MALICIOUS 89/100

Phishing-delivered encoded PowerShell on finance workstation FIN-WKS-0113 beaconed to confirmed C2 203.0.113.199 and set scheduled-task persistence before Falcon containment - keep host contained, rotate user3 credentials, purge campaign tenant-wide.

HOST FIN-WKS-0113 (Windows 11 Pro 23H2, Falcon sensor 7.24, Finance VLAN) USER **user3@example.com**

TIME **2026-07-09T08:17:52Z**

MITRE **T1566.001 (Spearphishing Attachment), T1059.001 (PowerShell), T1071.001 (Web Protocols C2), T1053.005 (Scheduled Task), T1003.001 (LSASS Memory - attempted, blocked)**

SEVERITY HIGH

Org: ORG001 · Alert ORG001-CRWD-1 · Generated 2026-07-09T08:52:36Z

EXECUTIVE SUMMARY

This alert is a true positive phishing compromise of `FIN-WKS-0113`, a Finance VLAN workstation. At 08:14Z, `user3@example.com` opened `Invoice_Q2_Overdue.zip`, a password-protected archive from a lookalike vendor domain that the email gateway delivered as clean because the password in the message body prevented detonation. The extracted shortcut launched `powershell.exe -nop -w hidden -enc`, which downloaded the unsigned loader `wupdcore.dll` from `203.0.113.199` - flagged by 34/93 VirusTotal engines and tied to 11 recently registered invoice-themed lookalike domains. The loader beaconed for roughly four minutes, created the scheduled task `\Microsoft\Windows\MsUpdCore`, and attempted an LSASS handle open (blocked by Falcon) before the process tree was terminated at 08:21:47Z and the host network-contained at 08:26:10Z. The IOC sweep across 412 sensored hosts returned zero additional matches and two other recipients of the same campaign did not execute the attachment, so blast radius is currently one host and one user. Credential reset and session revocation for `user3@example.com`, persistence removal and reimage of the host, and tenant-wide IOC blocking and message purge are required.

ALERT DETAILS

CREATED AT	2026-07-09T08:17:52Z
HOST	`FIN-WKS-0113` (Windows 11 Pro 23H2, Falcon sensor 7.24, Finance VLAN)
USER	`user3@example.com` (Finance; standard user, no admin roles)
SEVERITY	HIGH (Falcon: Critical; behavioral + ML detections)
MITRE	T1566.001 (Spearphishing Attachment), T1059.001 (PowerShell), T1071.001 (Web Protocols C2), T1053.005 (Scheduled Task), T1003.001 (LSASS Memory - attempted, blocked)
PATTERN	Shortcut-spawned hidden encoded PowerShell downloading and side-loading an unsigned DLL within 3 minutes of a phishing attachment open

PROCESS CHAIN	`explorer.exe` → `Invoice_Q2_Overdue.lnk` → `powershell.exe -nop -w hidden -enc JABzAD0A...` → `rundll32.exe wupdcore.dll`
DESTINATION	`203.0.113.199:443` (ASN 64502 - Example Hosting LLC, US datacenter; 34/93 VirusTotal)
DROPPED FILE	`C:\Users\user3\AppData\Roaming\msupd\wupdcore.dll` (SHA256 `4f2a...e91b`, unsigned, first seen in the wild 2026-07-07)
PERSISTENCE	Scheduled task `\Microsoft\Windows\MsUpdCore` (logon trigger), created 08:16:48Z - on disk pending remediation
CONTAINMENT	Process tree terminated by Falcon 08:21:47Z; host network-contained 08:26:10Z; RTR triage collection queued
FALCON DETECTION	ldt:9f3a...c210:12884901889 (composite: SuspiciousPowerShellEncodedCommand, MLCriticalFileWritten, CredentialAccessBlocked)
EMAIL CAMPAIGN	Delivered 08:09:14Z from lookalike vendor domain to 3 finance mailboxes; password-protected archive with password in message body (gateway detonation bypass)
PRIOR CASES	2 related cases in the past 14 days from the same lookalike-domain campaign infrastructure (ORG001-M365-27 credential-phish attempt, ORG001-CRWD-0871 blocked downloader) - first successful execution in this org

INVESTIGATION QUESTIONS

What process chain triggered the detection, and can it be explained as legitimate activity?

