

# Cybereason vs. RansomEXX Ransomware

By Cybereason Nocturnus

Archived: 2026-04-05 17:12:58 UTC

Over the last few months, the [Cybereason Nocturnus Team](#) has been tracking the activity around the [RansomEXX](#) ransomware. It has been active since 2018, but came to fame in 2020 in attacks on major organizations such as the Texas Department of Transportation. RansomEXX started as a Windows variant, but a [Linux variant](#) was discovered earlier this year.

## Key Findings

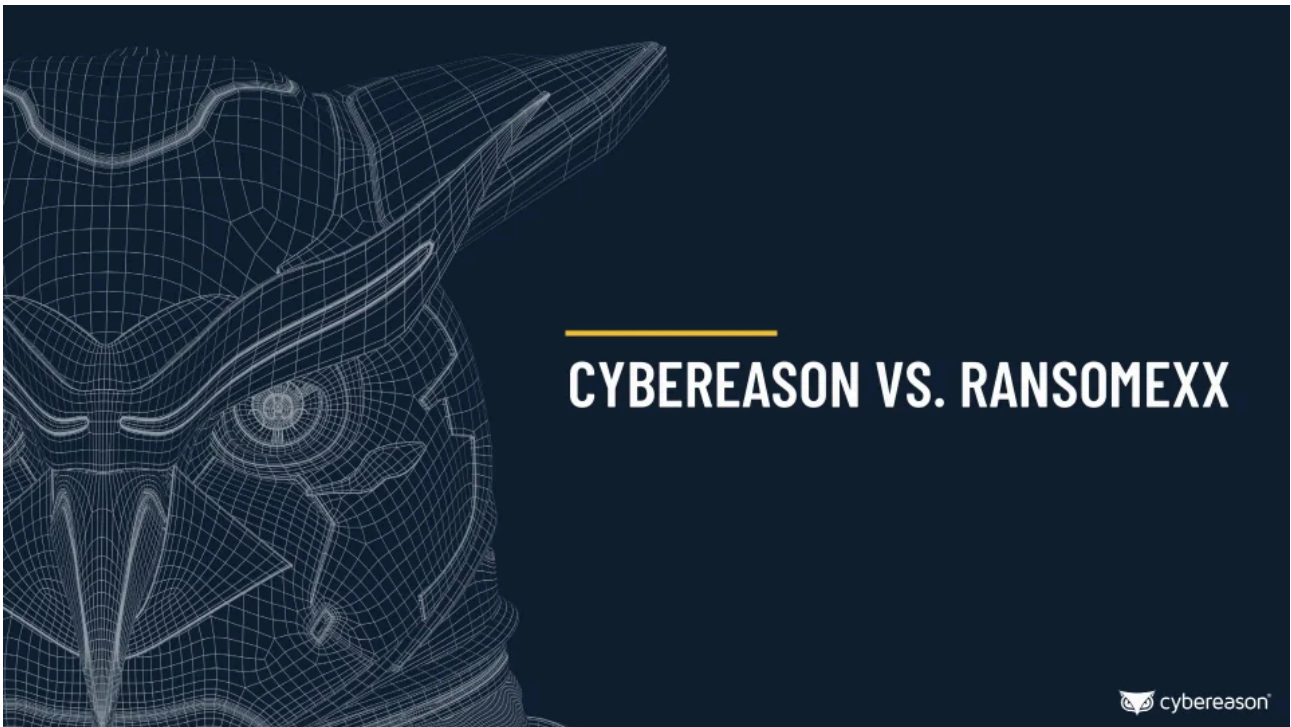
**Human-operated targeted attacks:** RansomEXX is being used as a part of multi-staged human-operated attacks targeting various government related entities and tech companies. It is being delivered as a secondary payload after initial compromise of the targeted network.

**Disables security products:** The Windows variant has a functionality that was [seen before](#) in other ransomware, disabling various security products for a smooth execution on the infected machine.

**Multi-Platform:** RansomEXX started solely as a Windows variant, but later a Linux variant was added to the arsenal, sharing similarities with its predecessor.

**Fileless ransomware:** RansomEXX is usually delivered as a secondary in-memory payload without ever touching the disk, which makes it harder to detect.

