

A Proactive Threat Intelligence Report

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

Team Cymru

April 8, 2025

BLOG

The Beast Returns: Analysis of a Beast Ransomware Server

By Will Thomas – Senior Threat Intelligence Advisor

Team Cymru analyzes and collects a wide variety of internet telemetry. This includes global NetFlow communications and open ports data, among other types of data such as X509 certificates, passive DNS, and WHOIS records.

While other organisations attempt to scan the entire Internet or guess which ports are statistically likely to be listening, our Open Ports data collection leverages Team Cymru’s unique NetFlow visibility to prioritize and perform targeted scans of hosts that are actively communicating. By filling in the known gaps, Team Cymru’s informed scanning enables faster discovery of live assets and operational infrastructure.

Overall, Team Cymru’s NetFlow visibility allows our open ports collection system to know where the connections and communications are happening and allows us to send just the right number of packets to validate listening services and make them available to users of Scout and Recon.

About Beast Ransomware

According to open source [reports](#), Beast is a Ransomware-as-a-Service (RaaS) that was first promoted on the underground forum RAMP in June 2024. Beast ransomware is [reportedly](#) the successor to Monster ransomware which was also offered on RAMP in March 2022. In August 2024, an offline builder for Beast ransomware was promoted with the option to configure builds for Windows systems, network attached storage (NAS) devices, and VMware ESXi hypervisors. Beast also specifically avoids encrypting data on devices located in Commonwealth of Independent States (CIS) countries, such as Russia, Belarus, and Moldova.

Based on an analysis of the BEAST LEAKS Tor data leak site by [RansomLook](#), Beast ransomware operations paused in November 2025 and resumed in January 2026. The operators have been fairly active, posting several victims to their leak site, during February to March 2026. At the time of writing, they appear to be continuing their operations.

Identification of a Beast Ransomware Server

In March 2026, Team Cymru detected an Open Directory on 5.78.84[.]144 hosted at AS212317. Using Team Cymru’s NetFlow-augmented Open Ports collection, we detected a list of notable file names running on Port 8000. Analysis of the file names revealed on the Beast operator’s server enabled us to understand the flow of their attacks from start, to middle, to the end.

Port	First Seen ↓	Last Seen ↓	Count ↓	Proto	Service	Banner ↓
> 8000	2026-03-11	2026-03-11	2	TCP	HTTP.TITLE	Directory listing for /
> 8000	2026-03-11	2026-03-11	2	TCP	HTTP.SERVER	SimpleHTTP/0.6 Python/3.9.2
> 8000	2026-03-11	2026-03-11	1	TCP	HTTP.OPENDIR	# Request Path:/ Directory Listing: Advanced_IP.exe Advanced_Port_Scanner_2.5.3869.ex...

Figure 1. A screenshot from Scout’s Open Ports Tab for 5.78.84[.]144.

Analysis of a Beast Operator's Toolkit

Through Team Cymru's collection system, we acquired the files from the server and analysed them. The files allowed us to break down the different stages of an intrusion by a Beast ransomware operator.

Reconnaissance & Network Mapping

Firstly, ransomware operators need to know where the high-value data lives before they encrypt it and hold it for ransom. In the Open Directory were copies of Advanced IP Scanner and Advanced Port Scanner. These are legitimate tools often deployed by ransomware groups to map internal networks and find open remote desktop protocol (RDP) or server message block (SMB) ports. We also uncovered Everything.exe, a fast file search engine that ransomware operators use to quickly locate sensitive files for exfiltration. Another file, FolderSize-x64, is used by Beast operators to identify which servers hold the most data, helping the attacker prioritize which machines to encrypt first for maximum impact.

Credential Theft

To move laterally and get to their goal of Domain Admin rights over the target network, they need passwords and credentials. Copies of Mimikatz, LaZagne, and Automim were identified on the server, the gold standard for dumping passwords from memory and recovering stored passwords from browsers, databases, and email clients. Another tool called enable_dump_pass.reg was uncovered too, which is a registry modification that forces Windows to store passwords in cleartext in memory (WDigest), making them harvestable by Mimikatz. Another script was found called Kerberos.ps1 that was likely used for Kerberoasting, whereby the attackers can extract service account tickets to crack them offline.

Persistence

Once they have credentials, they need to move laterally. A copy of AnyDesk was stored on the server, a well known remote monitoring and management (RMM) tool used by a plethora of ransomware groups, including the most notorious like Qilin and Akira. It is useful for these adversaries due to antivirus and endpoint detection and response (EDR) systems not usually blocking it as malicious by default. It can therefore persist undetected on target systems.

