Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

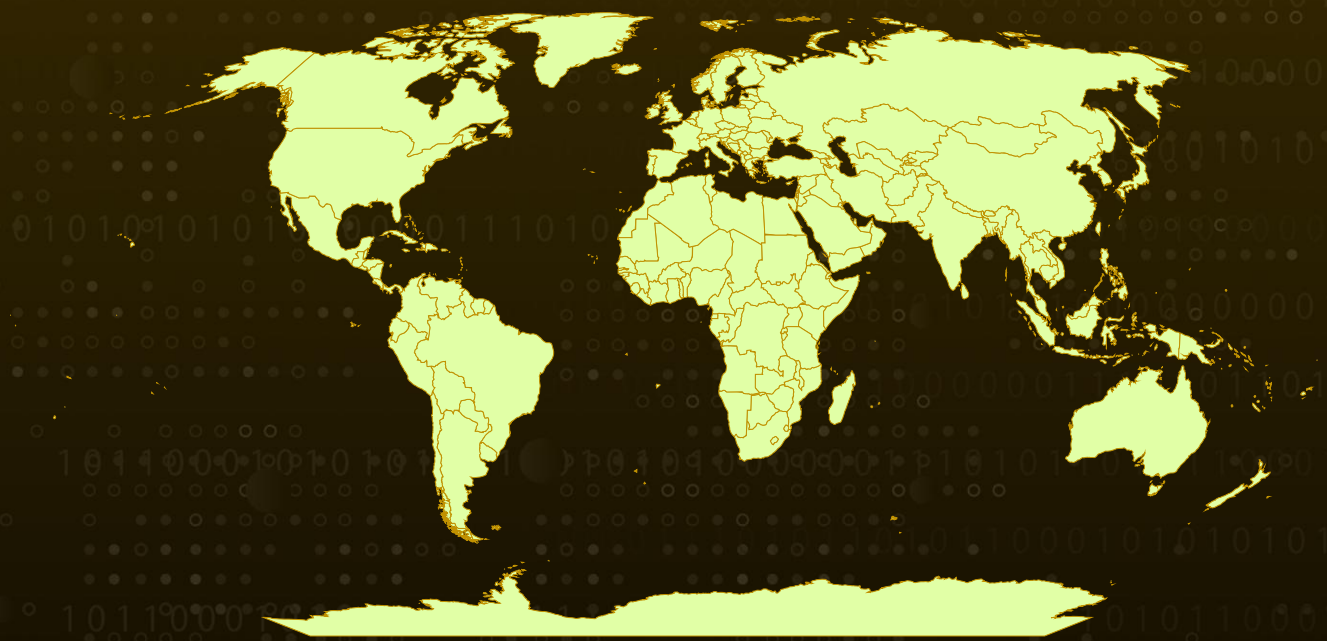
CastleBot Rising: The Evolving Malware-as-a-Service Threat

Date of Publication	Admiralty Code	TA Number
August 11, 2025	A1	TA2025245

Summary

Attack Discovered: Early 2025
Targeted Countries: Worldwide
Malware: CastleBot
Attack: CastleBot is a fast-evolving malware framework sold as part of a Malware-as-a-Service operation, giving cybercriminals a powerful, flexible tool to launch large-scale attacks. First emerging in early 2025, it spreads mainly through fake software installers promoted via SEO poisoning, tricking victims into downloading it. Once on a system, CastleBot runs through multiple stages, starting with a lightweight stager, followed by a loader, and ending with a core backdoor capable of stealing information, deploying more malware, and laying the groundwork for ransomware. It communicates with its operators over encrypted channels, can adapt tasks mid-campaign, and uses advanced techniques to evade detection. Linked to campaigns delivering other dangerous threats like NetSupport RAT and WarmCookie, CastleBot's modular design and rapid development make it a growing threat in today's cybercrime ecosystem.

Attack Regions



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

Attack Details

#1 CastleBot is an emerging malware framework within the rapidly expanding Malware-as-a-Service (MaaS) market, designed with adaptability and scalability. First identified in early 2025, it has swiftly evolved from a newcomer into a sophisticated toolkit capable of delivering infostealers and backdoors, often laying the groundwork for ransomware attacks. Its distribution relies heavily on trojanized software installers hosted on fake websites, frequently promoted through SEO poisoning to trick victims into downloading malicious files.

#2 The framework is composed of three key components: a stager, a loader, and a core backdoor. The stager, a lightweight shellcode, is built for flexibility, enabling CastleBot to integrate with various delivery methods. It uses the DJB2 hashing algorithm for dynamic API resolution and disguises its payload retrieval as Googlebot HTTP traffic. Once decrypted with hardcoded XOR keys, these payloads, containing both the CastleBot core and loader, are prepared for execution through memory permissions adjustments.

