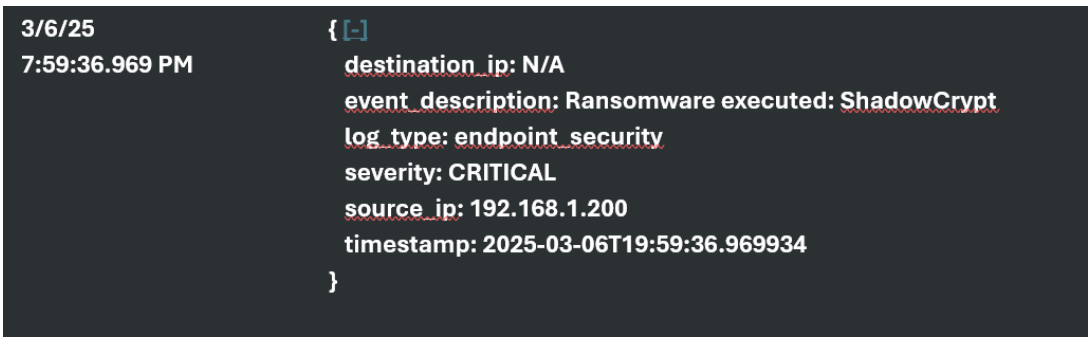

Figure 8: ShadowCrypt ransomware execution

5.6 Phase 6: Persistence

Evidence: Splunk Query: `sourcetype="endpoint_security" "Scheduled Task"` **MITRE ATT&CK:** T1053.005 - Scheduled Task/Job: Scheduled Task

Analysis: Attacker created scheduled task `SystemUpdate` and modified registry key `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` for persistence.

6 Scope and Impact

6.1 Compromised Systems

- **WORKSTATION-01 (192.168.1.10):** Initial compromise point via malicious PDF macro
- **192.168.1.50:** Target of credential attacks and lateral movement
- **192.168.1.100:** Used for scheduled task modification and process injection
- **192.168.1.200:** Final ransomware deployment point

6.2 Data at Risk

- **Customer Financial Records:** Potentially exposed through credential compromise
- **Proprietary Trading Algorithm:** Targeted intellectual property
- **Active Directory Credentials:** Hash values potentially compromised

6.3 Business Impact Assessment

Category	Impact Description
Operational	Critical banking services disruption
Financial	Financial recovery costs and lost revenue
Reputational	Customer confidence drop post-incident

6.4 Indicators of Compromise (IOCs)

- **Files:** Q1_Performance_Review.pdf (SHA-256: a1b2...)
- **Processes:** Suspicious svchost.exe spawns
- **Network:** C2 communications to 185.143.223.47

7 Internal Communications

7.1 Employee Notification Email

To:	All Employees
Subject:	INC250306_5689_Group1 - Critical Security Incident Notification
Body:	Dear Team, We are writing to inform you about a critical security incident detected in our systems on March 6, 2025. Our Security Operations Center (SOC) has identified unauthorized activity linked to a sophisticated cyberattack targeting our network. **Immediate Actions Required:** • **Password Reset:** Change your network password immediately via the Employee Portal • **Email Vigilance:** Report suspicious emails (unexpected attachments or requests) • **Workstation Checks:** Disconnect and report any unusual device behavior **Incident Overview:** • Threat actor gained access via malicious email attachment • No evidence of customer data compromise found • Business operations remain unaffected **Important Reminders:** • Never share credentials or bypass security protocols • Verify sender authenticity before opening attachments • Report anomalies immediately Regards, Apex Financial Security Team **For Immediate Assistance:** IT Security Team Contact: Email: apexitsecurity@gmail.com Phone: 518-898-5796

8 Recommendations

8.1 Immediate Containment Actions

- **Network Segmentation:**
  - Isolate VLANs 10, 20, and 30 completely
  - Implement firewall rules blocking all traffic from compromised subnets
- **Credential Reset:**
  - Force password reset for all domain users (especially privileged accounts)
  - Disable NTLM authentication temporarily
- **Forensic Preservation:**

  - Create disk images of affected systems before restoration
  - Preserve memory dumps from critical servers

8.2 Technical Controls Implementation

- **Endpoint Protection:**
  - Deploy application whitelisting (AppLocker)
  - Enable macro restrictions in Office applications
- **Privileged Access Management:**
  - Implement Microsoft LAPS for local admin passwords
  - Deploy Just-In-Time admin access through PAM solution
- **Detection Enhancements:**
  - Create Splunk alerts for WMI and PsExec usage patterns
  - Implement Windows Event Forwarding for critical authentication events

8.3 Organizational Improvements

- **Security Awareness:**
  - Conduct phishing simulation exercises bi-monthly
  - Implement mandatory training for macro security risks
- **Incident Response:**
  - Develop playbooks for ransomware scenarios
  - Conduct tabletop exercises quarterly
- **Backup Strategy:**
  - Implement 3-2-1 backup rule with offline copies
  - Test restoration procedures monthly

9 Appendix

9.1 Splunk Queries

- Spear-phishing: `sourcetype="email_gateway" "Spear-phishing"`
- Macro execution: `sourcetype="endpoint_security" "malicious macro"`
- Authentication events: `sourcetype="authentication" ("Failed login" OR "Successful login" OR "Pass-the-hash")`
- Lateral movement: `sourcetype="endpoint_security" ("WMI" OR "PsExec")`
- Ransomware: `sourcetype="endpoint_security" "Ransomware"`
- Persistence: `sourcetype="endpoint_security" ("Scheduled Task" OR "Registry key")`

9.2 MITRE ATT&CK Mapping

- T1566.001 - Spearphishing Attachment
- T1204.002 - Malicious File
- T1110 - Brute Force
- T1078 - Valid Accounts
- T1550.002 - Pass the Hash
- T1047 - WMI
- T1569.002 - PsExec

- T1486 - Data Encrypted for Impact
- T1053.005 - Scheduled Tasks

9.3 Screenshot Index

- Figure 1: Spear-phishing email
- Figure 2: Malicious macro execution
- Figure 3: Failed login attempt
- Figure 4: Successful compromise
- Figure 5: Pass-the-hash attack
- Figure 6: WMI execution
- Figure 7: PsExec execution
- Figure 8: Ransomware deployment