**Detected and prevented:** The [Cybereason Defense Platform](#) fully detects and prevents the RansomEXX ransomware.



## Background

TheRansomEXX family, also known as Defray777 and Ransom X, runs as a solely in-memory payload that is not dropped to disk, making it highly evasive. RansomEXX was involved in three major attacks in 2020 against [Texas TxDOT](#) in May of 2020, against [Konica Minolta](#) in the end of July, and against [Brazil's court system](#) in the beginning of November.

In addition, last December RansomEXX operators published [stolen credentials from Embraer](#), one of the largest aircraft makers in the world, on its own leaks website as part of the ongoing [double extortion trend](#).

In mid 2020, a Linux variant of RansomEXX emerged. This variant, despite sharing [similarities](#) with the Windows variant, is [simpler](#) than its predecessor and lacks many features such as disabling security software and command and control communication. There are decryptors for both variants, and the threat actors send paying victims a private key to decode their files.

## RansomEXX Analysis

This analysis focuses on the Windows variant of RansomEXX, which can be classified as fileless malware because it is [reflectively loaded](#) and executed in memory without touching the disk. Analysis of this sample reveals that it is partially obfuscated but includes indicative information such as the “ransome.exe” string that can be seen hard coded in the binary:

```
.ransom.exe.?ReflectiveLoader@@YG  
KPAX@Z.....
```

*ransom.exe string hardcoded in the binary*

Upon execution, RansomEXX starts decrypting some strings necessary for its operation:

```
do
{
    v5 = v17;
    v12[v4] = byte_E6E438[v4] ^ (byte_E6E428[v4] + (v4 & 0x7F));
    byte_E6E42A[v5 + v4] = byte_E6E439[v4] ^ (byte_E6E429[v4] + ((v4 + 1) & 0x7F));
    byte_E6E42B[v16 + v4] = byte_E6E43A[v4] ^ (byte_E6E42A[v4] + ((v4 + 2) & 0x7F));
    byte_E6E42C[v15 + v4] = byte_E6E43B[v4] ^ (byte_E6E42B[v4] + ((v4 + 3) & 0x7F));
    byte_E6E42D[v14 + v4] = byte_E6E43C[v4] ^ (byte_E6E42C[v4] + ((v4 + 4) & 0x7F));
    v6 = byte_E6E42D[v4] + ((v4 + 5) & 0x7F);
    v4 += 6;
    v12[v4 - 1] = byte_E6E437[v4] ^ v6;
}
while ( v4 < 12 );
```

*RansomEXX's strings decryption routine*

The mutex the malware creates is generated from the GUID of the infected machine:

8D95 ECFCFFF	lea edx,dword ptr ss:[ebp-314]	edx:L"{14ADA678-10B6-E8F3-2127-DF66E5B89DE3}"
52	push edx	
6A 00	push 0	
6A 00	push 0	
FF15 9091E600	call dword ptr ds:[<&CreateMutexw>]	
FF15 7C91E600	call dword ptr ds:[<&GetLastError>]	

*The GUID generated on the infected machine*

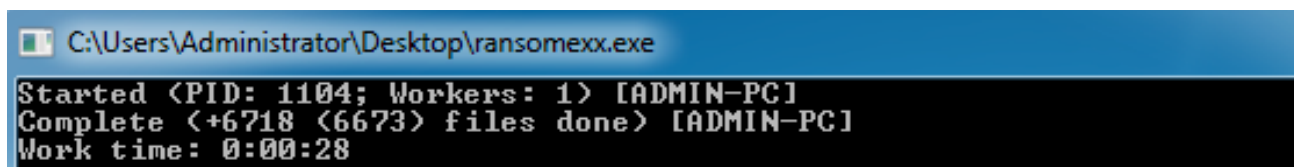
The decrypted strings at this point include mainly logs:

mov ecx,dword ptr ss:[ebp-14]	
push eax	
push ecx	
call dword ptr ds:[<&GetCurrentProcessId>]	
push eax	
push esi	
call ransomexx.E51A20	esi:"started (PID: %u; workers: %u) [%s]\n"
add esp,10	

*Decrypted logging string*

RansomEXX spawns a separate thread in the background to handle the logging process.

