Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

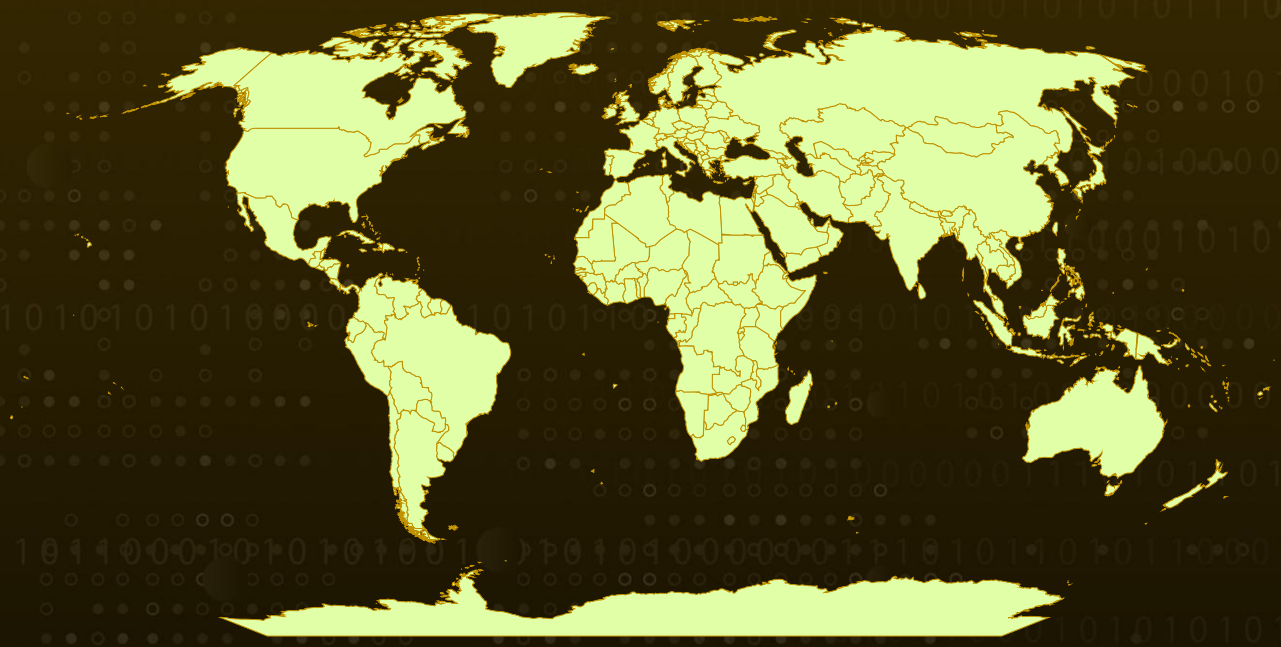
# DEAD#VAX: AsyncRAT Deployment via IPFS-Hosted VHD Phishing

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| February 05, 2026 | A1 | TA2026036 |

# Summary

**First Seen:** 2026
**Targeted Regions:** Worldwide
**Targeted Platforms:** Windows
**Malware:** AsyncRAT
**Campaign:** DEAD#VAX
**Attack:** The DEAD#VAX campaign combines clever social engineering with stealthy technical tricks, luring victims through convincing business-themed phishing emails that deliver a seemingly harmless document which quietly mounts a virtual drive and launches a multi-stage infection chain. By bypassing common security protections, evading analysis environments, and injecting its payload into trusted Windows processes, the attack ultimately deploys AsyncRAT entirely in memory, giving attackers persistent, covert control over compromised systems while leaving minimal forensic traces behind.

## Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Targeted  Non-Targeted

# Attack Details

**#1**

The DEAD#VAX campaign begins with a carefully crafted phishing email masquerading as a message from Progressive Components, a legitimate global supplier of tooling components. Sent under the display name “Progressive Purchasing,” the email uses a deceptive double-address format that appears trustworthy while actually routing through a suspicious or compromised domain. The message creates a sense of urgency by framing the content as a business-related request that requires a response within two days. To further reduce suspicion, the email even includes a fake “Virus scan completed. No threats detected” banner, making the content appear safe. Victims are then prompted to download what looks like a standard PDF document. Still, the file is actually a Virtual Hard Disk (VHD) hosted through IPFS infrastructure, allowing attackers to distribute payloads via decentralized storage.