#3 The CastleBot core operates as a highly capable backdoor, complete with its own API resolution mechanism and encrypted configuration handling. It communicates with its C2 infrastructure using ChaCha encryption, exchanging serialized, encrypted containers of task data. These containers can hold a range of instructions, from deploying additional malware to performing detailed system reconnaissance, enabling highly customized and chained operations. The malware is engineered to escalate privileges, detect virtualized analysis environments, prevent system restarts, and harvest extensive system information before securely transmitting it to its operators.

#4 One of CastleBot's most dangerous traits is its flexible task execution model. Each task specifies a "launch_method," defining how the payload will be executed. This includes injecting PE files into suspended processes, bypassing memory checks with undocumented Windows functions, and creating scheduled tasks for persistence. Its design allows operators to alter payloads mid-operation, ensuring that no two infections are identical. This modular approach empowers affiliates to shift objectives quickly from information theft to ransomware delivery without needing to redeploy the malware entirely.

#5 By mid-2025, CastleBot had expanded its capabilities to include a "wow64_bypass" feature for launching 32-bit binaries from the SysWOW64 directory, as well as stealthier injection techniques such as QueueUserAPC to reduce forensic traces. The malware has ties with campaigns delivering other major threats like NetSupport RAT, SecTopRAT, HijackLoader, and MonsterV2. Infection vectors vary, from weaponized ZIP archives masquerading as legitimate installers to ClickFix-based PowerShell execution chains. In many cases, these operations have led directly to the deployment of backdoors like WarmCookie, known to facilitate ransomware attacks.

Recommendations

- **Avoid shady downloads:** Only install software from official vendor websites or trusted app stores. Fake download pages and GitHub repos are a major CastleBot delivery trick.
- **Keep your systems patched:** Update operating systems, browsers, and all software regularly. Many loaders used by CastleBot rely on exploiting outdated components.
- **Segment and limit permissions:** Restrict admin rights to only those who absolutely need them. CastleBot tries to run with elevated privileges to carry out attacks.
- **Monitor outbound connections:** CastleBot uses encrypted C2 communications, but unusual connections to unfamiliar domains or over uncommon ports should be investigated immediately.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control
T1566 Phishing	**T1036** Masquerading	**T1027** Obfuscated Files or Information	**T1055** Process Injection
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1082** System Information Discovery	**T1140** Deobfuscate/Decode Files or Information

T1053 Scheduled Task/Job	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.010 AutoHotKey & AutoIT
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1068 Exploitation for Privilege Escalation	T1608 Stage Capabilities
T1608.006 SEO Poisoning	T1105 Ingress Tool Transfer	T1204 User Execution	T1106 Native API
T1574 Hijack Execution Flow	T1574.001 DLL		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[:]//173[.]44[.]141[.]89/service/download/data_4x[.]bin, hxxp[:]//173[.]44[.]141[.]89/service/download/data_3x[.]bin, hxxp[:]//173[.]44[.]141[.]89/service/, hxxp[:]//mhousecreative [.]com/service/, hxxp[:]//80[.]77[.]23[.]48/service/, hxxp[:]//62[.]60[.]226[.]73/service/, hxxp[:]//107[.]158[.]128[.]45/service/, hxxp[:]//62[.]60[.]226[.]73/service/, hxxp[:]//mhousecreative[.]com/service/download/general_1, hxxp[:]//173[.]44[.]141[.]89/service/download/docusign2[.]exe, hxxp[:]//107[.]158[.]128[.]105/c91252f9ab114f26[.]php, hxxps[:]//google[.]herionhelpline [.]com/app/AcerUSBUpdate[.]exe, hxxps[:]//google[.]herionhelpline [.]com/app/light1_v5_signed[.]html, hxxps[:]//google[.]herionhelpline[.]com/app/SlackUpdateWeb[.]html, hxxp[:]//107[.]158[.]128[.]45/service/download/Exchanger32[.]zip, hxxp[:]//107[.]158[.]128[.]45/service/download/CCver_Setup[.]exe
IPv4	170[.]130[.]165[.]112
SHA256	202f6b6631ade2c41e4762e5877ce0063a3beabce0c3f8564b6499a1164c1e04, a2898897d3ada2990e523b61f3efaacf6f67af1a52e0996d3f9651b41a1c59c9, d6eea6cf20a744f3394fb0c1a30431f1ef79d6992b552622ad17d86490b7aa7b,

