

HiveForce Labs

THREAT ADVISORY



ACTOR REPORT

TA585 Leverages ClickFix Technique and MonsterV2 Malware

Date of Publication

October 15, 2025

Admiralty Code

A1

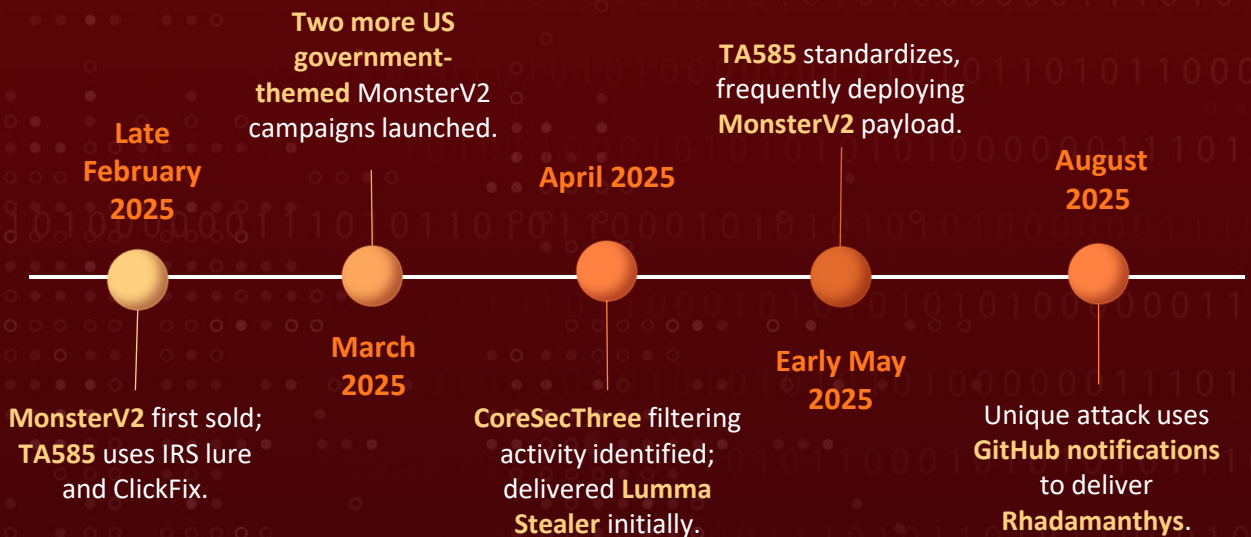
TA Number

TA2025316

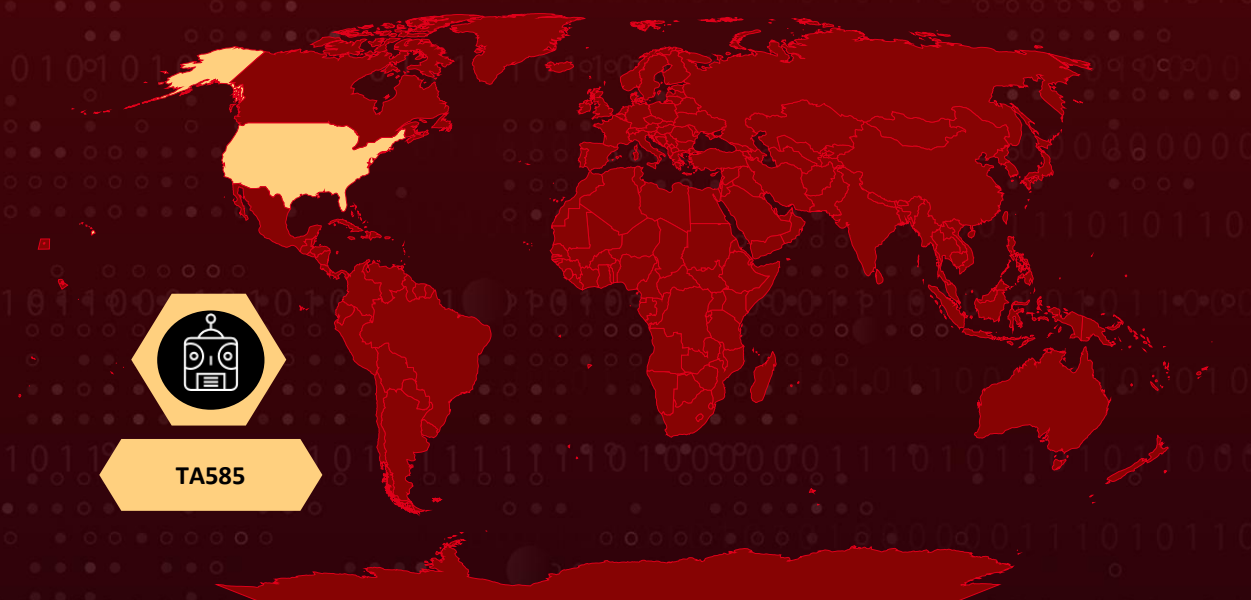
Summary

First Seen: 2025
Targeted Country: United States
Targeted Platform: Windows
Targeted Industries: Finance, Accounting
Threat Actor: TA585
Malware: MonsterV2, Lumma, Rhadamanthys
MonsterV2 MaaS Pricing Model: \$800–\$2,000 per month

