SECURITY INCIDENT REPORT

Dai Wok Foods - FIN7 Ransomware Campaign

CONFIDENTIAL - INTERNAL USE ONLY

Incident ID: DWF-2023-001
Report Date: May 20, 2023
Analyst: Cyber Threat Intelligence Team
Severity: CRITICAL
Attribution: FIN7 (Carbanak)

Executive Summary

Dai Wok Foods experienced a sophisticated multi-stage cyberattack orchestrated by the FIN7 threat group, beginning in early April 2023. The attack leveraged social engineering tactics themed around food poisoning complaints to establish initial access, followed by credential harvesting, lateral movement, and preparation for ransomware deployment.

Key Impact Metrics

- **Initial Compromise:** April 2, 2023 (food poisoning phishing campaign)
- **Secondary Wave:** May 6, 2023 (law enforcement warning coincided with ransomware preparation)
- **Targets:** 15 employee roles across restaurant operations
- **Threat Actor:** FIN7 (confirmed through IOC correlation)
- **Attack Vector:** Spear-phishing with weaponized Excel attachments

⚠️ Law Enforcement Alert

A law enforcement agency warned Dai Wok Foods about targeted attacks coinciding with multiple restaurant sites experiencing system lockouts. This indicates an active ransomware campaign in progress.

Threat Actor Attribution

FIN7 (Carbanak) - Confirmed Attribution

Evidence: PowerShell payload hash `c5k3fsys.3bp.ps1` matches known FIN7 indicators

VirusTotal Classification: Trojan.PowerShell/Malgent

Recent Operations: Threat intelligence indicates FIN7 has shifted to ransomware operations

Tactical Evolution: Group has evolved from point-of-sale attacks to full-spectrum ransomware campaigns targeting restaurant chains and hospitality sector

Attack Phases & Timeline

Phase 1: Initial Access (April 2023)

April 2, 2023 - 20:40:54 UTC

Food Poisoning Phishing Campaign: Delphia Evans receives suspicious email with subject "[EXTERNAL] Formal action on food poisoning" from county.county@yahoo.com

April 3, 2023 - 18:04:56 UTC

Lateral Phishing: John Garcia (Logistics Coordinator) receives phishing email containing link to complaints-cityofficialsfood.com

April 3, 2023 - 18:38:38 UTC

Link Activation: John Garcia clicks malicious link from host LVJW-LAPTOP

April 3, 2023 - 18:39:12 UTC

Malware Deployment: large_order.xlsx downloaded to C:\Users\jogarcia\Downloads\
SHA256: b9d3c969135f1e9abe22fd744c691ec1d1bc0853beffe5aed3f8b78b3d738501

April 4, 2023 - 10:14:35 UTC

Security Alert: Employee deevans reports suspicious email to security team

Phase 2: Persistence & Reconnaissance

April 3, 2023 - Post-infection

PowerShell Execution: FIN7 PowerShell payload executed via cmd.exe

```
cmd.exe /c start %SYSTEMROOT%\system32\WindowsPowerShell\v1.0\powershell.exe -noni -nop -exe bypass -f \\share1\Admin$\c5k3fsys.3bp.ps1
```

Phase 3: Ransomware Preparation (May 2023)

May 6, 2023 - 08:33:13 UTC

First Ransomware Campaign Email: Initial contact from threat actor using restaurant@verizon.com

May 12, 2023 - 09:22:48 UTC

Weaponized Attachment: "Local_County_Updates.xlsx" distributed by restaurant@verizon.com (reply-to: miguel_waters@hoisumsupplies.com)

May 12, 2023 - 10:00:55 UTC

Second Compromise: William Perez (Ingredient Procurement) clicks malicious link, enabling further system access

Technical Analysis

Initial Access Vector

- **Social Engineering Theme:** Food poisoning complaints targeting restaurant staff
- **Primary Target:** Delphia Evans (delphia_evans@daiwokfoods.com, ABVJ-MACHINE, IP: 192.168.0.31)
- **Email Volume:** 15 external emails received by Delphia, 64 total emails sent by attackers

Reconnaissance Activities

Threat actors conducted reconnaissance on company structure:

- `http://daiwokfoods.com/search?query=store%20managers`
- `https://daiwokfoods.com/search?query=dai%20wok%20marketing`
- `http://daiwokfoods.com/search?query=customer%20service`

MITRE ATT&CK Techniques

- **T1574.002 - DLL Side-Loading:** Primary technique for malware execution
- **T1566 - Phishing:** Email-based initial access
- **T1059.001 - PowerShell:** Post-exploitation payload execution
- **T1490 - Inhibit System Recovery:** Shadow copy deletion via `vssadmin.exe delete shadows /All /Quiet`

Malware Analysis

```
# FIN7 PowerShell Payload Execution cmd.exe /c start
%SYSTEMROOT%\system32\WindowsPowerShell\v1.0\powershell.exe -noni -nop -exe bypass -f
\\share1\Admin$\c5k3fsys.3bp.ps1 # Shadow Copy Deletion (Ransomware Preparation)
vssadmin.exe delete shadows /All /Quiet # Associated Utilities cy.exe # Custom FIN7 utility
notepad.exe # Process masquerading winutils.dll # Malicious DLL component
```

Indicators of Compromise (IOCs)

Type	Indicator	Description	Geolocation
IP Address	179.58.169.157	Malicious domain hosting	Bolivia
IP Address	2.20.114.29	Credential stuffing attempts	Italy
Email	county.county@yahoo.com	Initial phishing sender	-
Email	official@verizon.com	Suspicious email address	-
Email	restaurant@verizon.com	Ransomware campaign sender	-
Email	miguel_waters@hoisumsupplies.com	Reply-to address	-
File Hash	b9d3c969135f1e9abe22fd744c691ec1d1bc0853beffe5aed3f8b78b3d738501	large_order.xlsx (malicious)	-
File	c5k3fsys.3bp.ps1	FIN7 PowerShell payload	-
File	Local_County_Updates.xlsx	Ransomware campaign attachment	-