When debugging the sample, the logs themselves can be seen in the console:



*Logging as seen in the command line*

The malware then continues with [terminating processes and system services](#) that may interfere with the execution, but excludes those that are relevant for its execution:

```
v2[0] = (int)L"AVP";  
v2[1] = (int)L"AcrSch2Svc";  
v2[2] = (int)L"Acronis VSS Provider";  
v2[3] = (int)L"AcronisAgent";  
v2[4] = (int)L"AcronixAgent";  
v2[5] = (int)L"Antivirus";  
v2[6] = (int)L"BackupExecAgentAccelerator";  
v2[7] = (int)L"BackupExecAgentBrowser";
```

```
dd offset aPowershellExe ; DATA XREF: sub_E524D0+5C↑r  
; sub_E524D0+64↑o ...  
; "powershell.exe"  
dd offset aRundll32Exe ; "rundll32.exe"  
dd offset aWerfaultExe ; "werfault.exe"  
dd offset aExplorerExe ; "explorer.exe"  
dd offset aVmnatExe ; "vmnat.exe"
```

Some of the terminated services as well as processes excluded from termination

Cybereason detects the execution of RansomEXX together with the below listed commands that are executed post-encryption. These commands' role is to prevent the victim from restoring their system by deleting backups, Windows error recovery etc. Cybereason also detects this malicious usage of Windows utilities:



*RansomEXX's attack tree as seen in the Cybereason Defense Platform*

The depicted above commands are as follows:

Command	Action
"C:\Windows\System32\fsutil.exe" usn deletejournal /D C:	fsutil.exe deletes the <a href="#">Update Sequence Number</a> journal
"C:\Windows\System32\wbadmin.exe" delete catalog -quiet	wbadmin.exe deletes the <a href="#">backup catalog</a>
"C:\Windows\System32\wevtutil.exe" cl Setup "C:\Windows\System32\wevtutil.exe" cl System "C:\Windows\System32\wevtutil.exe" cl Application "C:\Windows\System32\wevtutil.exe" cl Security	wevtutil clears <a href="#">event logs</a>
"C:\Windows\System32\bcdedit.exe" /set {default} bootstatuspolicy ignoreallfailures "C:\Windows\System32\bcdedit.exe" /set {default} recoveryenabled no	<a href="#">bcdedit</a> disable recovery mode
"C:\Windows\System32\cipher.exe" /w:C:	cipher <a href="#">overwrites deleted data</a> in drive C
"C:\Windows\System32\schtasks.exe" /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable	schtasks disables the system restore scheduled task
"C:\Windows\System32\wevtutil.exe" sl Security /e:false	wevtutil disables the security event <a href="#">logs</a>

After preparation of the environment RansomEXX encrypted the files on the victim's machine and the following note is left on the machine:

---

Greetings, !

Read this message CAREFULLY and contact someone from IT department.  
Your files are securely ENCRYPTED.  
No third party decryption software EXISTS.  
MODIFICATION or RENAMING encrypted files may cause decryption failure.

You can send us an encrypted file (not greater than 400KB) and we will decrypt it FOR FREE,  
so you have no doubts in possibility to restore all files from all affected systems ANY TIME.  
Encrypted file SHOULD NOT contain sensitive information (technical, backups, databases, large documents).  
The rest of data will be available after the PAYMENT.  
Infrastructure rebuild will cost you MUCH more.

Contact us ONLY if you officially represent the whole affected network.  
The ONLY attachments we accept are non archived encrypted files for test decryption.  
Speak ENGLISH when contacting us.

Mail us: @protonmail.com  
We kindly ask you not to use GMAIL, YAHOO or LIVE to contact us.  
The PRICE depends on how quickly you do it.

