THREAT ANALYSIS: Beast Ransomware

By Cybereason Security Services Team

Archived: 2026-04-06 00:19:42 UTC

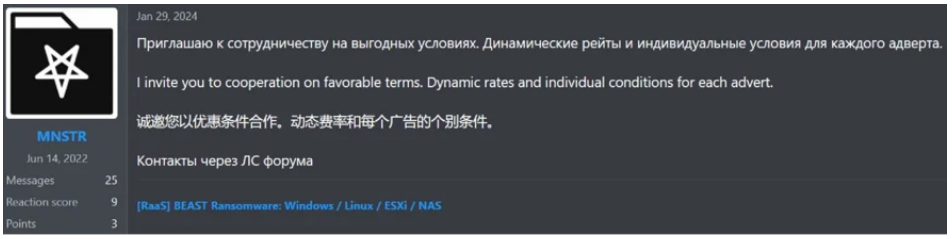
Cybereason issues Threat Analysis reports to investigate emerging threats and provide practical recommendations for protecting against them. In this Threat Analysis report, Cybereason investigates the Ransomware-as-a-Service (RaaS) known as Beast and how to defend against it through the Cybereason Defense Platform.

KEY POINTS

- **Expanding Marketplace:** The Beast Ransomware group provides various tools with constant version updates. These updates are made to appeal to wider audiences across the underground cybercrime ecosystem.
- **Binary Customizations:** The Beast RaaS platform offers affiliates numerous options for building ransomware binaries that target Windows, Linux, and ESXi systems, enabling tailored configurations to suit different operational requirements.
- **Detection And Prevention:** The Cybereason Defense Platform employs advanced Anti-Ransomware and Anti-Malware features, designed to detect and block ransomware payloads like Beast before they can execute.

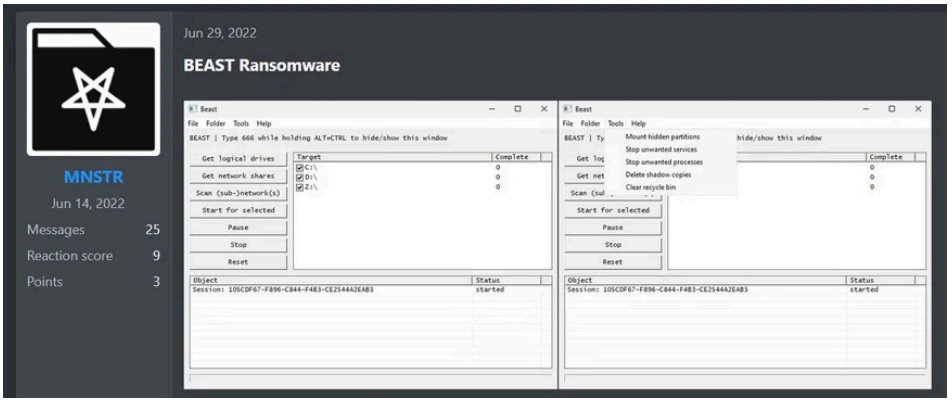
INTRODUCTION

The Beast Ransomware group has been active since 2022. Recently, a Beast Ransomware partnership program and new capabilities were promoted on the underground forums in June. The group has updated and created various versions to meet the market demand.



Invitation to cooperate in Russian, English and Chinese languages.

Previous versions of the Beast Ransomware, also known as Monster, were developed using the Delphi programming language and offered as a Ransomware-as-a-Service (RaaS) platform.