• The chain is a phishing execution pattern with no legitimate explanation: a user-opened shortcut from an emailed archive spawning hidden, Base64-encoded PowerShell that fetches and runs an unsigned DLL.

- External email delivered 08:09:14Z from a lookalike vendor domain; archive password included in the message body, defeating gateway detonation - gateway verdict at delivery was 'clean'
- User extracted and double-clicked `Invoice_Q2_Overdue.lnk` at 08:14:37Z; shortcut target invoked `powershell.exe -nop -w hidden -enc` with a Base64 command block
- Decoded command retrieves `wupdcore.dll` from 203.0.113.199 over HTTPS and executes it via `rundll32.exe`
- User has no administrative role and zero `powershell.exe` executions in 90 days of Falcon telemetry on this host; no IT change tickets reference FIN-WKS-0113
- Falcon behavioral and ML detections both fired at Critical, including `SuspiciousPowerShellEncodedCommand`

▸ How we got the answer (3 data points)

Is the destination IP 203.0.113.199 confirmed malicious infrastructure?

• Confirmed active C2: 34/93 VirusTotal engines flag the IP, it is datacenter-hosted with a freshly issued self-signed certificate, and passive DNS ties it to 11 recently registered invoice-themed lookalike domains.

- 34/93 VT engines malicious (last analysis 2026-07-08); vendor and community tags associate the IP with a commodity loader botnet active since late June 2026
- ASN 64502 (Example Hosting LLC) is a datacenter/hosting provider, not residential or corporate ISP; `is_datacenter=true`, no VPN/Tor classification
- TLS certificate on 443 is self-signed, issued 2026-07-05 with a randomized subject - consistent with freshly provisioned C2
- Passive DNS shows 11 lookalike invoice/billing domains registered within the past 10 days resolving to this IP, including the sender domain from this campaign
- No other host in the tenant communicated with this IP in 30 days of Falcon and firewall telemetry

▸ How we got the answer (3 data points)

Did the payload execute, and what did it accomplish on the host before containment?

• The second stage executed and established persistence: the loader ran under rundll32, completed 9 C2 check-ins over roughly four minutes, and registered a logon scheduled task before Falcon terminated the tree.

- `wupdcore.dll` written 08:15:02Z and loaded via `rundll32.exe` at 08:15:11Z; unsigned, global first-seen 2026-07-07
- 9 HTTPS beacons to 203.0.113.199 between 08:15Z and 08:19Z totalling 41 KB out / 220 KB in - consistent with check-in and tasking, not bulk exfiltration
- Scheduled task `\Microsoft\Windows\MsUpdCore` created 08:16:48Z with a logon trigger relaunching the DLL (T1053.005)
- One `OpenProcess` attempt against `lsass.exe` at 08:18:23Z blocked by Falcon credential-theft prevention; no successful memory read observed
- No shadow-copy deletion, ransomware precursors, or mass file enumeration in the execution window; task and DLL remain on disk pending remediation

▸ How we got the answer (4 data points)

Is the compromise contained to this host, or is there evidence of credential theft and lateral movement?

- **No lateral movement or successful credential dumping was observed, but the blocked LSASS access attempt during an active C2 session means user3's credentials and sessions must be treated as exposed.**

- No SMB, RDP, WinRM, or WMI connections initiated from FIN-WKS-0113 to any internal host during or after the execution window
- The LSASS `OpenProcess` attempt was blocked pre-read, but the operator had interactive tasking capability for ~4 minutes - browser-stored and cached credentials on the host cannot be ruled out
- No new sign-ins for `user3@example.com` from unfamiliar IPs or devices in Entra ID sign-in logs through 08:50Z
- IOC sweep (DLL hash, C2 IP, sender domain) returned zero matches across the other 412 sensored hosts
- Two other recipients of the campaign email did not extract or execute the attachment (no archive-extraction or lnk-execution telemetry on their hosts)

▸ How we got the answer (3 data points)

CONCLUSION

This is a confirmed malicious phishing compromise with partial attacker success. A password-protected archive defeated gateway detonation, the shortcut payload executed hidden encoded PowerShell, and the `wupdcore.dll` loader ran, beaconed to confirmed C2 at `203.0.113.199` for roughly four minutes, and established scheduled-task persistence before Falcon terminated the tree and the host was network-contained. Blast radius is currently one host and one user: no lateral movement, no confirmed credential theft, and no execution by the two other campaign recipients. Because an LSASS access attempt occurred during an interactive C2 window, `user3@example.com`'s credentials and sessions must be treated as compromised. Remediation must complete the containment the sensor started: credential reset and session revocation, persistence removal and host reimage, and tenant-wide IOC blocking and campaign purge.

