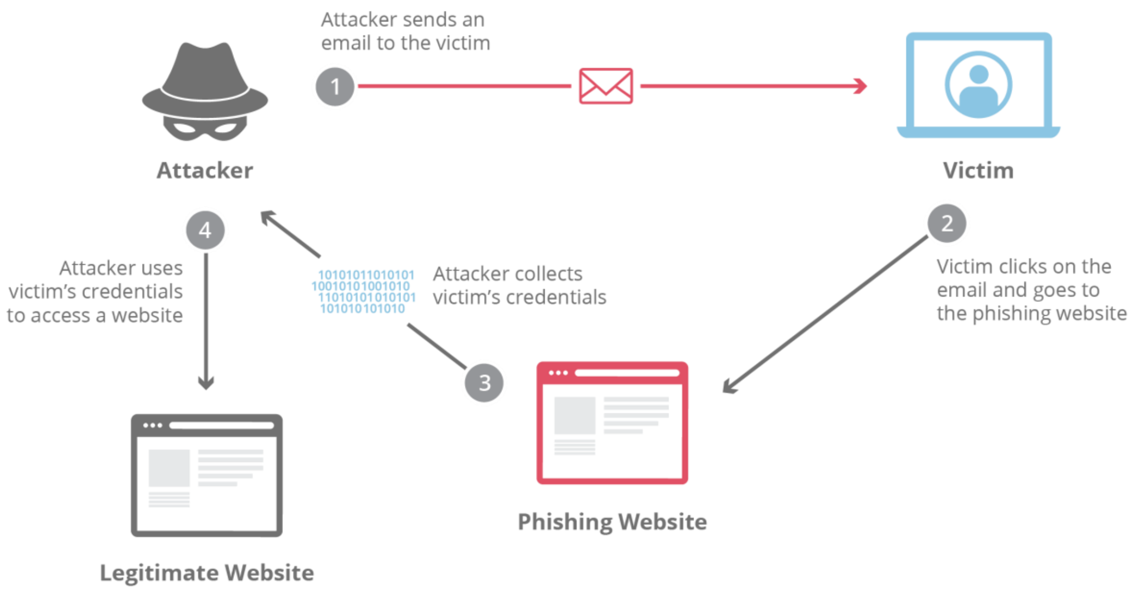
Team Fluffy Bird

Manideep Reddy Kota
Vivek Veman

What is phishing?

- “Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other important data in order to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similar to how a fisherman uses bait to catch a fish.



Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim’s credentials to access a website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim’s credentials
3
Phishing Website
Legitimate Website

EMAIL FILE 1 : Direct Deposit

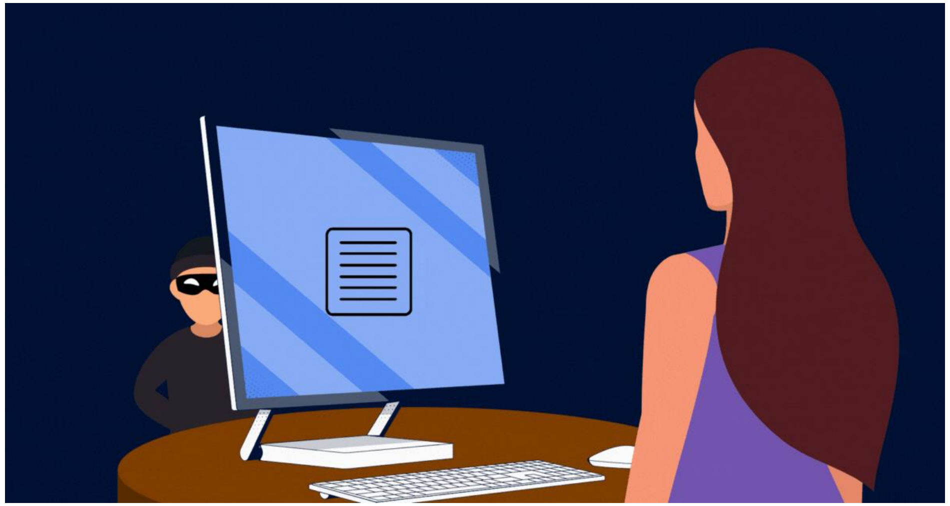
Recipient: J Smith (`jsmith@widgetco.acme`)

