Sophisticated Attack Chain Leads to Data Exfiltration at Major Corporation

Executive Summary

A sophisticated cyber attack chain was detected between October and November 2024, involving multiple stages from initial compromise through lateral movement to eventual data exfiltration. The attack began with a targeted phishing campaign and culminated in the unauthorized creation of cloud infrastructure used for data theft.

On October 15, 2024, the attack commenced with a sophisticated phishing campaign targeting an employee named Dalia Miles. The attack leveraged a malicious email masquerading as a "SAM.gov Tutorial" with an early bird discount offer. The email contained a suspicious PNG file loaded from dotsply.com, which led to credential harvesting when the victim accessed the malicious URL.

Attack Progression

Phase 1: Reconnaissance and Initial Access

- The attacker successfully harvested corporate credentials through the phishing site
- Security tools detected password exposure to non-corporate sites
- Initial foothold was established on the victim's workstation (DALIAPCW11)

Phase 2: Discovery and Lateral Movement

- On October 24, the attacker deployed LogMeIn software to enumerate security products
- A DLL side-loading technique was observed using sc.exe
- The LanSweeper service was exploited to perform SMB-based network discovery
- Successful lateral movement was achieved to multiple systems including:
    - POSTGRESRV (Database Server)
    - User workstations (STEV-LAPTOP, KEREN-LAPTOP)

Phase 3: Command and Control

By November 4, the compromised POSTGRESRV was observed making suspicious DNS requests to a domain associated with ShadowPad malware, indicating the establishment of command and control infrastructure.

Phase 4: Data Exfiltration

The attack culminated in two major data exfiltration attempts:

1. Large-scale data transfer from POSTGRESRV to a newly created EC2 instance via SSH
2. Unauthorized EC2 instance creation using compromised credentials

Key Behavioral Detections

1. User Entity Behavioral Analytics (UEBA)

The XDR platform demonstrated sophisticated user behavior analytics through multiple detections:

Anomalous Login Pattern Detection

- Alert: "Possible lateral movement attempt"
- Behavioral Indicator: The system detected unusual concurrent login patterns where administrator credentials were used to access multiple machines (POSTGRESRV and others) while legitimate users (karen.newman, steve.maden) were actively logged in
- Significance: This detection shows XDR's ability to baseline normal user access patterns and flag deviations

Password Security Monitoring

- Alert: "Corporate password exposure"
- Behavioral Indicator: Real-time detection of corporate credential exposure to non-corporate websites
- Context: The system correlated the user (Dalia.Miles), their workstation (DALIAPCW11), and the suspicious URL in real-time

2. Process Behavior Analysis

Security Product Discovery

- Alert: Detection of LogMeIn process discovering security products
- Behavioral Indicator: WMI query patterns typical of security product enumeration
- Significance: Shows XDR's ability to detect reconnaissance activities based on process behavior rather than just signatures

DLL Side-Loading Detection

- Alert: "behavioral.win.dllsideloading.p"
- Process Monitored: sc.exe
- Behavioral Indicator: Unusual DLL loading patterns associated with the legitimate Windows service controller
- Advanced Detection: Correlation between process behavior and user context (Dalia.Miles logged on)

3. Network Behavior Analytics

SMB Traffic Analysis

- Alert: Unusual SMB connectivity pattern
- Behavioral Indicator: The lansweeperservice.exe process showing abnormal network share enumeration
- Context-Aware Detection: System noted the absence of logged-in users during this activity

- Correlation: Connected this behavior to the larger lateral movement pattern

Data Exfiltration Detection

- Alert: Large data upload prevention
- Behavioral Analysis: Detected abnormal data transfer volumes over SSH
- Context: Correlated the source (POSTGRESRV) with the unauthorized EC2 instance
- Prevention: Active blocking of the exfiltration attempt

4. Cloud Integration Behavioral Detection

Cloud Resource Creation Analysis

- Alert: Suspicious EC2 instance creation
- Behavioral Indicator: Unauthorized use of compromised credentials for cloud resource provisioning
- Integration: Shows XDR's ability to correlate on-premise activity with cloud platform actions

Advanced XDR Capabilities Demonstrated

1. Cross-Stack Correlation

- Integration of endpoint, network, cloud, and identity telemetry
- Ability to track attack progression across different security domains
- Correlation of seemingly unrelated events into a coherent attack chain

2. Context-Aware Detection

- User context integration with process behavior
- Authentication pattern analysis
- Asset relationship mapping

3. Preventive Controls

- Active prevention of data exfiltration
- Integration with cloud security controls
- Real-time response to detected threats

Detection Engineering Insights

1. Detection Stack Coverage

- MITRE ATT&CK alignment across multiple tactics
- Coverage of both Windows and cloud infrastructure
- Integration of multiple data sources for comprehensive visibility

2. False Positive Mitigation

- Use of context to validate alerts
- Correlation of multiple behavioral indicators

- Integration of user, process, and network context

3. Response Automation Opportunities

- Automated response to suspected data exfiltration
- Cloud resource provisioning controls
- Created Indicators of compromise to prevent further usage
- Spread the indicators to all the relevant security tools available
- Network isolation capabilities

Technical Indicators

Malicious Infrastructure

- C2 Domain: kmjugkknhncmflkubs.gtmpmkkwenmsfxjrkmcslpctcnimm.jnl.time.dsqurey.com
- Phishing URL: https://dotsply.com/pixel/fetch
- Compromised Asset: EC2-10.72.10.16

Affected Systems

- Primary Victim Workstation: DALIAPCW11
- Compromised SQL Server: POSTGRESRV
- Additional Compromised Systems: STEV-LAPTOP, KEREN-LAPTOP

MITRE ATT&CK Techniques Observed

- TA0042: Resource Development
- T1518: Software Discovery
- TA0001: Initial Access
- TA0011: Command and Control
- T1566: Phishing
- T1021: Remote Services
- T1135: Network Share Discovery
- T1574: Hijack Execution Flow
- TA0010: Exfiltration

Conclusion

This incident demonstrates a well-orchestrated attack chain that progressed from initial phishing to data exfiltration over approximately one month. The attackers showed sophistication in their use of legitimate tools and services to avoid detection while maintaining persistence and expanding their foothold within the network.