### *The ransom note left on the victim's machine*

The commands that disable file recovery and system restore after successfully encrypting the victim's files, and can also be observed clearly in the sample's code:

```
v13[1] = (int)L"bcdedit.exe";
v13[3] = (int)L"bcdedit.exe";
v2 = L"wbadmin.exe";
v12 = L"wbadmin.exe";
v13[0] = (int)L"delete catalog -quiet";
v13[2] = (int)L"/set {default} recoveryenabled no";
v13[4] = (int)L"/set {default} bootstatuspolicy ignoreallfailures";
v13[5] = (int)L"schtasks.exe";
v13[6] = (int)L"/Change /TN "\\Microsoft\\Windows\\SystemRestore\\SR\\" /disable";
v13[7] = (int)L"wevtutil.exe";
v13[8] = (int)L"cl Application";
v13[9] = (int)L"wevtutil.exe";
v13[10] = (int)L"cl System";
v13[11] = (int)L"wevtutil.exe";
v13[12] = (int)L"cl Setup";
v13[13] = (int)L"wevtutil.exe";
v13[14] = (int)L"cl Security";
v13[15] = (int)L"wevtutil.exe";
v13[16] = (int)L"sl Security /e:false";
v13[17] = (int)L"fsutil.exe";
v13[18] = (int)L"usn deletejournal /D C:";
v13[19] = 0;
v13[20] = 0;
v3 = 0;
```

*Part of the post-encryption commands in RansomEXX's code*


## **Cybereason Detection and Prevention**

Cybereason detects the Windows utilities that are executed post-encryption as malicious and triggers a [Malop](#)(™) for all of them:


 <b>wbadmin.exe</b> Malicious process Backup catalog deletion	 admin-pc	 Infection
 <b>fsutil.exe</b> Malicious process Update Sequence Number journal deletion	 admin-pc	 Infection
 <b>ransomexx.exe</b> Ransomware Cybereason Threat Intelligence identified an executable as ransomware	 admin-pc	 Ransomware

*Detection of the ransomware and malicious uses of windows utilities by the Cybereason Defense Platform*

Looking at the Malop that was triggered by *fsutil*, the evidence for malicious activity can be seen together with the suspicions mapped to the MITRE ATT&CK matrix:

  
**Malicious process**  
**fsutil.exe**  
Update Sequence Number journal deletion


---

 **Suspicious (1)**

---

T1107 - File Deletion, T1070 - Indicator Removal on Host : fsutil.exe  
deleted the Update Sequence Number journal change (ATT&CK:  
Defense Evasion - File Deletion, Indicator Removal on Host)

---

 **Evidence (2)**

---


fsutil.exe deleted the Update Sequence Number journal change

---

Evidence of a new process

*Suspicious and evidence triggered by fsutil*

When Cybereason anti-ransomware prevention is turned on, the execution of the RansomEXX is prevented using the AI module:

 <b>ransomexx.exe</b> Unknown malware	Prevented	ADMIN-PC	December 29, 2020 at 4:28:55 PM GM...
Description Artificial intelligence detected unknown malware		Path c:\users\administrator\desktop\ransomexx.exe	

*Execution prevention of RansomEXX by the Cybereason Defense Platform*

## Security Recommendations

- **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* - [more information for customers can be found here](#)
- **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - [more information can be found here](#)
- **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities
- **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data
- **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering
- **Indicator's of Compromise:** Includes C2 Domains, IP addresses, Docx files SHA-1 hashes, and Msi files. Open the chatbot on the lower right-hand side of this blog to download your copy.

## MITRE ATT&CK BREAKDOWN

Defense Evasion	Impact	Execution	Discovery	Privilege Escalation
<a href="#">Impair Defenses:</a> <a href="#">Disable or Modify Tools</a>	<a href="#">Data Encrypted for Impact</a>	<a href="#">Command and Scripting Interpreter:</a> <a href="#">Windows Command Shell</a>	<a href="#">Obfuscated Files or Information</a>	<a href="#">Process Injection</a>

<a href="#"><u>Indicator Removal on Host: File Deletion</u></a>	<a href="#"><u>Inhibit System Recovery</u></a>	<a href="#"><u>Command and Scripting Interpreter: Unix Shell</u></a>	<a href="#"><u>System Information Discovery</u></a>	
		<a href="#"><u>Scheduled Task/Job</u></a>	<a href="#"><u>File and Directory Discovery</u></a>	
			<a href="#"><u>Software Discovery: Security Software Discovery</u></a>	
			<a href="#"><u>Process Discovery</u></a>	

Daniel Frank 



Daniel Frank is a senior Malware Researcher at Cybereason. Prior to Cybereason, Frank was a Malware Researcher in F5 Networks and RSA Security. His core roles as a Malware Researcher include researching emerging threats, reverse-engineering malware and developing security-driven code. Frank has a BSc degree in information systems.

---

Source: <https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware>