Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

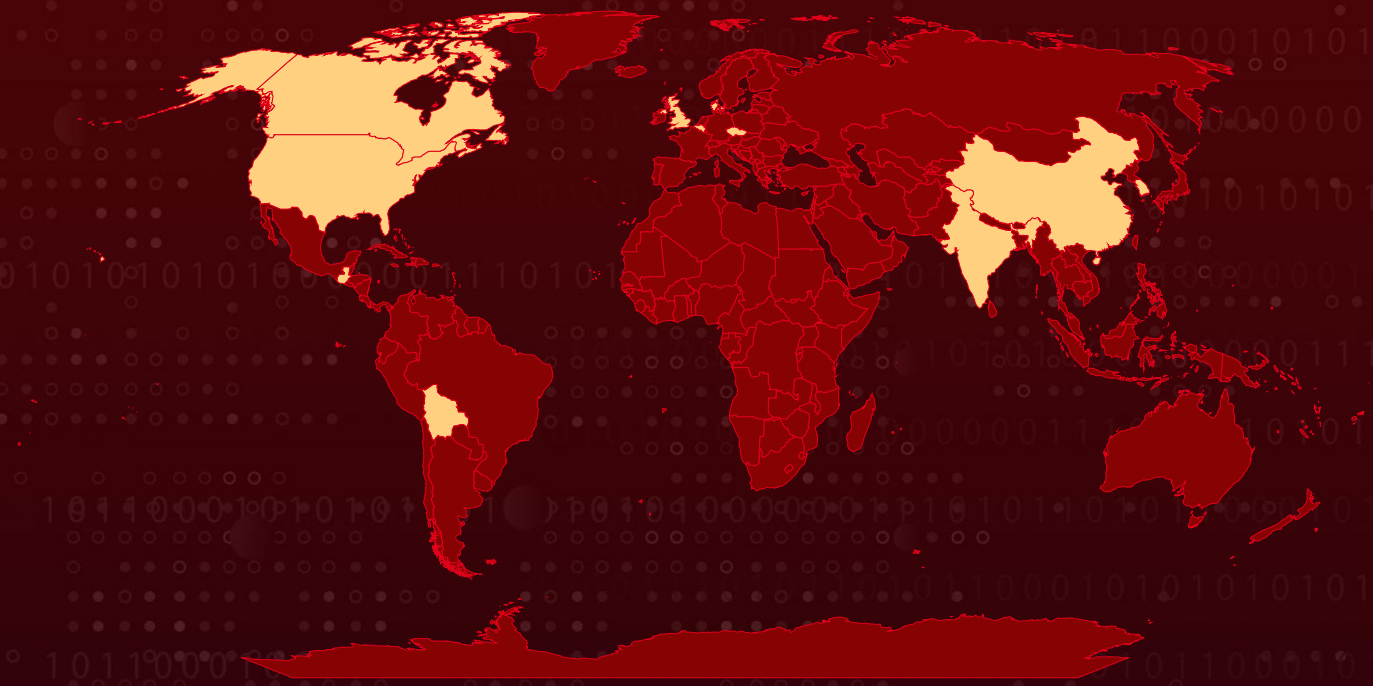
Tracking Beast: Tools, Techniques, and Tradecraft in RaaS Operations

Date of Publication	Admiralty Code	TA Number
March 27, 2026	A1	TA2026085

Summary

First Seen: March 2022
Targeted Regions: Belgium, Bolivia, Canada, China, Czechia, Denmark, Guatemala, India, South Korea, United Kingdom, United States
Targeted Platforms: Windows, Linux, VMware ESXi, Network Attached Storage (NAS)
Targeted Industries: Manufacturing, Business Services & Consulting, Education, Pharmaceutical, Healthcare, Aerospace, Defense, Transportation, Financial, Construction, Legal, Engineering, Real Estate, Heavy Equipment & Machinery, Government, Nonprofits, Medicine, IT, Insurance
Malware: Beast Ransomware
Attack: Beast is a Ransomware-as-a-Service (RaaS) platform whose affiliates gain initial access via phishing emails or compromised RDP endpoints, then deploy a curated toolkit for network reconnaissance, credential theft, lateral movement, and data exfiltration before encrypting files using Elliptic-curve and ChaCha20 algorithms. The group operates a Tor-based data leak site (BEAST LEAKS) to execute double extortion, threatening public exposure of stolen data unless ransom demands are met.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

Beast ransomware first appeared in March 2022 as an upgraded version of the earlier Monster ransomware. It operates as a Ransomware-as-a-Service (RaaS) platform, allowing affiliates to generate customized malware builds for Windows, Linux, and VMware ESXi environments. This flexibility enables attackers to tailor attacks to different infrastructures while maintaining a consistent core framework.

#2

Initial access is typically gained through phishing emails and exposed Remote Desktop Protocol (RDP) services. In several campaigns during 2024, attackers sent emails disguised as copyright complaints or job applications. Victims were directed to external download pages hosting compressed archives, often layered to avoid detection. Inside, the ransomware was hidden behind document-style icons to appear legitimate and increase the chance of execution.

