Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

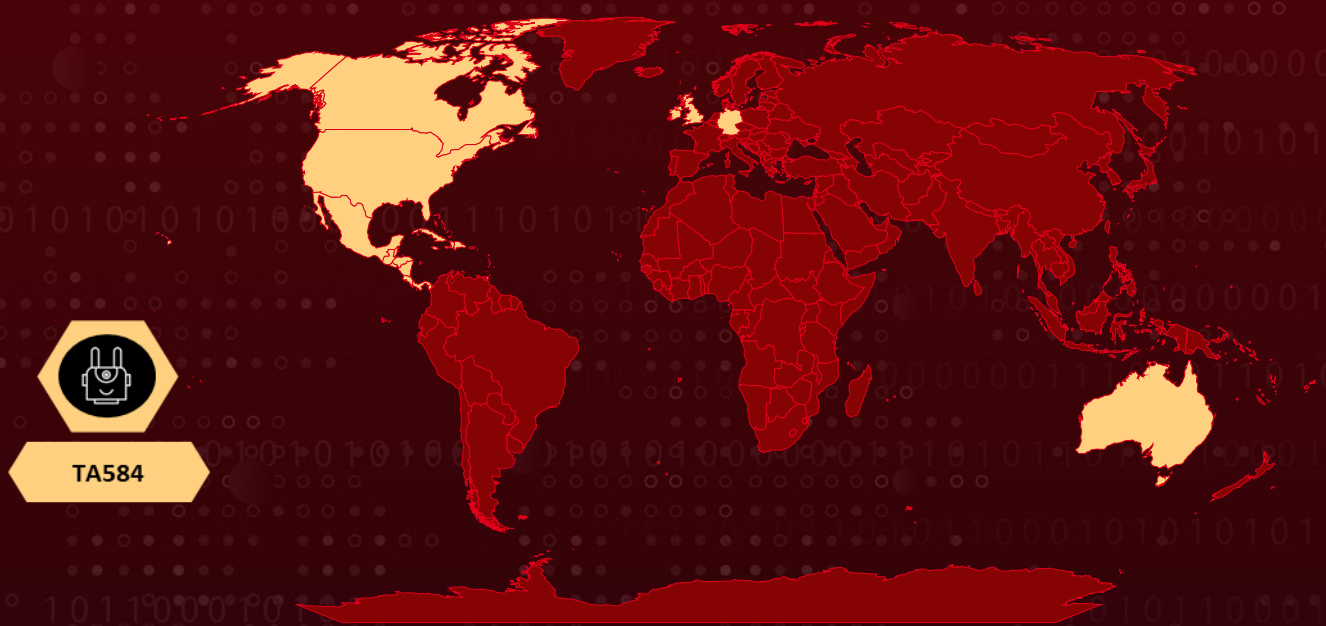
TA584 and the Business of Breach: Selling Access at Scale

Date of Publication	Admiralty Code	TA Number
January 30, 2026	A1	TA2026029

Summary

First Seen: 2020
Targeted Regions: Antigua and Barbuda, Bahamas, Barbados, Belize, Canada, Costa Rica, Cuba, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Trinidad and Tobago, United States, United Kingdom, Ireland, Germany, Australia
Targeted Platform: Windows
Targeted Industries: Healthcare, Government, Financial Services, Education, Business Services, Hospitals, Technology, Retail, Insurance, Construction, Automotive
Threat Actor: TA584
Malware: Tsundere Bot, XWorm
Attack: TA584 is a long-running initial access broker active since 2020 that conducts large-scale phishing campaigns using ClickFix social engineering to deliver Tsundere Bot and XWorm malware. The actor impersonates trusted organizations and sends high-volume, targeted emails containing filtered links that lead victims to CAPTCHA-based landing pages designed to trick them into executing malicious PowerShell commands. The operation relies on layered redirection, infrastructure rotation, and IP filtering to evade detection, indicating a mature, scalable phishing operation focused on broad and sustained access generation.

Attack Regions



Attack Details

#1

TA584 is a well-established initial access broker active since late 2020. It runs large-scale phishing campaigns that rely on ClickFix social engineering to deliver Tsundere Bot and XWorm malware. The operation focuses on speed, volume, and user manipulation rather than exploit-based intrusion.

#2

The attack begins with phishing emails sent from compromised legitimate accounts or trusted email platforms such as SendGrid and Amazon SES. These messages impersonate recognizable entities, including healthcare providers, government bodies, recruitment firms, and common business services. Each email contains a unique, victim-specific link that applies geofencing and IP filtering before allowing access to the next stage.

#3

Victims who pass these checks are redirected to themed landing pages that display slide-based CAPTCHAs. Completing the CAPTCHA leads to a ClickFix prompt instructing the user to open the Windows Run dialog and execute a provided command. This step persuades the victim to manually launch a malicious PowerShell command, bypassing many security controls.

#4

Once active, Tsundere Bot establishes persistent communication with its controller and profiles the system to generate a unique victim identifier. It collects basic hardware and operating system details and halts execution on systems configured for CIS-region languages, indicating deliberate targeting controls. Persistence is reinforced through an accompanying XWorm variant that hides registry run keys using null-byte obfuscation and launches hidden PowerShell activity at every reboot.

