Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

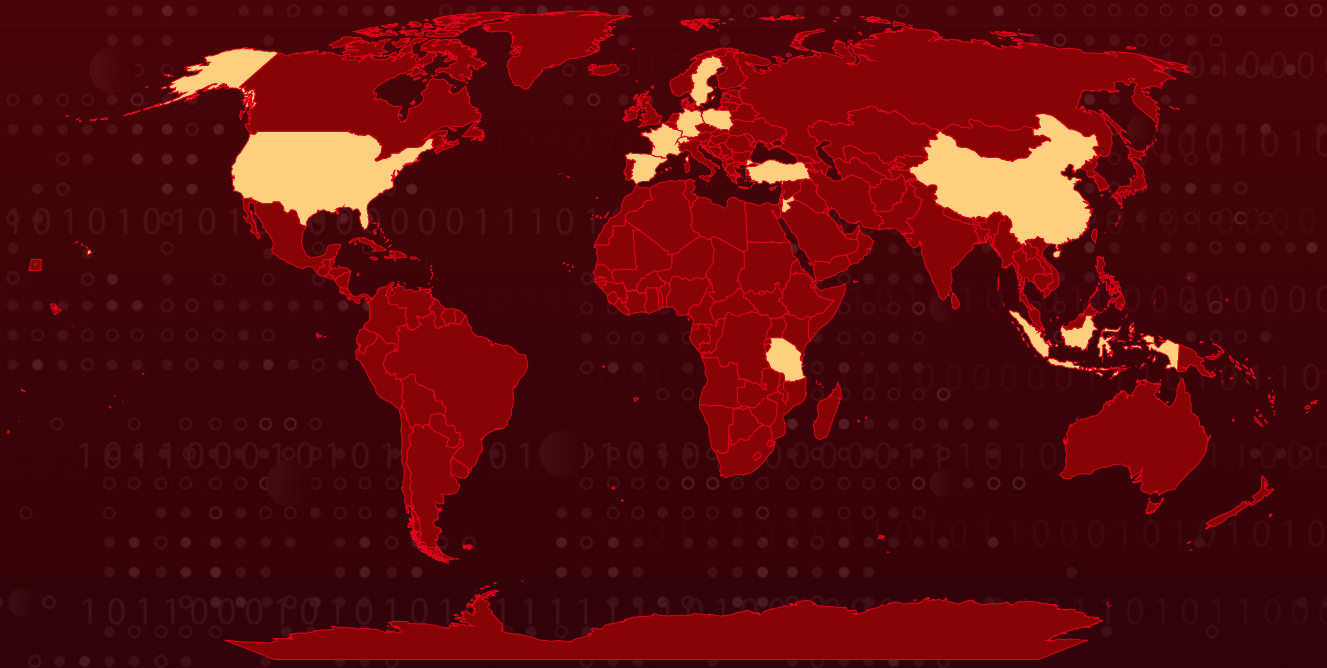
A New Ransomware Threat: Hellcat's Rapid Expansion

Date of Publication	Admiralty Code	TA Number
April 11, 2025	A1	TA2025110

Summary

First Seen: Mid-2024
Targeted Countries: United States, China, Germany, Turkey, Indonesia, Jordan, Poland, Switzerland, France, Sweden, Spain, Tanzania
Malware: Hellcat
Targeted Platforms: Windows
Ransom Demand: $125,000
Targeted Industries: Critical infrastructure, Government, Educational institutions, Energy, Financial Services, Technology, Casino & Gambling, Media, Telecommunications, Transportation, Manufacturing
Attack: HellCat is a Ransomware-as-a-Service (RaaS) operation that emerged in 2024, leveraging a decentralized affiliate model to deliver customized payloads and infrastructure. It gains access through phishing or exploiting vulnerabilities, then exfiltrates data and encrypts systems in a double-extortion scheme. The ransomware shares code similarities with Morpheus, indicating a shared toolkit. Its growing sophistication targets high-value sectors, urging strong cyber defenses and backups.