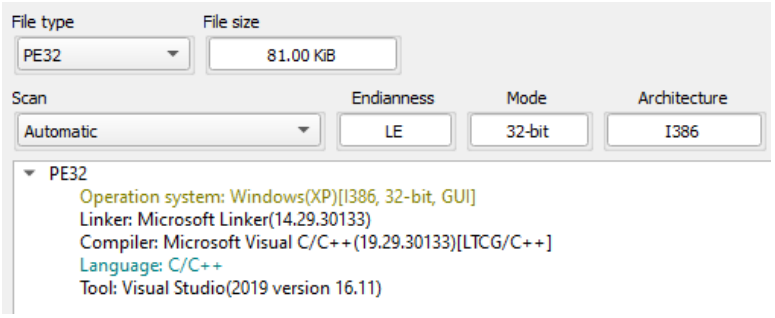
First Appearance Of Beast Ransomware On The Russian Anonymous Marketplace

TECHNICAL ANALYSIS

Beast Operating System Support – Windows

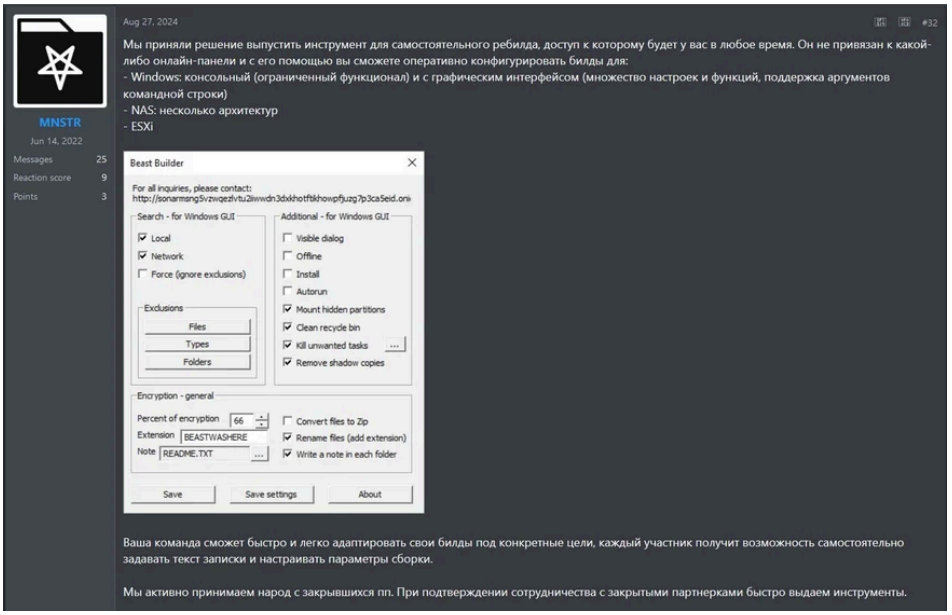
The current known Windows versions of Beast demonstrate the following capabilities:

- Combination of Elliptic-curve and ChaCha20 encryption model
- Written in the C programming language



Beast Windows Binary

- Segmented file encryption
- ZIP wrapper mode - Files are converted on the fly to *.zip* with ransom note inside
- Multithreaded queue for encryption
- Processes/Services termination
- Shadow copy delete
- Mounting hidden partitions
- Subnet scanner
- In August 2024, offline builder was promoted with option to configure builds for Windows, NAS, ESXi.



New Beast Offline Builder

Beast Operating System Support – Linux And ESXi

The Beast Linux version has the following capabilities (controllable via command line argument):

- Selectable path for encryption
- Enable/disable certain functionality
- Ransom note generation from external file
- Daemon mode
- Written in C and Go programming languages

The VMWare ESXi version also has the following additional options:

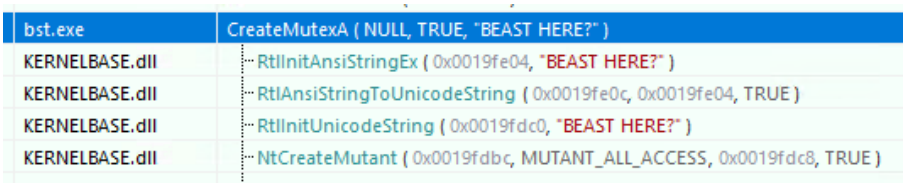
- Option to shut down a VM and machine's files encryption
- Option to exclude some *vmid*

Linux & ESXi Version Parameters

Binary Analysis - BEAST HERE?