Sender: "WidgetCo — a division of Acme" `<hr@widgettco.acme>` (note the subtle misspelling: `widgettco` instead of `widgetco`)

Subject: *Action Required: Update Your Direct Deposit Information*

Message:

- Claims the employee's **direct deposit info is missing/outdated**.
- Urges them to update it before **15 June 2024**.
- Provides a link: `https://widgettco.acme/verify?uid=STU-20240612-WDG001`.
- Warns paycheck may be delayed if not updated.



Email File 2 : Suspicious Email

Recipient: J Hipps (jhipps@widgetco.acme)

Sender: "WidgetCo — a division of Acme" <hr@widgettco.acme>

Subject: *Action Required: Update Your Direct Deposit Information*

Date: 12 June 2024

Message Summary:

- Alerts employee that their **direct deposit information is missing or outdated**.
- Directs them to **update details immediately** to ensure payroll disbursement.
- Sets a **deadline of 15 June 2024**.
- Provides a link: https://widgettco.acme/verify?uid=STU-20240612-WDG001.
- Suggests contacting the “Payroll office via HR portal” if the message was received in error.

Summary of mails & Our Conclusion

These emails are part of a **phishing campaign** targeting WidgetCo employees. The attackers attempt to harvest sensitive payroll/banking details by:

- Using a **lookalike sender domain**.
- Creating **urgency** with a payroll deadline.
- Embedding a **malicious verification link**.

- Why Phishing?
  spoofed domain (`widgettco.acme` instead of `widgetco.acme`).
  Similar content , asks to update using links .
  Language: Delivered as multipart (plain text + HTML) to appear professional and legitimate.

Plan of Action

- Incident Summary
- Detection and Timeline of Events(Log Exploration)
- Impact Assessment
- Root Cause Analysis
- Immediate Containment Actions
- Remediation and Recovery Steps
- Preventive Measures / Long-Term Improvements

Log Exploration

- Normal Activities/ Expected Activities:
  - KerberosAudit entries: Many users (jdoe, zking, mbrown, ljones, etc.) are authenticating to domain controller AAA-01 (10.1.3.11). That’s expected.
  - O365 traffic: Users like fthomas, jhipps, ljones, asmith, etc. running OUTLOOK.EXE to o365.mail.widgetco.acme. Looks like standard email use.
  - WebProxy/Firewall entries: Users browsing legitimate sites (finance, weather, sports news, Yahoo, etc.). These look normal
  - WindowsSecurity events like winlogon.exe, chrome.exe, excel.exe starting up are usually normal user activity.

Suspicious Activities or Flags

We Managed to figure some activities , which weren't common and marked as flags.

a)Remote Server login
b) PowerShell execution to download files

c) Modifying credential's using registry
d)Execute DLL file
e) Adding user to Domain Admins group

Activity 1: Encoded Powershell

- Timestamp: 2024-06-15 10:15:12Z
- Execution Made: Powershell command
- User Affected : Local System
- Alert : Triggered
- Actions Made: The Encoded Command was in base64 , which when decoded translates to query that tries to query Local Security Authority Server Service (LSASS) Memory
  - What is LSASS protection?
    - SASS protection is a Windows security feature that protects the Local Security Authority Subsystem Service (LSASS) process from unauthorized access and memory dumps, which attackers use to steal credentials

- Conclusion : Possibility Of Credential Dumping Via LSASS querying.