Attack Regions



Attack Details

#1

HellCat first emerged in mid-2024 as a Ransomware-as-a-Service (RaaS) operation, quickly distinguishing itself through a decentralized affiliate model. By offering customized payloads, infrastructure, and support to affiliates in exchange for a revenue share, HellCat has been able to scale its reach across the world. This affiliate-driven approach complicates attribution, as individual campaigns may vary significantly in sophistication and target selection, yet all bear the HellCat banner.

#2

Initial access for HellCat affiliates commonly involves both social engineering and exploitation of public-facing applications. Spear-phishing emails carrying malicious Office documents or ZIP archives often embedding obfuscated PowerShell scripts remain a primary vector. Simultaneously, HellCat actors have leveraged zero-day and unpatched vulnerabilities in platforms like Atlassian Jira and VPN appliances to gain direct entry without user interaction, harvesting credentials via infostealer malware such as Lumma Stealer and Redline before moving laterally using legitimate administrative tools.

#3

A defining feature of HellCat operations is its double-extortion strategy. After establishing a foothold, operators exfiltrate sensitive data ranging from proprietary documents to personal records to cloud storage or TOR-accessible drop sites before encrypting endpoints. Victims receive ransom demands not only for decryption keys but also to prevent the public release of stolen data, with attackers sometimes employing culturally resonant taunts (e.g., demanding “$125,000 in baguettes”) to amplify reputational pressure. This psychological dimension increases the likelihood of payment, as organizations seek to avoid both operational downtime and public embarrassment.

#4

Technical analyses reveal substantial code overlaps between HellCat and other ransomware strains most notably Morpheus suggesting a shared builder or toolkit underlying multiple RaaS brands. Both HellCat and Morpheus payloads employ in-memory reflective loading to avoid disk artifacts and leverage similar command-and-control stagers, although definitive proof of formal collaboration remains elusive.

#5

In early 2025, HellCat campaigns continued to target high-value sectors, in March, educational institutions fell victim to a zero-day exploit in a popular VPN appliance, resulting in rapid network infiltration and encryption within hours, and more recently four U.S. and European companies including HighWire Press and LeoVegas Group were compromised via stolen Jira credentials, leading to extensive data theft and subsequent ransomware deployment across critical systems. These incidents underscore HellCat’s agility in selecting high-value targets and exploiting both human and technical vulnerabilities.

Recommendations

Apply Security Patches and Updates Promptly: Prioritize timely updates for public-facing applications (e.g., Jira, VPNs). Employ continuous scanning to identify and remediate exposed services.

Deploy Endpoint Detection and Response (EDR) Solutions: Utilize EDR tools to monitor and analyze endpoint activities, enabling the detection and swift response to suspicious behaviors indicative of ransomware attacks.

Restrict User Privileges and Network Access: Apply the principle of least privilege by limiting user access rights to only what is necessary for their roles. Implement network segmentation to contain potential ransomware spread and regularly audit privileged accounts.

Strengthen Email Security and Filtering: Implement advanced email filtering solutions to block malicious attachments, links, and phishing attempts. Technologies such as SPF, DKIM, and DMARC can authenticate senders and reduce the risk of email-based attacks.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an Hellcat ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0005 Defense Evasion	TA0010 Exfiltration	TA0002 Execution
TA0007 Discovery	TA0040 Impact	TA0008 Lateral Movement	TA0011 Command and Control
TA0003 Persistence	T1567 Exfiltration Over Web Service	T1490 Inhibit System Recovery	T1567.002 Exfiltration to Cloud Storage

