DFIR Report

Team Name: FluffyBird

October 3, 2025

1 Executive Summary

Date of Report: October 3, 2025
Reported By: Vivek Veman Karnati, Manideep Reddy Kota
Team Name: FluffyBird

Incident Summary:
WidgetCo experienced a coordinated phishing campaign that led to the compromise of two employee accounts: widgetco\jhipps and widgetco\jsmith. Both attacks followed a multi-stage kill chain involving phishing, malware execution, persistence, privilege escalation, lateral movement, and data exfiltration. Sensitive corporate and personal data was exfiltrated to cloud services (Dropbox, GitHub), followed by the deployment of ransom notes from "Unit Sparky."

2 Incident Details

Incident Name/Title: WidgetCo Phishing and Data Exfiltration
Date & Time of Detection:

- jhipps: 2024-06-15 10:15:05Z
- jsmith: 2024-06-15 10:15:10Z

Detection Method: UBA anomaly + SIEM correlation across Email Gateway, VPN, DNS, Windows Security, and CASB logs.
Systems Affected: WIN-HOST01, FILESERVER01, MAIL-GW01, WIN-HOST11
Users Involved: widgetco\jhipps, widgetco\jsmith

Indicators of Compromise (IOCs):

- Domains: widgettco.acme

- Malicious URLs:
  - `http://widgettco.acme/home/newsite/download/`
  - `http://widgettco.acme/home/newsite/sseddsd.ps1/`
- Malicious Files:
  - `C:\Users\jhipps\AppData\Local\Temp\lslkd9.dll`
  - `C:\Users\jhipps\AppData\Local\Temp\update.exe`
- Persistence:
  - Registry Run Key: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\updateServ`
  - Scheduled Task: `\Microsoft\Windows\UpdateCheck`
- Malicious IP: `66.220.242.222` (attacker's C2)
- Exfiltration:
  - `https://gist.github.com/...`
  - `https://dropbox.com/api/2/upload/sdhiien`

—

3 Timeline of Events

Compromised Account: jhipps (WIN-HOST01)

Timestamp (UTC)	Event / Action Description
2024-06-15 10:15:00	Phishing email delivered (Direct Deposit scam)
2024-06-15 10:15:05	Unusual login for `jhipps` from foreign IP
2024-06-15 10:15:08	Outlook launched, user interacts with malicious email
2024-06-15 10:15:14	DNS request to typo domain `widgettco.acme`
2024-06-15 10:15:30	DLL executed via `rundll32.exe`
2024-06-15 10:15:35	PowerShell with encoded command runs
2024-06-15 10:15:36	PowerShell downloads second-stage script
2024-06-15 10:15:45	Persistence via registry + scheduled task
2024-06-15 10:15:50	`update.exe` dropped to disk
2024-06-15 10:16:00	VPN login from foreign IP
2024-06-15 10:16:05	Lateral movement to FILESERVER01 (RDP session)
2024-06-15 10:16:30	User added to Domain Admins group
2024-06-15 10:16:50	Data exfiltration to GitHub/Dropbox
2024-06-15 10:16:55	`patient_records.xlsx` accessed and exfiltrated
2024-06-15 10:17:00	Ransom note received from "Unit Sparky"

Compromised Account: jsmith (WIN-HOST11)

Timestamp (UTC)	Event / Action Description
2024-06-15 10:15:05	Phishing email delivered to `jsmith@widgetco.acme`
2024-06-15 10:15:10	VPN connection from suspicious IP (10.1.1.45) using jsmith credentials
2024-06-15 10:15:14	DNS request for malicious domain `widgettco.acme`
2024-06-15 10:15:20	PowerShell downloads and executes payload from `widgettco.acme`
2024-06-15 10:15:30	Registry key modified for persistence (`updateService`)
2024-06-15 10:15:35	Scheduled task created: `\Microsoft\Windows\UpdateCheck`
2024-06-15 10:15:45	RDP session initiated to `66.220.242.222`
2024-06-15 10:15:55	Sensitive files accessed by jsmith's account
2024-06-15 10:16:05	Data exfiltrated via Dropbox POST request
2024-06-15 10:16:15	PowerShell writes `ransom_note.txt` to disk

4 Analysis

Root Cause: Phishing emails successfully bypassed defenses and were clicked by users.
Attack Vector: Email phishing via typo-squatted domain.
Attacker Techniques: DLL injection, PowerShell, persistence via registry and tasks, VPN access, RDP lateral movement, cloud exfiltration.
Evidence Collected: Email artifacts, malicious DLL/EXE, PowerShell logs, persistence keys, ransom notes.

5 Impact Assessment

Data Accessed/Exfiltrated:

- `patient_records.xlsx` (PII/PHI)
- Proprietary models and intellectual property

Business Impact:

- Confirmed breach of sensitive personal and business data
- Regulatory risk (HIPAA, GDPR)
- Ransom demand with risk of data leak

—

6 Mitigation & Response

Actions Taken (Proposed):

- Disabled accounts: `jhipps`, `jsmith`
- Isolated WIN-HOST01 and WIN-HOST11
- Blocked malicious IP 66.220.242.222 and domains widgettco.acme

Remediation Steps:

- Remove the malicious registry key, scheduled task, and any malicious files downloaded from all compromised hosts.
- Remove persistence artifacts
- Re-image compromised endpoints
- Force a password reset for all user accounts, especially all Domain Admin accounts.
- Enforce MFA for VPN access

Control Gaps & Recommendations:

- Enhance phishing detection and user training
- Strengthen SIEM rules for VPN anomalies and cloud exfiltration
- Segment network to restrict lateral RDP movement

7 Appendices

Log Files Reviewed: Email Gateway, VPN, DNS, Windows Security, CASB
Screenshots/Diagrams: Recommended attack timeline and network flow diagram
Tools Referenced: SIEM, EDR, Volatility, Sysinternals, forensic toolkit