Activity 2 : Remote Code Retrival

- Timestamp: 2024-06-15 10:15:20Z
- Execution Attempted: Powershell Command
- User Affected: JSmith
- Alert Type triggered:Windows
- Actions Made: Downloads content from http://widgettco.acme/home/newsite/download/. This is remote code retrieval.
  - What is remote code retrival:
    - it is a tactic that malicious actors use to achieve remote code execution (RCE). RCE is a critical cyberattack that allows an attacker to run malicious code on a target system from a remote location.

    Conclusion : Possible try to attempted RCE(Remote Code Execution)

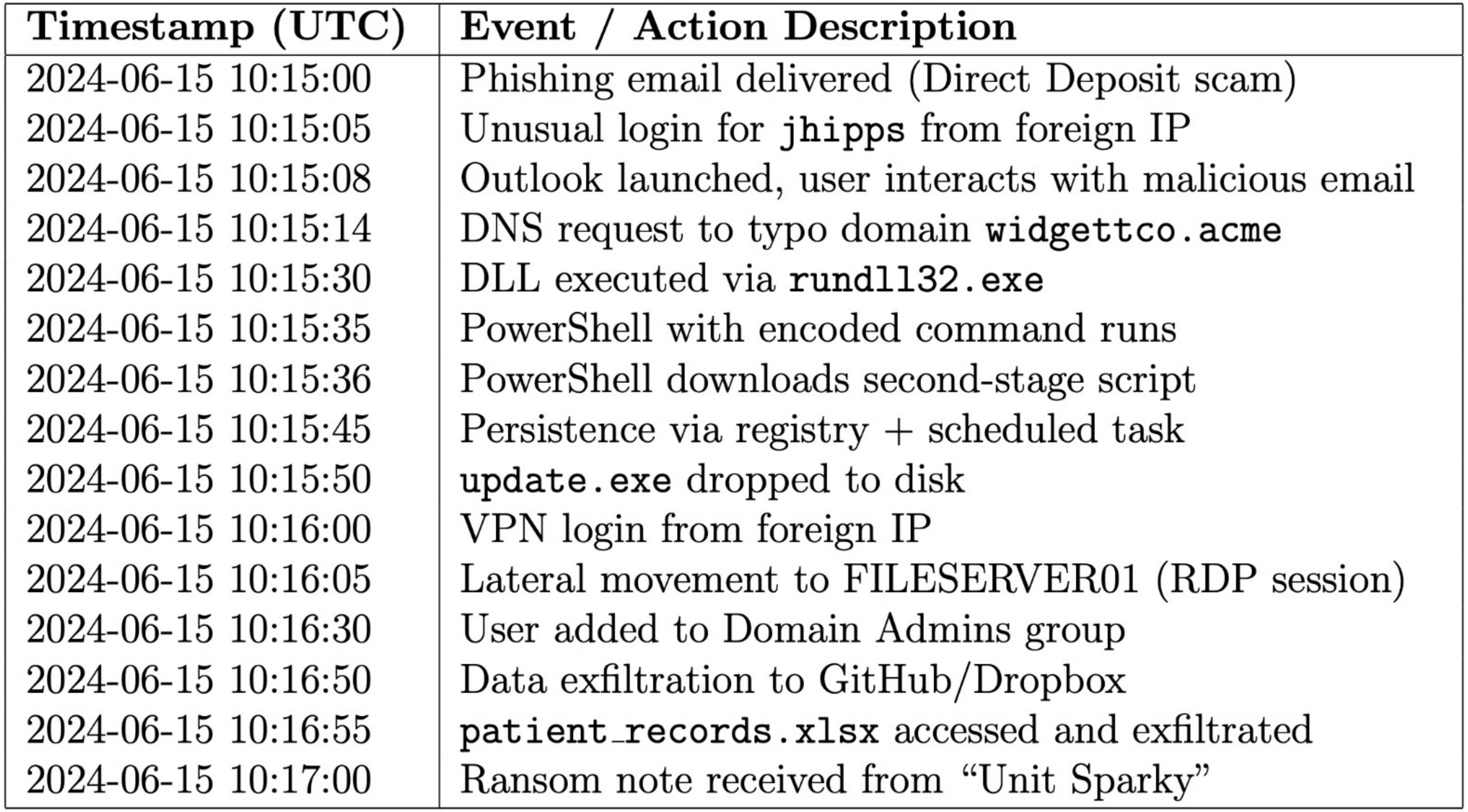
Activity 3 :Lateral Movement/Recon

- Timestamp: 2024-06-15 10:15:35Z
- Execution Made: Powershell command
- User Affected : jhipps
- Alert Type Triggered : Windows