**#2**

Once downloaded and opened, the VHD file is automatically mounted by Windows as a virtual drive. This technique cleverly bypasses the Mark-of-the-Web security control, since files inside the mounted container do not inherit the untrusted status typically assigned to internet downloads. Inside the drive, victims encounter a Windows Script File disguised with a double extension to resemble a harmless PDF. When executed, the script launches a heavily obfuscated batch file that begins checking the system environment, including verifying administrative privileges, detecting virtualized environments, and checking system memory to avoid sandbox analysis. The script then copies itself and uses PowerShell to parse its own content, extracting hidden payload data embedded within specific lines.

**#3**

This hidden payload undergoes several layers of deobfuscation before execution. The process removes Unicode noise, decodes Base64 content, applies XOR-based decryption, and performs character shifting to reveal the final stage. The decrypted result is a PowerShell-based loader responsible for persistence and process injection. It establishes stealthy persistence mechanisms through hidden scheduled tasks and VBS launchers while preparing to inject malicious code into trusted Microsoft-signed processes such as RuntimeBroker.exe, OneDrive.exe, taskhostw.exe, and sihost.exe, allowing the activity to blend into legitimate system operations.

**#4** The injection process follows a familiar pattern used in many advanced threats, leveraging Windows APIs to open target processes, allocate memory, write malicious code, and execute it remotely. To avoid reinfecting already compromised processes, the malware scans for a specific marker sequence before injecting. The final payload delivered through this chain is AsyncRAT, an open-source remote access trojan that grants attackers extensive control over infected machines. Capabilities include keylogging, screen and webcam capture, clipboard monitoring, file access, remote command execution, and long-term persistence. Notably, the payload operates entirely in memory as encrypted shellcode, never appearing on disk in a recognizable form, making detection significantly more challenging.

# Recommendations

- **Block IPFS Gateway Domains:** Configure network firewalls and web proxies to block or alert on connections to IPFS gateway domains such as w3s.link, ipfs.io, and similar decentralized storage gateways that are commonly abused for malware hosting.
- **Restrict VHD File Mounting:** Implement Group Policy settings to prevent automatic mounting of VHD, VHDX, ISO, and IMG files or require elevated privileges for mounting operations to mitigate Mark-of-the-Web bypass techniques.
- **Enable File Extension Visibility:** Ensure file extension visibility is enabled for all users across the organization to help identify disguised files using double extensions such as filename.pdf.wsf.
- **Deploy Process Injection Detection:** Implement Sysmon or equivalent endpoint logging to monitor for Win32 API calls associated with process injection including VirtualAllocEx, WriteProcessMemory, CreateRemoteThread, and OpenProcess with suspicious access flags.
- **Implement Email Gateway Controls:** Configure email security gateways to block or quarantine emails containing links to IPFS gateways and to flag messages with urgency manipulation language combined with download links.
- **Monitor Scheduled Task Creation:** Implement detection rules for newly created scheduled tasks that execute wscript.exe or PowerShell scripts, particularly those with randomized or suspicious naming conventions.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1566: Phishing | T1566.001: Spearphishing Attachment |
| | | T1566.002: Spearphishing Link |
| Execution | T1059: Command and Scripting Interpreter | T1059.001: PowerShell |
| | | T1059.003: Windows Command Shell |
| | | T1059.005: Visual Basic |
| | | T1059.007: JavaScript |
| Persistence | T1053: Scheduled Task/Job | T1053.005: Scheduled Task |
| Defense Evasion | T1027: Obfuscated Files or Information | T1027.002: Software Packing |
| | T1140: Deobfuscate/Decode Files or Information | |
| | T1218: System Binary Proxy Execution | |
| | T1497: Virtualization/Sandbox Evasion | T1497.001: System Checks |
| | T1055: Process Injection | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| Credential Access | T1056: Input Capture | T1056.001: Keylogging |
| Discovery | T1082: System Information Discovery | |
| Collection | T1113: Screen Capture | |
| | T1125: Video Capture | |
| | T1115: Clipboard Data | |
| Command and Control | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | T1573: Encrypted Channel | |
| Exfiltration | T1041: Exfiltration Over C2 Channel | |
| Impact | T1565: Data Manipulation | T1565.001: Stored Data Manipulation |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | 365265cf9749d7b04d2c037449cbfae23bcb75ed6e2eb1f161ca680e94ca466e, a048fc039ba6d1e22736c9142998de79445f878136664958f9b11156aaf1b61f, 7fa075ed827095b4531cb35f650ccf6345c3799734e4ed30d9f52e72c0711713, 7e4646d0cf91153653c5e366f98a65aad5ef363e0edeb246c809f53085971453, 3d3342af3608399704d5daf9dc061ad1f8b243531fd9ef8497a10c6a9dd59661, b77312ea8cdec4a33be790cf9587a93389b56e735a3c9560cd9116a4b115e2ec, bcccb21d96d0ed7d6d1bb2e33e9981287addb94314b3cbbd9d5d7332c47f7b80, 601d9deea6467a57e42c355d481331cd78d6487bd160a081332420c69f214455, 4c6c9ec88d00a3b77e6288afc4ee9974ac07a2c73012c3e1a017c457dcf22d87 |

