New CatB Ransomware Employs 2-Year Old DLL Hijacking Technique To Evade Detection

minerva-labs.com/blog/new-catb-ransomware-employs-2-year-old-dll-hijacking-technique-to-evade-detection/

Natalie Zargarov | 29.12.22 | 4 Minutes Read

We recently discovered ransomware, which performs MSDTC service DLL Hijacking to silently execute its payload. We have named this ransomware CatB, based on the contact email that the ransomware group uses. The sample was first uploaded to VT on November 23, 2022 and tagged by the VT community as a possible variant of the Pandora Ransomware. The assumed connection to the Pandora Ransomware was due to some similarities between the CatB and Pandora ransom notes. However, the similarities pretty much end there. The CatB ransomware implements several anti-VM techniques to verify execution on a “real machine”, followed by a malicious DLL drop and DLL hijacking to evade detection.

CatB ransomware contains two files, the dropper (version.dll), packed with UPX, and the ransomware payload (oci.dll). The dropper handles anti-VM checks, dropping the ransomware payload and executing it.

Anti-VM

CatB dropper implements three anti-VM/sandbox evasion techniques:

> **Processor core check** – Real computers nowadays all have at least two processors, so if the ransomware detects only one CPU core, that would be a strong indicator that it is currently residing on in a sandbox.The ransomware retrieves system information by GetSystemInfo API function and checks the number of processors. If there are less than two processors, it exits and does not execute.

```
lea     rcx, [rbp+2D0h+SystemInfo] ; lpSystemInfo
call    cs:GetSystemInfo
cmp     [rbp+2D0h+SystemInfo.dwNumberOfProcessors], 2
jb      loc_7FF8042913E2
```

Figure 1 – Processor check

Total Physical memory check – As opposed to virtual machines, real machines today all have at least 2GB RAM, and usually have between 4GB and 32GB. The CatB Ransomware detects VMs/sandboxes by checking physical memory size. This is done by retrieving the information about both the physical and virtual memory using the GlobalMemoryStatusEx API function. In our case, the ransomware checks and exits if the machine has at less than 2GB of physical memory.

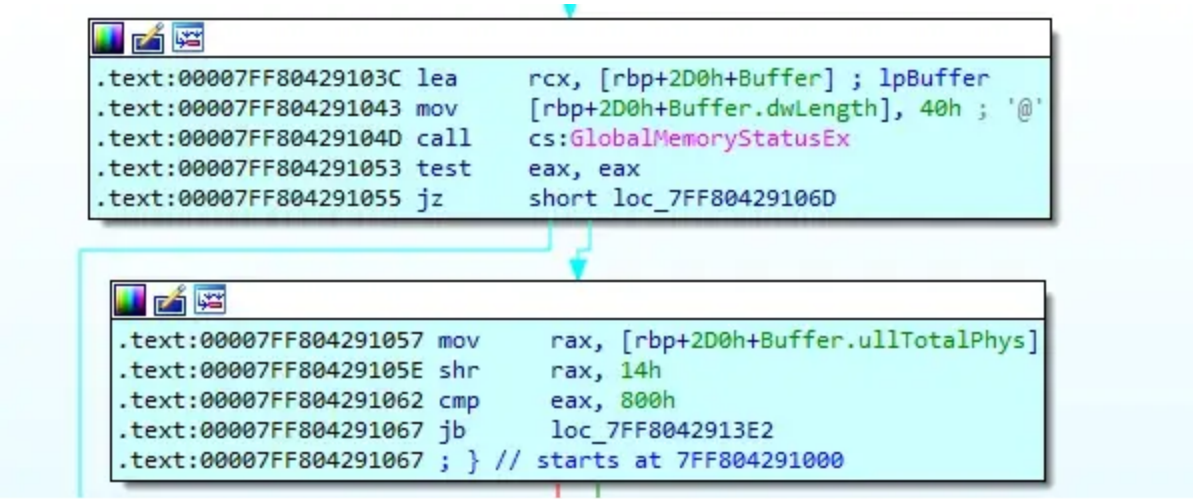

Figure 2 – Physical memory check

Hard Drive size – Malware can check the machine hdd size and continue execution leaning on that parameter. This can be done by using the DeviceIoControl Api function with '0x70000' passed as the dwIoControlCode parameter. CatB ransomware will execute only in a machine with at least a 50GB hard drive.