- Actions Made: The Encoded powershell command which tried enumerate logged-in users and AD computers, and list shares.
    - What is Lateral movement?
        - Lateral movement refers to the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets.
- Conclusion : Possibility Of Access to Sensitive Information.

Activity 4 :

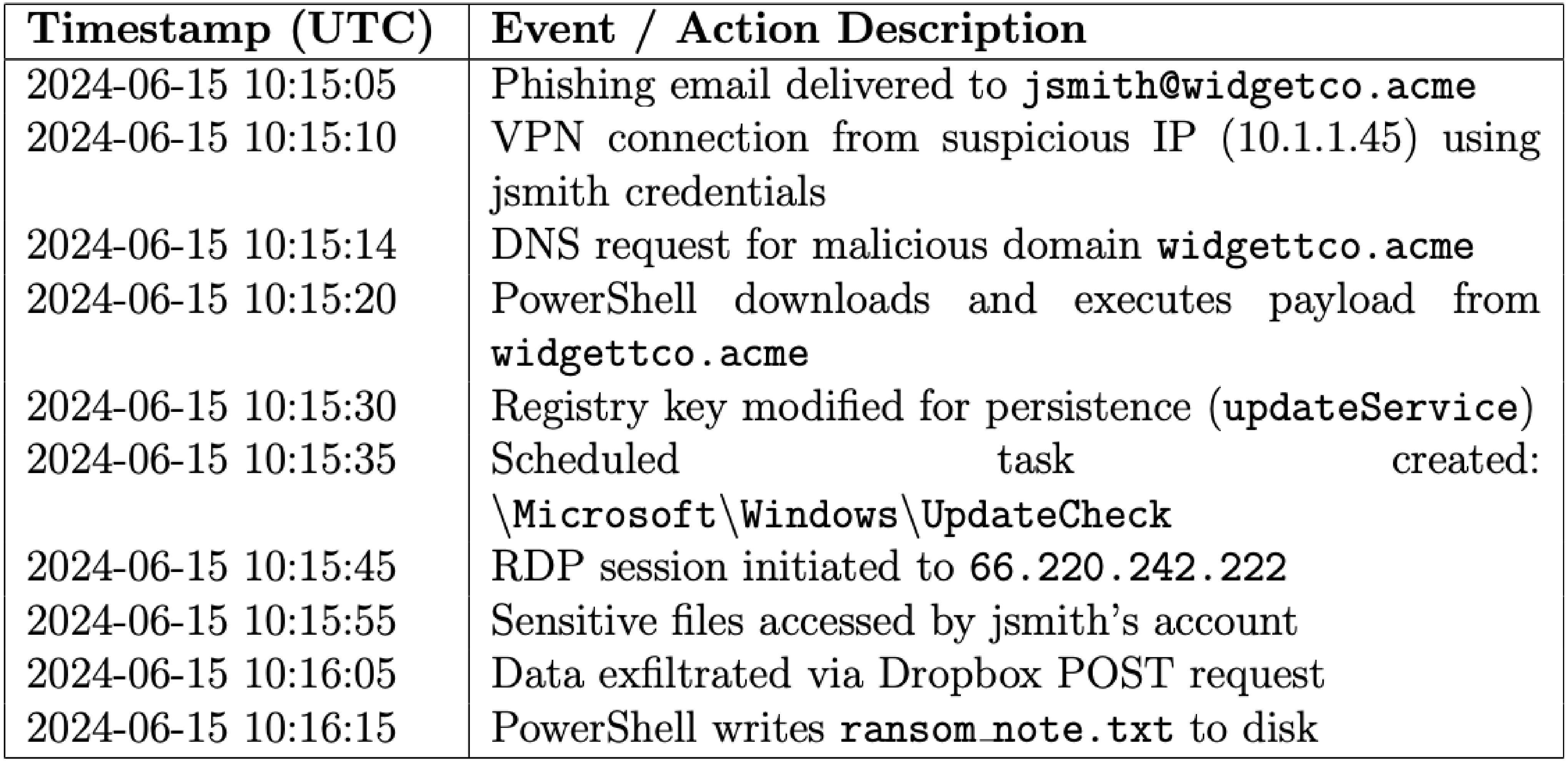
- Timestamp: 2024-06-15 10:15:36Z
- Execution Made: Powershell payload delivered
- User Affected : jhipps
- Alert : Triggered
- Actions Made: The Encoded Command was responsible for downloading and executing a Powershell payload.
  - What is Powershell Payload?
    - A PowerShell payload is malicious code or commands executed through the PowerShell framework on a Windows system.
- Conclusion : Possibility Of Sytem being affected to by the payload.