Timeline



Actor Map



Actor Details

#1

TA585 is a sophisticated, financially motivated cybercriminal actor known for operating its own vertically integrated “owned attack chain.” Unlike many groups that outsource distribution or initial access, TA585 registers and manages its own infrastructure, controls email delivery, and directs the malware installation process. This autonomy provides greater operational control, resilience, and consistency across campaigns, which have primarily targeted finance and accounting organizations through small, focused attacks.

#2

The group’s initial intrusion phase relies on high-trust social engineering, often impersonating U.S. government entities such as the IRS or Small Business Administration. One particularly effective tactic abuses legitimate services like GitHub notifications. TA585 tags legitimate accounts within a controlled repository, prompting GitHub to send authentic notification emails containing malicious links. This method exploits GitHub’s trusted reputation to evade standard email security filters.

#3

Once the victim interacts with the lure, the infection chain uses the [ClickFix](#) technique, a deceptive web-based lure typically disguised as a CAPTCHA. Victims are tricked into manually running a PowerShell command via the Windows Run dialog (Win+R), enabling the attacker to bypass browser defenses and some endpoint detection sandboxes.

#4

TA585 employs an infrastructure pattern known as CoreSecThree, where the lure page continuously “beacons” to its server. The final payload is delivered only after the malicious script executes and the MonsterV2 malware checks in from the same victim IP. First advertised on criminal forums in early 2025, MonsterV2 is a premium Malware-as-a-Service (MaaS) platform costing \$800–\$2,000 monthly.

#5

It combines remote access, credential theft, data exfiltration, and webcam capture, with built-in geo-fencing to avoid CIS countries. The malware is often protected with the SonicCrypt crypter for obfuscation. TA585’s end-to-end control, selective targeting, and innovative delivery techniques make it one of the more adaptive and resilient cybercrime operations observed in 2025.

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
TA585	-	United States	Finance, Accounting
	MOTIVE		
	Financial gain		

Recommendations



User Awareness Training: Educate users to recognize phishing attempts, especially those mimicking trusted U.S. government agencies (IRS, SBA), and to be cautious about executing PowerShell commands or clicking on CAPTCHA overlays that prompt manual actions.



Restrict PowerShell Usage: Implement policies that prevent non-administrative users from running PowerShell scripts or commands, especially via Windows Run dialog, to block the ClickFix infection technique's execution path.



Email Security and Filtering: Enhance email filtering solutions to detect and block phishing emails exploiting legitimate platforms like GitHub notifications and impersonations of trusted entities. Use threat intelligence feeds to update these filters regularly.



Web Security Controls: Monitor for malicious web injections and block access to suspicious pages that use fake CAPTCHA overlays or unusual JavaScript behavior consistent with CoreSecThree.



Endpoint Detection and Response: Deploy advanced endpoint protection that can detect obfuscated and encrypted malware like MonsterV2, including behavior-based detection for RAT and stealer activities.

Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0007</u> Discovery
<u>TA0005</u> Defense Evasion	<u>TA0040</u> Impact	<u>TA0010</u> Exfiltration	<u>TA0009</u> Collection
<u>TA0006</u> Credential Access	<u>TA0008</u> Lateral Movement	<u>TA0011</u> Command and Control	<u>T1053</u> Scheduled Task/Job
<u>T1566.002</u> Spearphishing Link	<u>T1566</u> Phishing	<u>T1204</u> User Execution	<u>T1204.001</u> Malicious Link
<u>T1199</u> Trusted Relationship	<u>T1547</u> Boot or Logon Autostart Execution	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.001</u> PowerShell
<u>T1189</u> Drive-by Compromise	<u>T1027</u> Obfuscated Files or Information	<u>T1082</u> System Information Discovery	<u>T1562.001</u> Disable or Modify Tools
<u>T1562</u> Impair Defenses	<u>T1036</u> Masquerading	<u>T1056</u> Input Capture	<u>T1056.001</u> Keylogging
<u>T1113</u> Screen Capture	<u>T1005</u> Data from Local System	<u>T1105</u> Ingress Tool Transfer	<u>T1041</u> Exfiltration Over C2 Channel
<u>T1071</u> Application Layer Protocol	<u>T1071.001</u> Web Protocols	<u>T1564.003</u> Hidden Window	<u>T1564</u> Hide Artifacts
<u>T1021</u> Remote Services			