TYPE	VALUE
SHA256	2a2cd6377ad69a298af55f29359d67e4586ec16e6c02c1b8ad27c38471145569, 8b2ebeff16a20cfcf794e8f314c37795261619d96d602c8ee13bc6255e951a43, cbaf513e7fd4322b14adcc34b34d793d79076ad310925981548e8d3cff886527, 05ecf871c7382b0c74e5bac267bb5d12446f52368bb1bfe5d2a4200d0f43c1d8, 5bca7f1942e07e8c12ecd9c802ecdb96570dfaaa1f44a6753ebb9ffda0604cb4, bf21161c808ae74bf08e8d7f83334ba926ffa0bab96ccac42dde418270387890, e6aab1b6a150ee3cbc721ac2575c57309f307f69cd1b478d494c25cde0baaf85, b45cce4ede6ffb7b6f28f75a0cbb60e65592840d98dcb63155b9fa0324a88be2, 03122e46a3e48141553e7567c659642b1938b2d3641432f916375c163df819c1, 12de997634859d1f93273e552dec855bfae440dcf11159ada19ca0ae13d53dff, c8f95f436c1f618a8ef5c490555c6a1380d018f44e1644837f19cb71f6584a8a, 8bf93cef46fda2bdb9d2a426fbcd35ffedea9ed9bd97bf78cc51282bd1fb2095, 4834bc71fc5d3729ad5280e44a13e9627e3a82fd4db1bb992fa8ae52602825c6, 53dddae886017fbfbb43ef236996b9a4d9fb670833dfa0c3eac982815dc8d2a5, Ab725f5ab19eec691b66c37c715abd0e9ab44556708094a911b84987d700aa62

References

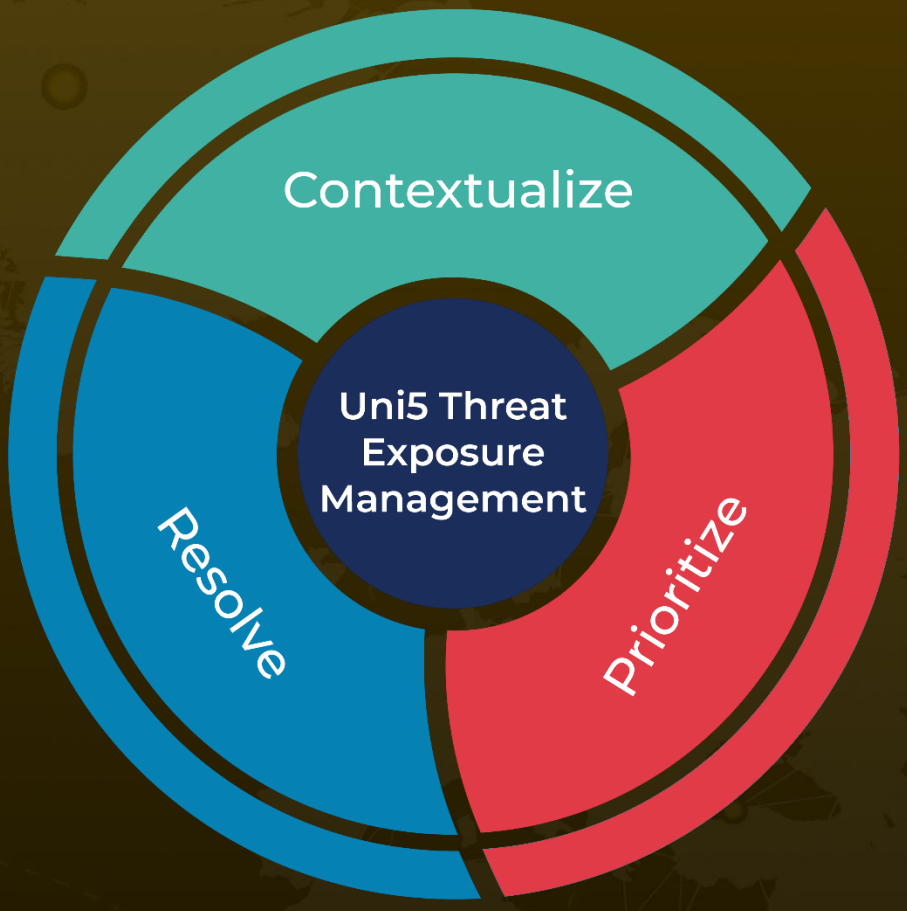
https://www.ibm.com/think/x-force/dissecting-castlebot-maas-operation

https://catalyst.prodaft.com/public/report/understanding-current-castleloader-campaigns/overview#heading-1000

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

August 11, 2025 • 5:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com