Timeline for 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"

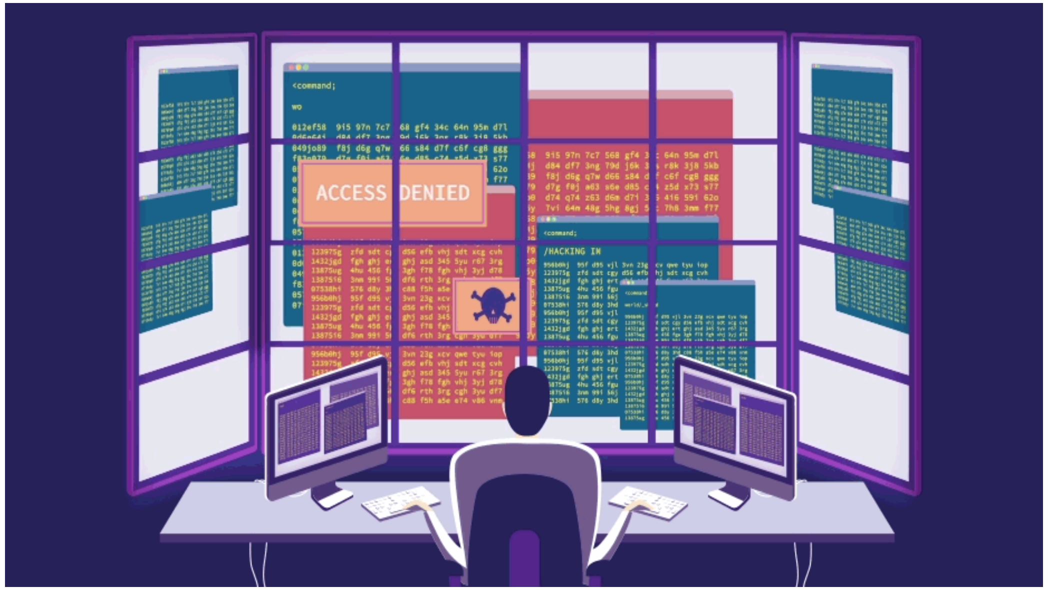
Timeline for Compromised Account: Jsmith(WIN-HOST1`)