| TYPE | VALUE |
| --- | --- |
| Domain | mingyitc[.]com |
| URL | hxxps[:]//bafybeiaj6jw2xhbppgji757tn3hg5uu6splaa5gyydkwnzwprzakcp44ve[.]ipfs[.]w3s[.]link/PurchaseOrder_0006094050126_%20Procomps_Docx[.]vhd |

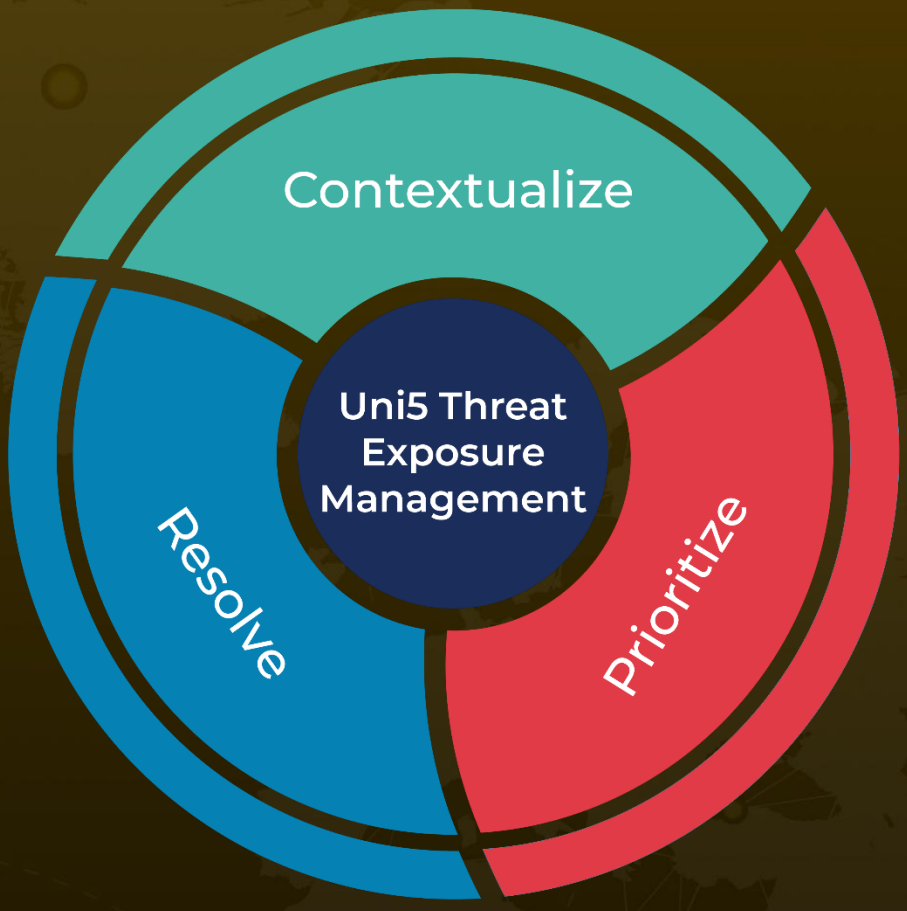
## References

https://www.securonix.com/blog/deadvax-threat-research-security-advisory/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**February 05, 2026 • 6:00 AM**

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com