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	ccac0311b3e3674282d87db9fb8a151c7b11405662159a46dda71039f2200a67, 666944b19c707afaa05453909d395f979a267b28ff43d90d143cd36f6b74b53e, 7cd1fd7f526d4f85771e3b44f5be064b24fbb1e304148bbac72f95114a13d8c5, 0e83e8bfa61400e2b544190400152a54d3544bf31cfec9dda21954a79cf581e9, d221bf1318b8c768a6d824e79c9e87b488c1ae632b33848b638e6b2d4c76182b, 69e9c41b5ef6c33b5caff67ffd3ad0ddd01a799f7cde2b182df3326417dfb78e, 6237f91240abdbe610a8201c9d55a565aabd2419ecbeb3cd4fe387982369f4ae, b36aac2ea25afd2010d987de524f9fc096bd3e1b723d615a2d85d20c52d2a711, 912ef177e319b5010a709a1c7143f854e5d1220d176bc130c5564f5efe8145ed, ba72e8024c90aefbfd56cdf2ab9033a323b63c83bd5df19268978cded466214e, e7bcd70f0ee4a093461cfb964955200b409dffd3494b692d54618d277cb309e, 399d3e0771b939065c980a5e680eec6912929b64179bf4c36cefb81d77a652da
IPv4:PORT	139[.]180[.]160[.]173[:]7712, 155[.]138[.]150[.]12[:]7712, 83[.]217[.]208[.]77[:]7712, 83[.]217[.]208[.]77[:]7712, 91[.]200[.]14[.]69[:]7712, 212[.]102[.]255[.]102[:]7712, 84[.]200[.]154[.]105[:]7712, 144[.]172[.]117[.]158[:]7712, 109[.]120[.]137[.]128[:]7712, 84[.]200[.]17[.]240[:]7712, 84[.]200[.]77[.]213[:]7712

References

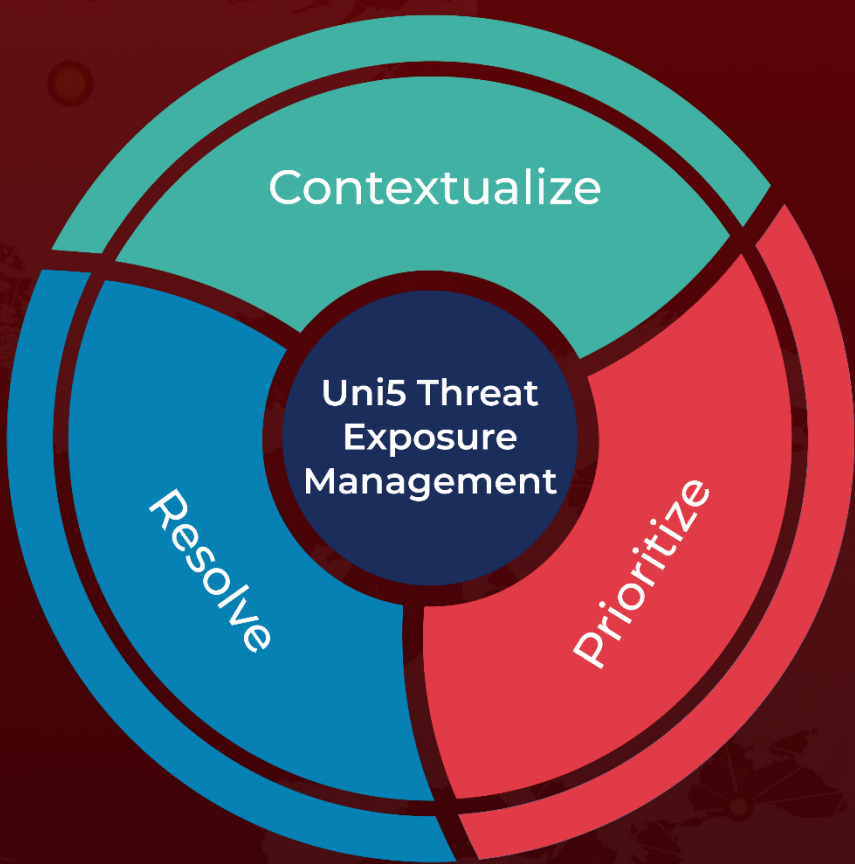
<https://www.proofpoint.com/us/blog/threat-insight/when-monster-bytes-tracking-ta585-and-its-arsenal>

<https://hivepro.com/threat-advisory/clickfix-deception-hackers-use-sharepoint-and-graph-api-to-deploy-havoc-malware/>

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
October 15, 2025 • 10:00 AM