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

Impacted Computers

- **WIN-HOST01** (compromised via account **jhipps**)
  - Malicious DLL executed (`lslkd9.dll`) via `rundll32.exe`
  - Malicious EXE dropped (`update.exe`) in `%LocalTemp%`
  - Registry run key set: `HKCU\...\Run\updateService`
  - Scheduled Task created (`\Microsoft\Windows\updateTask`)
  - Ransom note created (`ransom_note.txt`)
  - Evidence of outbound connections to attacker C2 (`66.220.242.222`) and cloud upload activity
- **WIN-HOST11** (compromised via account **jsmith**)
  - PowerShell payload execution and persistence (`updateService`, `UpdateCheck` scheduled task)
  - Ransom note written to disk
  - Data exfiltration observed to Dropbox / GitHub Gist
- **FILESERVER01** (accessed during lateral movement)
  - SMB access from compromised host(s): sensitive shares read
- **MAIL-GW / O365 / VPN / CASB** (infrastructure components used or showing evidence)
  - Mail Gateway: phishing delivery
  - VPN: suspicious external login(s) using compromised credentials
  - CASB/WebProxy: cloud upload events (Dropbox/Gist)



Impacted Users

Widgetco\jhipps — *Primary compromise on WIN-HOST01*

- Received phishing email → clicked link to `widgettco.acme`
- Outlook/PowerShell execution chain observed (DLL → PowerShell → second-stage payload)
- VPN login from foreign / suspicious IP observed (external access)
- Performed file access on FILESERVER01 (SMB) and uploaded data to cloud services
- Account used in privilege changes (evidence of Domain Admin group add in logs)

Widgetco\jsmith — *Primary compromise on WIN-HOST11*

- Phishing email delivered & clicked → PowerShell download & execute
- Persistence (registry/run + scheduled task) and RDP connections observed
- Sensitive files accessed and exfiltrated to Dropbox/Gist
- **Other users**
- No direct full compromise observed, but at risk due to lateral movement & elevated admin account changes

Impacted Files

- **Accessed / Likely Exfiltrated:**

`patient_records.xlsx` — sensitive PII/PHI (CASB confirms read & upload activity)

`proprietary_model.bin` — IP / proprietary model file (access logged)

- **Malicious / Persistence Artifacts:**
- `C:\Users\jhipps\AppData\Local\Temp\lslkd9.dll` (malicious DLL executed)
- `C:\Users\jhipps\AppData\Local\Temp\update.exe` (malicious binary)
- Registry: `HKCU\...\Run\updateService`
- Scheduled tasks: `\Microsoft\Windows\updateTask` / `\Microsoft\Windows\UpdateCheck`

- **Ransomware / Extortion Artifacts:**
- `ransom_note.txt` written to compromised hosts (WIN-HOST01 / WIN-HOST11)

- **Exfil Destinations (evidence):**
- `https://dropbox.com/api/2/files/upload/...` (POSTs observed)
- `https://gist.github.com/...` (uploads/POSTs observed)

Mitigation & Response(ACTION ITEMS)

Account Controls

- Disabled compromised accounts: `widgetco\jhipps`, `widgetco\jsmith`
- Forced password resets & implemented MFA on all VPN/remote access

Host Isolation & Cleanup

- Isolated **WIN-HOST01**, **WIN-HOST11**, **FILESERVER01** from the network
- Deleted malicious registry keys & scheduled tasks (`updateService`, `UpdateCheck`, `updateTask`)
- Re-imaged compromised systems from clean backups

Network & C2 Blocking

- Blocked malicious IP/domain: `66.220.242.222`, `widgettco.acme`
- Temporarily restricted outbound traffic to Dropbox & GitHub Gist

Mitigation & Response(ACTION ITEMS)

Monitoring & SIEM Improvements

- Enhanced rules for unusual VPN logins, encoded PowerShell, and cloud uploads
- Improved CASB monitoring for shadow IT and unsanctioned cloud storage

User Awareness & Hardening

- Conducted phishing awareness training for employees
- Strengthened email filtering to detect lookalike domains