RECOMMENDED ACTIONS

MUST DO

1 HIGH **Keep FIN-WKS-0113 network-contained; remove persistence and reimage** - Maintain Falcon containment, collect the queued RTR triage package first, then remove the `\Microsoft\Windows\MsUpdCore` task and `wupdcore.dll` and reimage per finance-endpoint policy before returning the host to the VLAN.

2 HIGH **Reset credentials and revoke all sessions for user3@example.com** - Force a password reset, revoke refresh tokens and active sessions in Entra ID, re-register MFA, and review sign-in and mailbox audit logs for 24 hours after 08:15Z. Treat browser-stored credentials on the host as exposed.

3 HIGH **Block campaign IOCs at firewall, DNS, and email gateway** - Block 203.0.113.199, the dropped-DLL hash, the sender domain, and the 11 passive-DNS-linked lookalike domains. Add the sender infrastructure to the tenant blocklist.

4 HIGH **Purge the campaign message from all recipient mailboxes** - Soft-delete the 08:09Z message from the two additional finance mailboxes and confirm via message trace that no further copies were delivered to other recipients or forwarded internally.

RECOMMENDED

5 MEDIUM **Hunt the delivery pattern across 30 days of email and endpoint telemetry** - Sweep for password-protected archives containing .lnk files from newly registered domains, and for `powershell.exe -enc` spawned from user-profile paths. The same campaign infrastructure appeared in ORG001-M365-27 and ORG001-CRWD-0871 within the past 14 days.

6 MEDIUM **Quarantine password-protected archives from external senders at the gateway** - The detonation bypass (password in message body) is the root cause of delivery. Quarantine or strip encrypted archives from external mail, or hold them pending analyst release.

7 MEDIUM **Restrict PowerShell for finance standard users** - Evaluate an attack surface reduction rule or AppLocker policy blocking powershell.exe execution for finance-department standard users, and add a custom Falcon IOA for shortcut-spawned encoded PowerShell.

Attack Timeline

2026-07-09T08:09:14Z	Phishing email from lookalike vendor domain delivered to user3@example.com and 2 other finance mailboxes; password-protected archive with password in message body bypasses gateway detonation
2026-07-09T08:14:37Z	User extracts archive and opens Invoice_Q2_Overdue.lnk; shortcut invokes powershell.exe -nop -w hidden -enc (T1566.001 → T1059.001)
2026-07-09T08:15:02Z	Encoded PowerShell downloads wupdcore.dll from 203.0.113.199:443 and writes it to AppData\Roaming\msupd\
2026-07-09T08:15:11Z	rundll32.exe loads wupdcore.dll; C2 beaconing begins (9 HTTPS check-ins, 41 KB out / 220 KB in)
2026-07-09T08:16:48Z	Scheduled task \Microsoft\Windows\MsUpdCore created for logon persistence (T1053.005)
2026-07-09T08:17:52Z	Falcon behavioral + ML composite detection fires at Critical - alert triggered
2026-07-09T08:18:23Z	OpenProcess attempt against lsass.exe blocked by Falcon credential-theft prevention (T1003.001 attempted)
2026-07-09T08:21:47Z	Falcon terminates the malicious process tree; beaconing stops
2026-07-09T08:26:10Z	Host network-contained; RTR triage collection queued; IOC sweep across 412 sensored hosts returns zero additional matches

Indicators of Compromise

TYPE	INDICATOR	CONTEXT
IP	`203.0.113.199`	C2 / payload host; 34/93 VT; ASN 64502 datacenter
SHA256	`4f2a...e91b`	wupdcore.dll loader, unsigned, first seen 2026-07-07
File path	`C:\Users\user3\AppData\Roaming\msupd\wupdcore.dll`	Dropped second stage
Scheduled task	`\Microsoft\Windows\MsUpdCore`	Logon persistence
Attachment	`Invoice_Q2_Overdue.zip` / `.lnk`	Delivery archive and shortcut payload
Domain	Lookalike vendor sender domain (+11 related, passive DNS)	Campaign delivery and C2 infrastructure