#5

Campaigns range from thousands to nearly two hundred thousand messages, with targeting shifting by region and sector over time. TA584 has maintained consistent tradecraft for years while gradually expanding its reach. Recent activity suggests continued experimentation with payloads and a sustained effort to broaden victim coverage.

Recommendations

Restrict PowerShell Execution: Enforce Group Policy restrictions to limit PowerShell access to approved roles only, materially reducing exposure to ClickFix-style social engineering and user-driven code execution.

Block Node.js in User Directories: Use application control policies such as AppLocker or Windows Defender Application Control to prevent execution of node.exe from non-standard, user-writable locations including AppData\Local directories.

Monitor PowerShell Spawning Node.js: Create detection rules for powershell.exe or cmd.exe spawning node.exe processes, particularly when Node.js is located in user profile directories or other non-standard locations.

Block Ethereum RPC Endpoints: Block or monitor outbound traffic to Ethereum RPC providers used by Tsundere Bot for C2 retrieval, preventing the malware from receiving command and control instructions via the blockchain.

Inspect WebSocket Traffic: Implement network monitoring to detect and inspect WebSocket connections to unknown or uncategorized domains, as Tsundere Bot uses WebSockets for C2 communication.

Monitor Registry for Hidden Keys: Deploy detection capabilities for registry modifications containing null-byte characters in key names, which are used by SharpHide for persistence evasion.

Implement Network Segmentation: Segment networks to limit lateral movement capabilities if initial compromise occurs, particularly isolating systems that may process sensitive healthcare or financial data.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
	T1078: Valid Accounts	T1078.004: Cloud Accounts
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1204: User Execution	T1204.001: Malicious Link
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1027: Obfuscated Files or Information	T1027.010: Command Obfuscation
	T1055: Process Injection	T1055.012: Process Hollowing
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
Discovery	T1082: System Information Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	T1102.002: Bidirectional Communication
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	T1584.003: Virtual Private Server

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	94[.]159[.]113[.]37, 85[.]236[.]25[.]119, 80[.]64[.]19[.]148, 85[.]208[.]84[.]208, 178[.]16[.]52[.]242, 94[.]159[.]113[.]64
IPv4:Port	193[.]17[.]183[.]126[:]3001
URL	hxxp[:]//94[.]159[.]113[.]37/ssd[.]png
SHA256	bbedc389af45853493c95011d9857f47241a36f7f159305b097089866502ac99, 441c49b6338ba25519fc2cf1f5cb31ba51b0ab919c463671ab5c7f34c5ce2d30

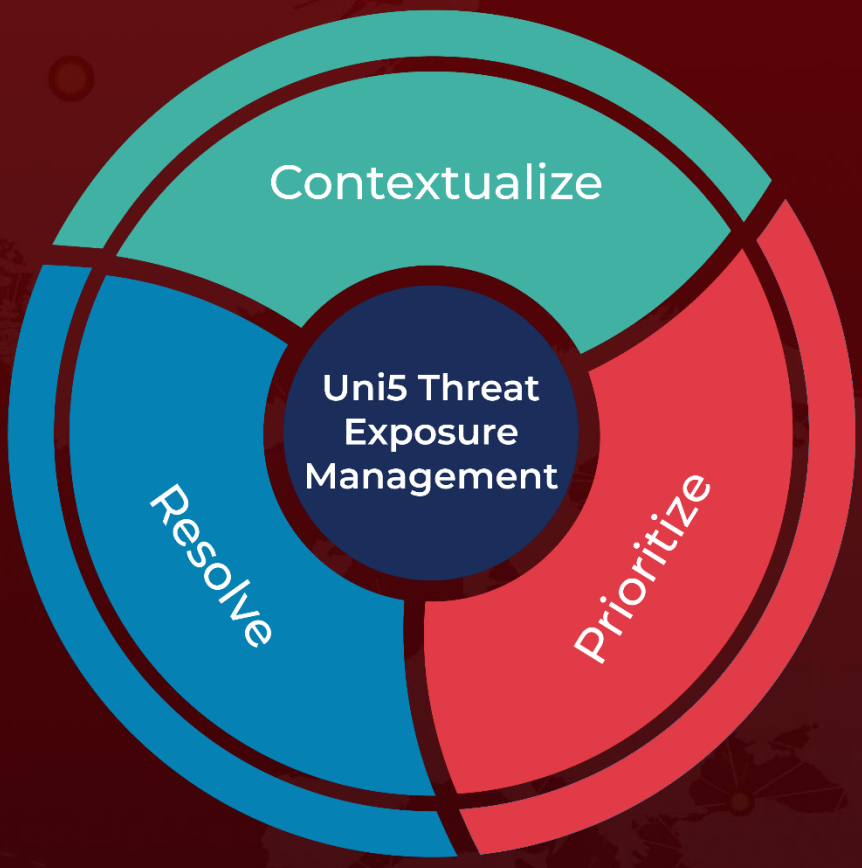
References

https://www.proofpoint.com/us/blog/threat-insight/cant-stop-wont-stop-ta584-innovates-initial-access

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

January 30, 2026 • 03:00 AM

More at www.hivepro.com