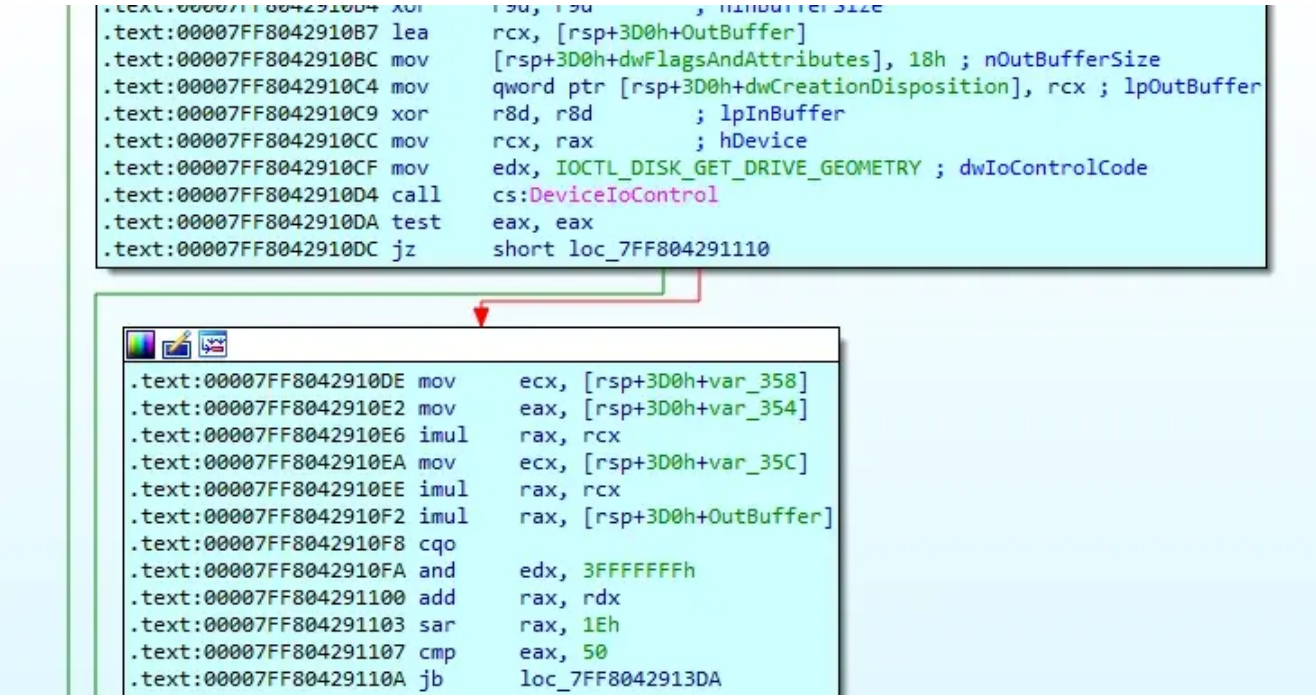

Figure 3 – Hard Disk size check

DLL Hijacking

If all anti-VM checks pass, the dropper will continue its execution and drop the ransomware payload (oci.dll) into the C:\Windows\System32 folder. Next, it looks for the MSDTC service (the Distributed Transaction Coordinator Windows service that is responsible for coordinating transactions between databases (SQL Server) and web servers) and changes its configurations.