#3

Once inside a system, Beast deploys environment-specific ransomware binaries generated through an offline builder, allowing the attack to proceed without an active command-and-control connection. The malware creates a mutex to prevent multiple instances from running and checks the victim's location, avoiding encryption on systems located in certain CIS countries. It then terminates active processes and services to ensure files can be encrypted without interference.

#4

Beast uses multithreaded encryption to speed up the process and secures files with a combination of elliptic-curve cryptography and ChaCha20. Encrypted files either receive a new extension or are placed into password-protected archives containing a ransom note, depending on the chosen configuration. Before launching the final encryption phase, attackers steal sensitive data to support double extortion. Stolen files are uploaded to cloud storage services using secure transfer tools.

#5

Victims are then threatened with a public data leak on the group's dedicated leak site, BEAST LEAKS, if payment is not made. To prevent recovery, Beast deletes shadow copies, disables backup features, and removes traces of its activity by clearing logs and deleting deployed tools. Finally, a ransom note is placed in affected directories, providing instructions for payment in exchange for a decryption key.

Recommendations

Harden RDP and Remote Access Exposure: Restrict RDP access to trusted IP ranges only, enforce multi-factor authentication (MFA) on all remote access solutions, and disable RDP entirely where it is not operationally required. Exposed RDP endpoints represent a primary initial access vector leveraged by Beast affiliates.

Disable WDigest Credential Caching: Enforce the registry setting HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential = 0 to prevent cleartext credentials from being stored in memory, directly countering the enable_dump_pass.reg-based credential harvesting technique used by Beast operators.

Protect Privileged Accounts and Service Credentials: Enforce the principle of least privilege across all accounts, restrict administrative access to dedicated workstations, and monitor for Kerberoasting indicators such as unusual LDAP queries for service accounts with Service Principal Names (SPNs). Rotate all service account passwords regularly.

Monitor and Restrict Lateral SMB Traffic: Enforce host-based firewalls to limit inbound and outbound SMB connections between endpoint systems. Deploy network detection rules to alert on anomalous internal SMB scanning activity, which is a reliable early indicator of Beast's self-propagation behavior.

Protect Volume Shadow Copies and Backup Infrastructure: Maintain offline, immutable backups of all critical systems and data, stored in a network segment not accessible from the primary environment. Monitor for WMI-based shadow copy enumeration and deletion queries (Select FROM Win32_ShadowCopy), and alert on any VSS deletion operations.

Restrict Cloud Storage Exfiltration Paths: Block unauthorized use of MEGASync and other cloud synchronization utilities through application control policies and firewall rules restricting outbound connections to Mega[.]nz. Establish DLP controls and monitor for anomalous data staging or large outbound transfer events preceding ransomware detonation.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
	T1133: External Remote Services	
	T1078: Valid Accounts	T1078.003: Local Accounts
		T1078.002: Domain Accounts
		T1078.001: Default Accounts
Execution	T1047: Windows Management Instrumentation	
	T1106: Native API	
Persistence	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1219: Remote Access Software	
Defense Evasion	T1036: Masquerading	T1036.001: Invalid Code Signature
	T1070: Indicator Removal	T1070.004: File Deletion
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
	T1620: Reflective Code Loading	
	T1055: Process Injection	
	T1112: Modify Registry	
Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
		T1003.005: Cached Domain Credentials

Tactic	Technique	Sub-technique
Credential Access	T1558: Steal or Forge Kerberos Tickets	T1558.003: Kerberoasting
Discovery	T1046: Network Service Discovery	
	T1083: File and Directory Discovery	
	T1135: Network Share Discovery	
	T1057: Process Discovery	
	T1016: System Network Configuration Discovery	
Lateral Movement	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
	T1569: System Services	T1569.002: Service Execution
Collection	T1119: Automated Collection	
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
	T1048: Exfiltration Over Alternative Protocol	T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Impact	T1486: Data Encrypted for Impact	
	T1489: Service Stop	
	T1490: Inhibit System Recovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	iplogger[.]co/1v1i85[.]torrent
Filenames	Advanced_IP.exe, Advanced_Port_Scanner_2.5.3869.exe, AnyDesk.exe, automim.rar, CleanExit.exe, comands.bat, dell%20logs.cmd, delllogs.cmd, disable_backup.bat, enable_dump_pass.reg, encrypter-linux-x64.run, encrypter-linux-x86.run, encrypter-windows-cli-x86.exe, encrypter-windows-gui-x86.%E2%80%A2xe, Everything.exe, FolderSize-2.6-x64.msi, Kerberos.ps1, klink.exe, klink27.bat, lazagne.bat, LaZagne.exe, laZagne_x86.exe, libcrypto.dll, log.ps1, low.exe, low64.exe, MEGAsyncSetup64.exe, mimikatz.exe, netscan.exe, netscan.msi, netscan.rar, netscan.xml, netscan.xml.exe, netscanold.exe, netscanold.xml, OpenSSH-Win32/, Pass-The-Hash_RDP.bat, PsExec.exe, runPsE.bat,