Like most ransomware, the initial compromise often occurs through various infection vectors, such as phishing emails, or compromised remote desktop protocol (RDP) endpoints.

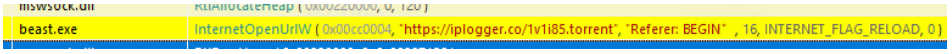
To prevent multiple instances of Beast running simultaneously on the same system, it creates a unique mutex with the string “BEAST HERE?”. This ensures efficient execution and enables the attacker to maintain control over the ransomware’s behavior on the infected system.



Beast Creates A Mutex Object With BEAST HERE? String

The latest version of Beast Ransomware specifically avoids encrypting data on devices located in Commonwealth of Independent States (CIS) countries, such as Russia, Belarus, and Moldova. This is achieved through code that checks the system's default language settings, country code, and retrieves the target's IP address.

If the ransomware detects that the device is in a CIS country, it halts encryption activities. This strategic exclusion is likely a tactic to avoid drawing attention or repercussions from authorities in those regions.



Checking Victim IP & Location By Connecting To iplogger.co

Beast performs SMB scans to automatically search for and infect vulnerable computers on nearby networks. This self-propagation mechanism can quickly spread the payload without requiring any human intervention.

```
beast.exe (3840) requested TCP 10.0.2.4:445
System (4) requested TCP 10.0.2.2:445
  0000: 00 00 00 45 FF 53 4D 42 72 00 00 00 00 18 53 C8  ...E.SMBr.....S.
  0010: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE  ................
  0020: 00 00 00 00 00 22 00 02 4E 54 20 4C 4D 20 30 2E  .....".."NT LM 0.
  0030: 31 32 00 02 53 4D 42 20 32 2E 30 30 32 00 02 53  12..SMB 2.002..S
  0040: 4D 42 20 32 2E 3F 3F 3F 00                       MB 2.???.
System (4) requested TCP 10.0.2.3:445
  0000: 00 00 00 45 FF 53 4D 42 72 00 00 00 00 18 53 C8  ...E.SMBr.....S.
  0010: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE  ................
  0020: 00 00 00 00 00 22 00 02 4E 54 20 4C 4D 20 30 2E  .....".."NT LM 0.
  0030: 31 32 00 02 53 4D 42 20 32 2E 30 30 32 00 02 53  12..SMB 2.002..S
  0040: 4D 42 20 32 2E 3F 3F 3F 00                       MB 2.???.
  0000: 00 00 00 45 FF 53 4D 42 72 00 00 00 00 18 53 C8  ...E.SMBr.....S.
svchost.exe (2336) requested UDP 8.8.8.8:53
  0010: 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FE  ................
  0020: 00 00 00 00 00 22 00 02 4E 54 20 4C 4D 20 30 2E  .....".."NT LM 0.
  0030: 31 32 00 02 53 4D 42 20 32 2E 30 30 32 00 02 53  12..SMB 2.002..S
Received A request for domain 'iplogger.co'.
  0040: 4D 42 20 32 2E 3F 3F 3F 00                       MB 2.???.
```

Beast SMB Scanning

Load Of RstrtMgr DLL (Restart Manager)

RstrtMgr.dll, the Restart Manager, is a critical system component that safeguards open and unsaved files during system reboots. It acts as a gatekeeper, prompting users to save their work before shutting down to prevent data loss. Beast Ransomware exploits this DLL in a malicious way.