T1059 Command and Scripting Interpreter	T1027 Obfuscated Files or Information	T1566.001 Spearphishing Attachment	T1041 Exfiltration Over C2 Channel
T1190 Exploit Public-Facing Application	T1059.001 PowerShell	T1562.001 Disable or Modify Tools	T1573 Encrypted Channel
T1562 Impair Defenses	T1021 Remote Services	T1486 Data Encrypted for Impact	T1566 Phishing
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1620 Reflective Code Loading	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	931396d6332709956237cf76ee246b01
SHA1	b834d9dbe2aed69e0b1545890f0be6f89b2a53c7
SHA256	4b2edadc8f90e9fcc976f02a9eda1640cd92c07718c0271842fbd4ca7e2906e2, 53c09e57cea028c0439477cd90bcf8f981067a120a2fb7b86d0f13017727a93a, 5b492a70c2bbded7286528316d402c89ae5514162d2988b17d6434ead5c8c274, 6924479c42b3732e0d57b34714b7210e14655ee1ca570ae4aab1d90c3f6c6428, 93aa8b0f950a7ea7f0cee2ba106efaacf673bb2b504ca0b9e87f9ea41acfb599, b8e71845cc8ccd668a3436d1952a6c57649974bb8399e599dc33afc4c0843be7, dcd7995038ad4839e88e5bb3bf654b4f7c2ad09780a39c9d47596ce717fd4ac2
Tor Address	hellcakbszllztlyqbjzwcbdhfrodx55wq77kmftp4bhnhsnn5r3odad[.]onion

Recent Breaches

https://www.test.gov
https://cvte.com
https://potomacfinancialpcg.com
https://asseco.com
https://racami.com
https://leovegasgroup.com
https://highwirepress.com
https://www.transsion.com
https://omnitracs.com
https://santillana.com
https://omnitracs.com
https://efi.com
https://ascom.com
https://onedealer.com

References

https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-hellcat-ransomware

https://www.scworld.com/brief/pilfered-jira-credentials-leveraged-in-hellcat-ransomware-attacks

https://www.sentinelone.com/blog/hellcat-and-morpheus-two-brands-one-payload-as-ransomware-affiliates-drop-identical-code/

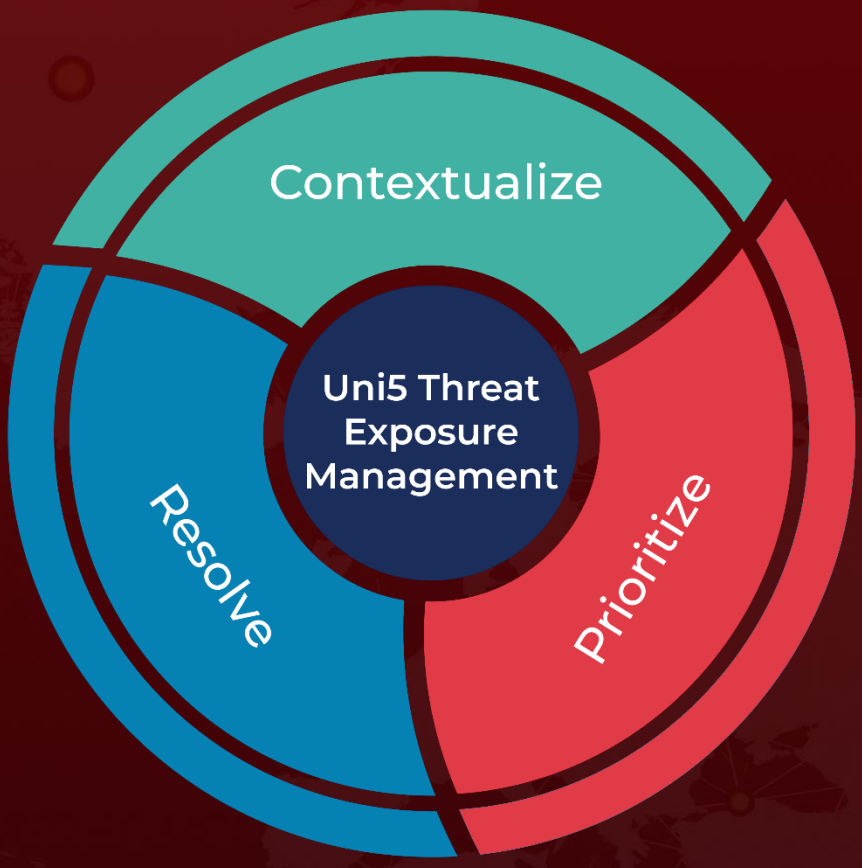
https://www.forbes.com/councils/forbestechcouncil/2025/03/26/decoding-hellcat-the-latest-nightmare-in-ransomware-attackers/

https://www.picussecurity.com/resource/blog/hellcat-ransomware

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

April 11, 2025 • 3:30 AM

More at www.hivepro.com