Malicious Domains (12 Total)

- complaints-lawoffice.business
- foodadministration-legal-services.com
- legal-services-complaints.business
- complaints-cityofficialsfood.business
- legal-services-lawoffice.com
- foodadministration-legal-services.business
- complaints-cityofficialsfood.com
- foodadministration-cityofficialsfood.business
- foodadministrationlegal-services.business
- cityofficialsfoodlawoffice.com
- foodadministrationcityofficialsfood.business
- foodadministrationcomplaints.business

Ransomware Infrastructure

- human-resources-operations.hk
- operationslegal-services.hk

- operations-management.hk

Compromised Personnel

Delphia Evans (deevans)

Email: delphia_evans@daiwokfoods.com
Role: Restaurant Staff
Hostname: ABVJ-MACHINE
IP Address: 192.168.0.31
Status: Initial phishing victim, reported suspicious activity

John Garcia

Role: Logistics Coordinator
Hostname: LVJW-LAPTOP
Status: Clicked malicious link, downloaded weaponized Excel file
Compromise: Credential stuffing attempts from 2.20.114.29 (Italy)

William Perez

Role: Ingredient Procurement
Status: Secondary wave victim, clicked ransomware campaign link

Attack Impact Assessment

Organizational Impact

- **15 Employee Roles Targeted:** Cross-functional targeting across restaurant operations
- **Multiple Restaurant Sites:** Law enforcement reports system lockouts across locations
- **Operational Disruption:** Potential for widespread ransomware deployment

Data at Risk

- Employee credentials and authentication systems
- Operational data and logistics information
- Financial records and procurement data
- Customer information and payment systems

Business Continuity Threats

- Point-of-sale system encryption
- Supply chain management disruption
- Customer service interruption
- Brand reputation damage

Immediate Response Actions

Critical (0-4 hours)

- **Isolation:** Immediately isolate ABVJ-MACHINE, LVJW-LAPTOP, and all systems accessed by William Perez
- **Account Security:** Reset passwords for deevans, John Garcia, and William Perez accounts
- **Network Blocking:** Block all IOC IP addresses and domains at network perimeter
- **Shadow Copy Protection:** Prevent vssadmin shadow deletion on critical systems
- **Backup Verification:** Immediately verify backup integrity and isolate offline backups

High Priority (4-24 hours)

- **Email Quarantine:** Search and quarantine all emails from suspicious senders
- **PowerShell Monitoring:** Implement enhanced monitoring for PowerShell execution
- **Credential Analysis:** Analyze authentication logs for lateral movement
- **System Imaging:** Create forensic images of compromised systems

Medium Priority (1-7 days)

- **FIN7 IOC Hunting:** Comprehensive search for additional FIN7 indicators
- **Email Security Enhancement:** Implement advanced attachment sandboxing
- **Staff Training:** Emergency security awareness training on food poisoning scams
- **DLL Side-Loading Prevention:** Implement application whitelisting

Long-term Security Improvements

Email Security

- Deploy advanced email security with behavioral analysis
- Implement DMARC, SPF, and DKIM authentication
- Create specific rules for food safety/legal themed emails

Endpoint Protection

- Deploy EDR with FIN7-specific detection rules
- Implement PowerShell execution monitoring
- Configure application whitelisting for DLL side-loading prevention

Network Security

- Implement network segmentation between restaurant locations
- Deploy DNS filtering for malicious domain blocking
- Enhance monitoring for lateral movement patterns

Backup Strategy

- Implement immutable backup solutions
- Create air-gapped backup systems
- Regular backup restoration testing

Detection Queries

```
// FIN7 PowerShell Detection ProcessEvents | where process_commandline has "powershell.exe"
and process_commandline has "-noni -nop -exe bypass" | project timestamp, hostname,
process_commandline // DLL Side-Loading Detection (T1574.002) ProcessEvents | where
process_name in ("cy.exe", "notepad.exe") and parent_process != "explorer.exe" | project
timestamp, hostname, process_name, parent_process // Shadow Copy Deletion Detection
ProcessEvents | where process_commandline has "vssadmin.exe delete shadows" | project
timestamp, hostname, process_commandline, user_account // Malicious Domain Detection
NetworkEvents | where domain has_any ("complaints-lawoffice.business", "foodadministration-
legal-services.com", "complaints-cityofficialsfood.com") | project timestamp, hostname,
domain, dest_ip
```

Lessons Learned

- **Social Engineering Sophistication:** FIN7 leveraged industry-specific themes (food poisoning) to increase credibility
- **Multi-Phase Campaign:** Attack spanned multiple months with distinct phases
- **Employee Reporting:** Delphia Evans' security report was crucial for early detection
- **Law Enforcement Coordination:** External threat intelligence provided critical attack context
- **Ransomware Evolution:** Confirmed FIN7's shift from POS attacks to ransomware operations

Conclusion

The Dai Wok Foods incident represents a sophisticated, multi-stage campaign by the FIN7 threat group targeting the restaurant industry. The attack demonstrates advanced social engineering techniques, persistent reconnaissance, and preparation for ransomware deployment. The identification of FIN7 attribution through PowerShell payload analysis and the correlation with law enforcement warnings indicates an active, ongoing campaign against the hospitality sector.

Immediate containment and long-term security improvements are critical to prevent full ransomware deployment and protect against future FIN7 campaigns. The organization's security awareness program should be enhanced with specific training on industry-targeted social engineering attacks.