Before encrypting a file, the ransomware stops services and processes in order to unlock and safely close open files.

```
beast.exe    InitializeCriticalSection ( 0x003c3518 )
beast.exe    LoadLibraryA ( "RstrtMgr.dll" )
```

```
RstrtMgr.dll    RegOpenKeyExW ( HKEY_LOCAL_MACHINE, "System\CurrentControlSet\Control", 0, KEY_QUERY_VALUE, 0x0019f7a4 )
RstrtMgr.dll    RegQueryValueExW ( 0x000002c0, "WaitToKillServiceTimeout", NULL, 0x0019f7a8, NULL, 0x0019f7b0 )
RstrtMgr.dll    memset ( 0x0019f7b4, 0, 64 )
RstrtMgr.dll    RegQueryValueExW ( 0x000002c0, "WaitToKillServiceTimeout", NULL, 0x0019f7a8, 0x0019f7b4, 0x0019f7b0 )
RstrtMgr.dll    wcstoul ( "5000", 0x0019f7a0, 10 )
RstrtMgr.dll    RegCloseKey ( 0x000002c0 )
RstrtMgr.dll    RegOpenKeyExW ( HKEY_LOCAL_MACHINE, "Software\Microsoft\RestartManager", 0, KEY_QUERY_VALUE, 0x0019f7a4 )
RstrtMgr.dll    RegOpenKeyExW ( HKEY_LOCAL_MACHINE, "Software\Microsoft\RestartManager", 0, KEY_QUERY_VALUE, 0x0019f7a4 )
```

The list of services targeted by Beast Ransomware is as following:

```
beast.exe    OpenServiceW ( 0x0748c318, "AcronisAgent", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "AcrSch2Svc", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "backup", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "BackupExecAgentAccelerator", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "BackupExecAgentBrowser", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "BackupExecDiveciMediaService", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "BackupExecJobEngine", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "BackupExecManagementService", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "BackupExecRPCService", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "BackupExecVSSProvider", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "CAARCUpdateSvc", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "CASAD2DWebSvc", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "ccEvtMgr", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "ccSetMgr", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "DefWatch", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "GxBlr", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "GxCIMgr", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "GxCVD", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "GxFWD", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "GxVss", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "Intuit.QuickBooks.FCS", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "memtas", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "mepocs", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "msexchange", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "PDVFSService", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "QBCFMonitorService", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "QBFCService", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "QBIDPService", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "RTVscan", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "SavRoam", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
beast.exe    OpenServiceW ( 0x0748c318, "sophos", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP )
```

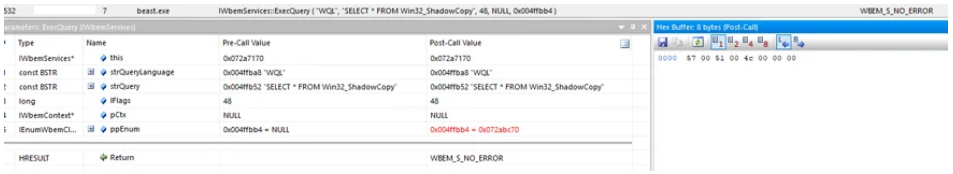
beast.exe	OpenServiceW (0x0748c318, "YooBackup", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "YooIT", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "zhudongfangyu", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQLFDLauncher", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQLSERVER", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLSERVERAGENT", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLBrowser", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLTELEMETRY", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MsDtsServer130", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SSISTELEMETRY130", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLWriter", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQL$VEEAMSQL2012", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLAgent$VEEAMSQL2012", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQL", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLAgent", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQLServerADHelper100", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQLServerOLAPService", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MsDtsServer100", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "ReportServer", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLTELEMETRY$HL", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "TMBMServer", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQL$PROGID", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQL$WOLTERSKLUWER", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLAgent$PROGID", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLAgent$WOLTERSKLUWER", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQLFDLauncher$OPTIMA", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "MSSQL$OPTIMA", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "SQLAgent$OPTIMA", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "ReportServer$OPTIMA", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "msftesql$SQLEXPRESS", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)
beast.exe	OpenServiceW (0x0748c318, "postgresql-x64-9.4", SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS | SERVICE_STOP)