TYPE	VALUE
Filenames	ssh.exe, TimeoutRun.bat, Un.exe, unins000%20-%20Atalho.lnk, winrar-x64-701.exe, WinSCP-6.5.3-Setup.exe
IPv4	5[.]78[.]84[.]144
SHA256	6718cb66521a678274e5672285bf208eac375827d622edcf1fe7eba7e7aa65e0, 479d0947816467d562bf6d24b295bf50512176a2d3d955b8f4d932aea2378227, cc0680de960f3e1b727b61a42e59f9c282bd8e41fe20146ed191c7f4bf9283a7, cf5c45be416d1b18dd67ffa95c6434691f1f9ba9c30754fa6fc9978c1f975750, 2ce62601491549ab91c9517e0accf3286ed29976f6ec359d31ddc060a8d99eb3, 812df0efea089b956d08352ff0a7e8789d43862dc3764f4441d4e1c1d1fb7957, 5bd8f9cbd108abc53fb1c44b8d10239a2a0a9dd20c698fd2fb5dc1938ae7ba96, 4c44ac1eea4bc7f4ea542d611b5658d7ac2729d79abe750da83f1581cd832eaf, 369034bf1d793fe56ea4d683a156722d825ad9829fc128117f82a26bc1d0480b, e01f5c7067dc984dceb883b10444b1a5b0f22ebd500baf9d9a88207f5033285d, dd09a2ef31d018fd83f186e3eaaccccdaa8a8c8779ced668abb06dc934d89a2d, dbbe792e6c804518909f8990a836552573522d126547429d6cd3fcb1f60d542c, e5aaa213818fe835f2716914238119fee746753aa4808e24aed817e929e6dcb8
TOR Address	beast6azu4f7fxjakiayhnssybibsgjnmy77a6duufqw5afjzfjhzuqd[.]onion

Recent Breaches

https://www.communicateuk.co.uk/
https://www.trinitycatholichs.org/
https://www.drkaler.com/
http://www.yulkok.com/index.do
https://www.ruskin.ac.uk/
https://www.sta-worthing.com/
https://www.orthospecialistsma.com/
https://commercialpaving.ca/
https://colletthulance.co.uk/
https://www.r-alibon.bardaglea.org.uk/
https://www.first4-recruitment.com/
https://www.idealforwarding.co.uk/

References

https://www.team-cymru.com/post/beast-ransomware-server-toolkit-analysis

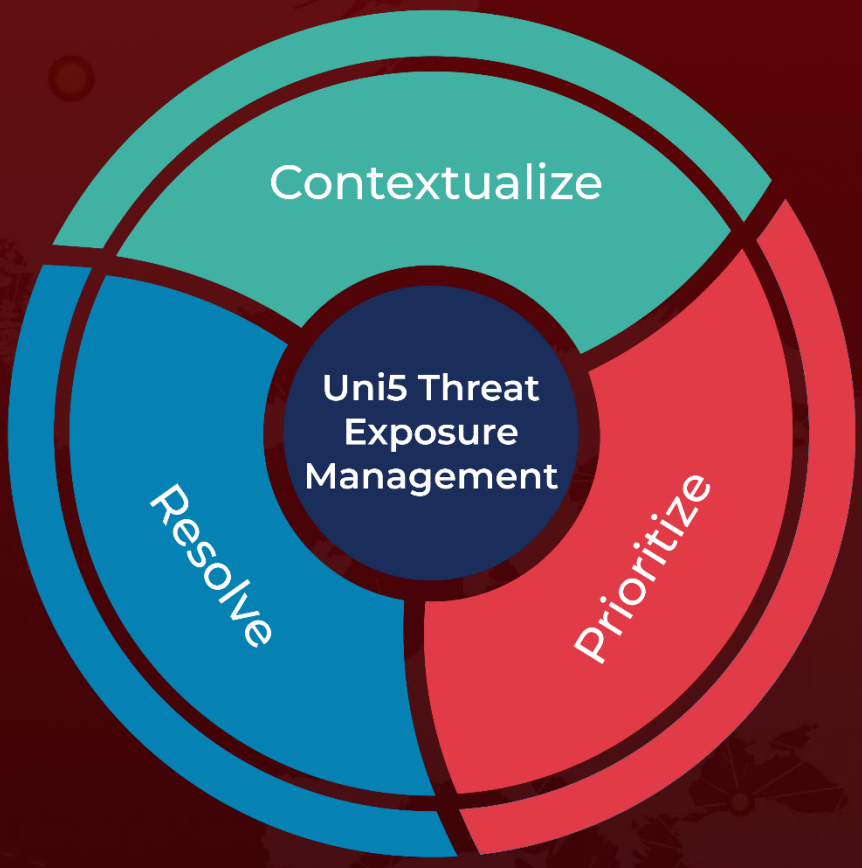
https://www.cybereason.com/blog/threat-analysis-beast-ransomware

https://socradar.io/blog/dark-web-profile-beast-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

March 27, 2026 • 07:30 AM

More at www.hivepro.com