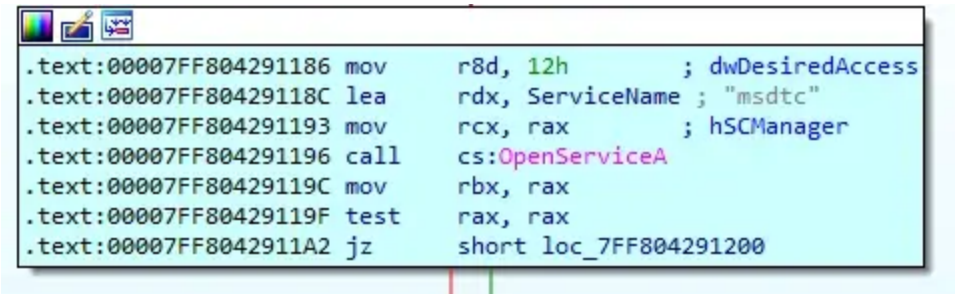

Figure 4 – MSDTC service

The configurations changed are the name of the account under which the service should run, which is changed from Network Service to Local System, and the service start option, which is changed from Demand start to Auto start for persistency if a restart occurs.

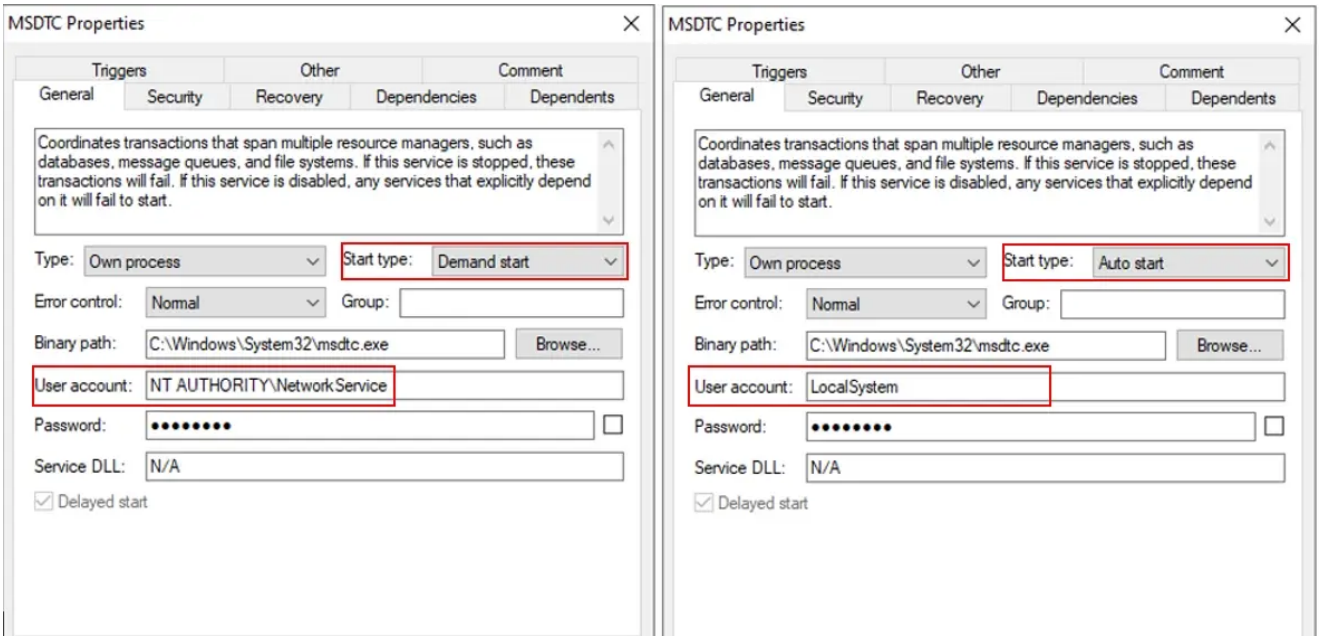

Figure 5 – Service Configuration Changes

The account under which the service runs was changed to grant admin rights to the service, as the Network Service account runs with user rights. The cChangeing of the start type will grants the ransomware the ability to executeion every time the system restarts.

The dropper starts the service after changing its configuration. When this service starts, it attempts to load, by default, several DLLs from the System32 folder. This gives it the opportunity to plant an arbitrary DLL (in our case, oci.dll) into this folder in order to execute malicious code.

Ransomware

The Malicious oci.dll file is loaded into the msdtc.exe process, after which the encryption process starts. CatB enumerates and encrypts specific hardcoded disks and folders:

1. Disk D:\
2. Disk E:\
3. Disk F:\
4. Disk G:\
5. Disk H:\
6. Disk I:\
7. All files under C:\Users and its sub-directories
8.