List of services targeted by Beast Ransomware

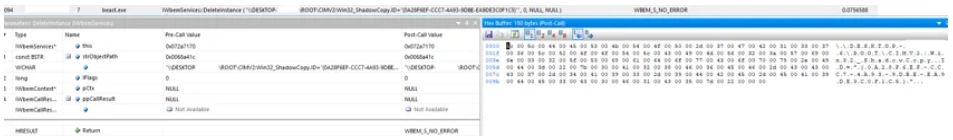
AcronisAgent	BackupExecDiveciMediaService	CAARCUpdateSvc	GxBlr	Intuit.Qu
AcrSch2Svc	BackupExecJobEngine	CASAD2DWebSvc	GxClMgr	Memtas
Backup	BackupExecManagementService	ccEvtMgr	GxCVD	Mepocs
BackupExecAgentAccelerator	BackupExecRPCService	ccSetMgr	GxFWD	Msexcha
BackupExecAgentBrowser	BackupExecVSSProvider	DefWatch	GxVss	PDVFSS
VeeamDeploymentService	VeeamNFSSvc	VeeamTransportSvc	VSNAPVSS	Vss
YooBackup	YooIT	Zhudongfangyu	MSSQLFDLauncher	MSSQLS
SQLTELEMETRY	MsDtsServer130	SSISTELEMETRY130	SQLWriter	MSSQL$
SQLAgent	MSSQLSERVERADHelper100	MSSQLServerOLAPService	MsDtsServer100	ReportSe
MSSQL$PROGID	MSSQL$WOLTERSKLUWER	SQLAgent$PROGID	SQLAgent$WOLTERSKLUWER	MSSQLF
ReportServer$OPTIMA	msftesql$SQLEXPRESS	Postgresql-x64-9.4	SavRoam	Wscsvc
SQLTELEMETRY$HL	MSSQL$OPTIMA	SQLSERVERAGENT	SQLAgent$VEEAMSQL2012	SQLAge
Veeam	Wuauserv	SQLBrowser	MSSQL	TMBMS

Shadow Copy Delete

When Shadow Copy delete process is initiated by Beast Ransomware, it calls the **IWbemServices::ExecQuery("WQL", "Select * FROM Win32_ShadowCopy")**WQL query to get the **IEnumWbemClassObject** object for querying shadow copies and **IWbemServices::DeleteInstance("\\MachineName\ROOT\CIMV2:Win32_ShadowCopy.ID="{Shadow Copy ID}"")** to delete them.



Beast Querying Shadow Copies



Beast Deleting Shadow Copies

File Encryption

Ransomware often employs multithreading to accelerate file encryption.

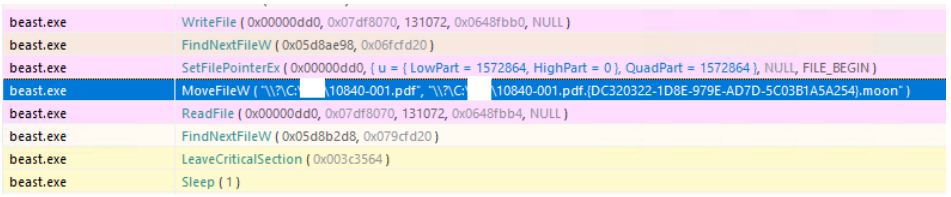
This technique involves the parent thread identifying and sending files for encryption to child threads.

The child threads then work concurrently, each encrypting a different file, significantly speeding up the overall encryption process. This approach leverages the system's hardware capabilities to encrypt files more efficiently.

Beast Ransomware Threads (demonstrating multithreading usage)

Beast uses powerful encryption methods to lock down files on all connected devices in a network. It targets a variety of file formats, such as documents, pictures, videos, and databases.

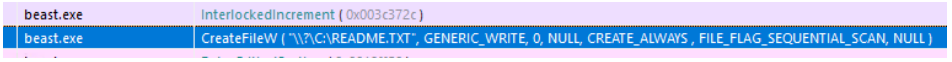
Once files are encrypted, victims can't access them unless they have the decryption key, which is controlled by the attackers.