Lateral Movement

To execute commands remotely and access systems across the network, the server had a copy of PsExec, a well-known Windows SysInternals tool, also used by many ransomware groups to spread inside a target environment. A copy of OpenSSH for Windows was also found on the server, which can be used by the attackers to create secure tunnels for remote access.

Exfiltration

Before encrypting, Beast ransomware operators will steal data to threaten the victim with a public leak via its Tor data leak site called BEAST LEAKS. To be able to steal the data, the Beast operator used MEGASync, another well-known tool used by many ransomware gangs. MEGASync works with Mega[.]nz and can be used to upload hundreds of Gigabytes of stolen data due to it being able to handle large volumes of data. The Beast operator was also using WinSCP and Klink too, which can be used to exfiltrate data via secure file transfer protocol (SFTP) and other protocols.

Impact

Perhaps the most interesting discovery from the Beast ransomware server were the files from the final stages of an attack. One file, called “disable_backup.bat”, is a batch script designed to delete Volume Shadow Copies (VSS) and disable Windows backups. This ensures the victim cannot simply restore their files after the attack. Another file called “CleanExit.exe” is likely a tool used by the Beast operator to wipe logs and their tools after the encryption is triggered, making forensic recovery harder.

Two standout file names are “encrypter-windows-cli-x86.exe” and “encrypter-linux-x64.run”, as these are the actual Beast ransomware binaries. The presence of both Windows and Linux (.run) versions of Beast ransomware suggests the targeting of both workstations and Linux Servers on VMware ESXi hypervisors.

Conclusion

The analysis of the Beast ransomware server successfully identified a wide array of tools used by the operators, providing a detailed breakdown of their tactics across the entire intrusion lifecycle. This further shows that through proactive collection of internet telemetry, we can identify a ransomware operator's entire toolkit before it can be used against its targets. This directly feeds into proactive defensive strategies.

Further, many of the tools stored on the Beast ransomware server are listed in the Ransomware Tool Matrix (see [here](#)), which is an open source knowledge base. It can be used by threat intelligence and threat hunting teams to track what tools are used by ransomware groups to help focus on what to block, detect, and hunt for in their environments.

Beast Ransomware Tool Matrix

Discovery	RMM Tools	Credential Theft	Networking	LOLBAS	Exfiltration
Advanced IP Scanner	AnyDesk	Automim	Klink	PsExec	MEGA
Advanced Port Scanner		LaZagne	OpenSSH		WinSCP

Discovery	RMM Tools	Credential Theft	Networking	LOLBAS	Exfiltration
Everything.exe		Mimikatz			
SoftPerfect NetScan					

Indicators of Compromise (IOCs)

Indicator	Description	ASN	Organization	GeoIP	Last Seen
5.78.84[.]144	Beast Ransomware Open Directory	AS212317	Hetzner	US	11 March 2026

Beast Ransomware SHA256 file hashes gathered from open source malware sandbox submissions:

6718cb66521a678274e5672285bf208eac375827d622edcf1fe7eba7e7aa65e0

479d0947816467d562bf6d24b295bf50512176a2d3d955b8f4d932aea2378227

cc0680de960f3e1b727b61a42e59f9c282bd8e41fe20146ed191c7f4bf9283a7

cf5c45be416d1b18dd67ffa95c6434691f1f9ba9c30754fa6fc9978c1f975750

2ce62601491549ab91c9517e0accf3286ed29976f6ec359d31ddc060a8d99eb3

812df0efea089b956d08352ff0a7e8789d43862dc3764f4441d4e1c1d1fb7957

5bd8f9cbd108abc53fb1c44b8d10239a2a0a9dd20c698fd2fb5dc1938ae7ba96

Full List of Open Directory File Names:

Advanced_IP.exe

Advanced_Port_Scanner_2.5.3869.exe

AnyDesk.exe

automim.rar

CleanExit.exe

comands.bat

dell%20logs.cmd

dellogs.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

runPSEXEC.bat

ssh.exe

TimeoutRun.bat

Un.exe

unins000%20-%20Atalho.lnk

winrar-x64-701.exe

WinSCP-6.5.3-Setup.exe

[Threat Actor, Campaign & Infrastructure Intelligence](#)

[Threat Intelligence Analyst](#)

[SOC Manager](#)

[Threat Reconnaissance](#)

[Infrastructure Attribution](#)

[Lateral Movement Detection](#)

[Ransomware](#)

[Malicious Infrastructure](#)

[Compromised Hosts](#)

[Proactive Threat Hunting Tools](#)

[Threat Research](#)

The latest articles straight to your inbox