Figure 6 – Hardcoded Disks

CatB avoids encrypting files with .msi, .exe, .dll, .sys, .iso extensions and the NTUSER.DAT file. An interesting thing about the CatB ransomware is that the ransom note is added into the beginning of every encrypted file and not as a separate file in every folder as most of the ransomwares do. It also doesn't change the file extensions. This might initially confuse users who may not notice the encryption and the file will just appear to be corrupted as they would be unable to open it as its binary contents are broken. The ransom note itself looks very similarly built to Pandora and Crypt ransom notes, with some sections actually being copy/pastes from them:

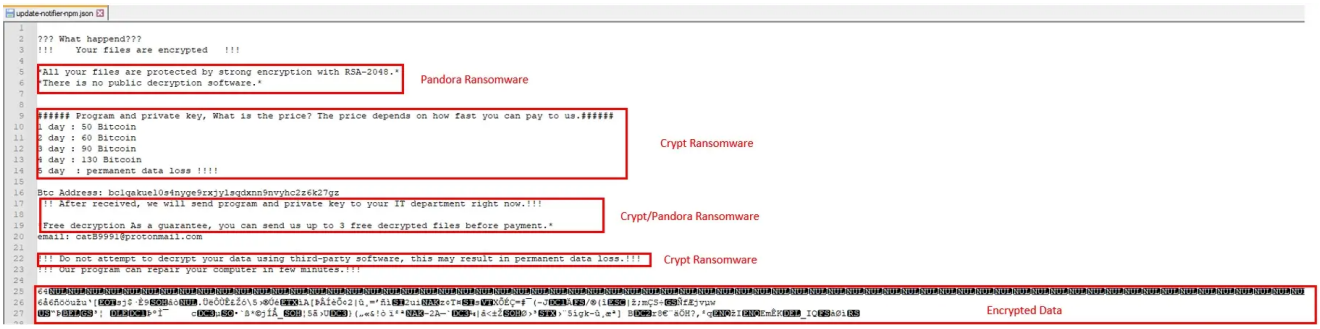

Figure 7 – Encrypted file

There is no official ransom name in the note and no tor website URL. The only method available to contact the ransomware operator is via email.

Prevention

Minerva Armor's Ransomware Protection Platform easily prevents CatB ransomware by simulating environmental data that the ransomware is actively trying to avoid.

For example when the ransomware queries for the number of processors, Minerva Armor leads it to believe that it is in an environment with only 1 CPU.

Figure 8 – Prevention

Relevant MITRE ATT&CK:

T1027 – Obfuscated Files or Information

T1036 – Masquerading

T1497 – Virtualization/Sandbox Evasion

T1082 – System Information Discovery

T1518.001 – Software Discovery: Security Software Discovery

T1486 – Data Encrypted for Impact

T1574.001 – Hijack Execution Flow: DLL Search Order Hijacking

IOC's

1. Version.dll – 3661ff2a050ad47fdc451aed18b88444646bb3eb6387b07f4e47d0306aac6642
1. Oci.dll – 35a273df61f4506cdb286ecc40415efaa5797379b16d44c240e3ca44714f945b
1. Bitcoin wallet address – bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz
1. Email contact – catB9991@protonmail.com

References

https://pentestlab.blog/2020/03/04/persistence-dll-hijacking/

See the Minerva Armor Platform in Action!

View a recorded demo or sign up for a one-on-one talk

Schedule A Demo

The technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user, or for the sole purpose of carrying out the transmission of a communication over an electronic communications network.

The technical storage or access is necessary for the legitimate purpose of storing preferences that are not requested by the subscriber or user.

The technical storage or access that is used exclusively for statistical purposes. The technical storage or access that is used exclusively for anonymous statistical purposes. Without a subpoena, voluntary compliance on the part of your Internet Service Provider, or additional records from a third party, information stored or retrieved for this purpose alone cannot usually be used to identify you.

The technical storage or access is required to create user profiles to send advertising, or to track the user on a website or across several websites for similar marketing purposes.

View preferences
{title} {title} {title}