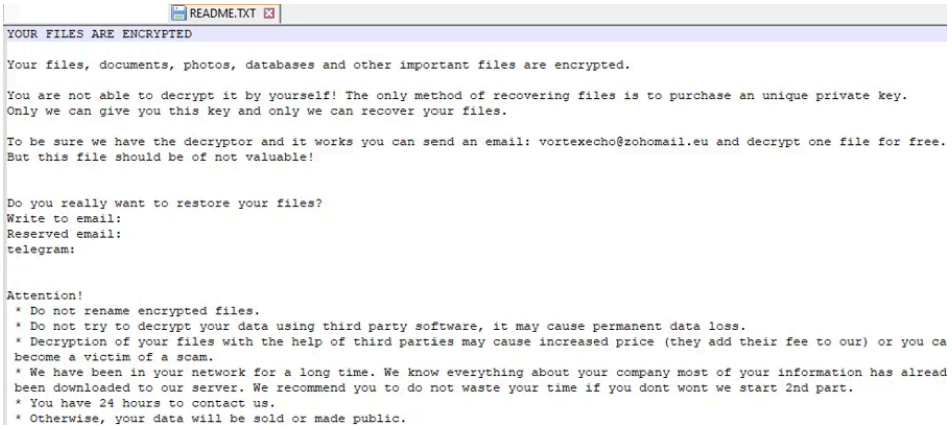
PDF File Encryption Process Example

Encrypted Files

The ransom note thread extracts and decodes the embedded ransom note, which was specified in the malware's settings. This note is then saved as a "README.txt" file in every directory that isn't explicitly excluded from encryption.



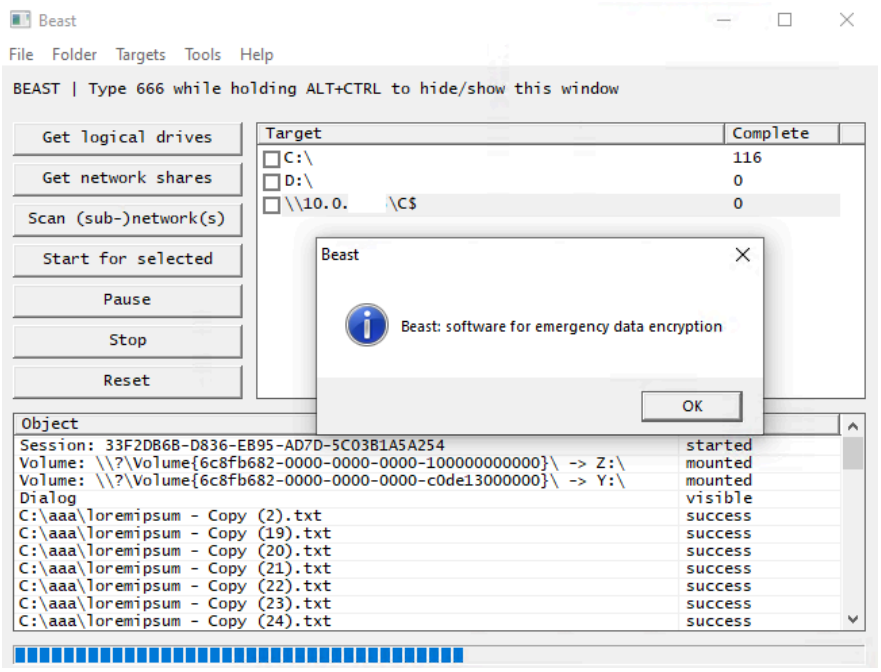
Creation Of The Ransom Note README.txt


README.TXT

```
YOUR FILES ARE ENCRYPTED

Your files, documents, photos, databases and other important files are encrypted.

You are not able to decrypt it by yourself! The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.

To be sure we have the decryptor and it works you can send an email: vortexecho@zohomail.eu and decrypt one file for free.
But this file should be of not valuable!


Do you really want to restore your files?
Write to email:
Reserved email:
telegram:


Attention!
 * Do not rename encrypted files.
 * Do not try to decrypt your data using third party software, it may cause permanent data loss.
 * Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you ca
become a victim of a scam.
 * We have been in your network for a long time. We know everything about your company most of your information has alread
been downloaded to our server. We recommend you to do not waste your time if you dont wont we start 2nd part.
 * You have 24 hours to contact us.
 * Otherwise, your data will be sold or made public.
```

Ransom Note

In order to see Beast Ransomware GUI during the encryption process, it is needed to press and hold ALT+CTRL and type ***666***:



Beast Ransomware GUI

Indicators of Compromise - IOCs

Cybereason shared a list of indicators of compromise related to this research :

IOC	IOC type	Description
iplogger[.]co/1v1i85[.]torrent	Domain Name	Geofencing IP query
4c44ac1eea4bc7f4ea542d611b5658d7ac2729d79abe750da83f1581cd832eaf	SHA-256	Beast Windows Encryptor
369034bf1d793fe56ea4d683a156722d825ad9829fc128117f82a26bc1d0480b	SHA-256	Beast Windows Encryptor
e01f5c7067dc984dceb883b10444b1a5b0f22ebd500baf9d9a88207f5033285d	SHA-256	Beast Windows Encryptor
dd09a2ef31d018fd83f186e3eaaccccdaa8a8c8779ced668abb06dc934d89a2d	SHA-256	Beast Windows Encryptor
dbbe792e6c804518909f8990a836552573522d126547429d6cd3fcb1f60d542c	SHA-256	Beast Windows Encryptor

Cybereason Recommendations:

- Follow and hunt Beast affiliate activity in order to identify pre-ransomware behaviors.
- Promote cybersecurity best practices such as multifactor authentication and patch management.
- For Cybereason customers on the Cybereason Defense Platform:
  - Enable Anti-Malware and set the Anti-Malware > Signatures mode to Prevent, Quarantine, or Disinfect.
  - Enable Anti-Ransomware (PRP), set Anti-Ransomware to Quarantine mode and enable shadow copy protection.

- Enable Application Control.
- Keep systems fully patched: Make sure your systems are patched in order to mitigate vulnerabilities.
- Regularly backup files and create a backup process and policy : Restoring your files from a backup is the fastest way to regain access to your data.
- Enable Variant Payload Prevention with prevent mode on Cybereason Behavioral execution prevention.

MITRE ATT&CK MAPPING

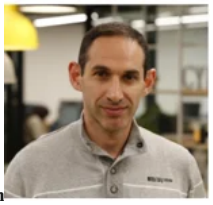
Tactic	**Techniques / Sub-Techniques**
TA0002: Execution	T1047 – Windows Management Instrumentation
TA0002: Execution	T1106 - Native API
TA0003: Persistence	T1543.003 – Create or Modify System Process: Windows Service
TA0007: Discovery	T1083 - File and Directory Discovery
TA0004: Privilege Escalation	T1078.001 – Valid Accounts: Default Accounts
TA0004: Privilege Escalation	T1078.002 – Valid Accounts: Domain Accounts
TA0007: Discovery	T1135 - Network Share Discovery
TA0007: Discovery	T1016 - System Network Configuration Discovery
TA0005: Defense Evasion	T1406.002 – Obfuscated Files or Information: Software Packing
TA0005: Defense Evasion	T1620 - Reflective Code Loading
TA0008: Lateral Movement	T1021.002 - Remote Service: SMB/Windows Admin Shares
TA0009: Collection	T1119 – Automated Collection
TA0040: Impact	T1486 - Data Encrypted for Impact
TA0040: Impact	T1489 – Service Stop
TA0040: Impact	T1490 – Inhibit System Recovery

References

https://blogs.blackberry.com/en/2022/09/some-kind-of-monster-raas-hides-itself-using-traits-from-other-malware

https://cyberint.com/blog/research/the-nature-of-the-beast-ransomware/

ABOUT THE RESEARCHER



Mark Tsipershtein, Security Researcher at Cybereason

Mark Tsipershtein, a security researcher at the Cybereason Security Research Team, focuses on research, analysis automation and infrastructure. Mark has more than 20 years of experience in SQA, automation, and security research.

Cybereason is dedicated to teaming with Defenders to end cyber attacks from endpoints to the enterprise to everywhere. Learn more about Cybereason XDR powered by Google Chronicle as well as Cybereason SDR, check out our Extended Detection and Response (XDR) Toolkit, or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.