CatB Ransomware | File Locker Sharpens Its Claws to Steal Data with MSDTC Service DLL Hijacking

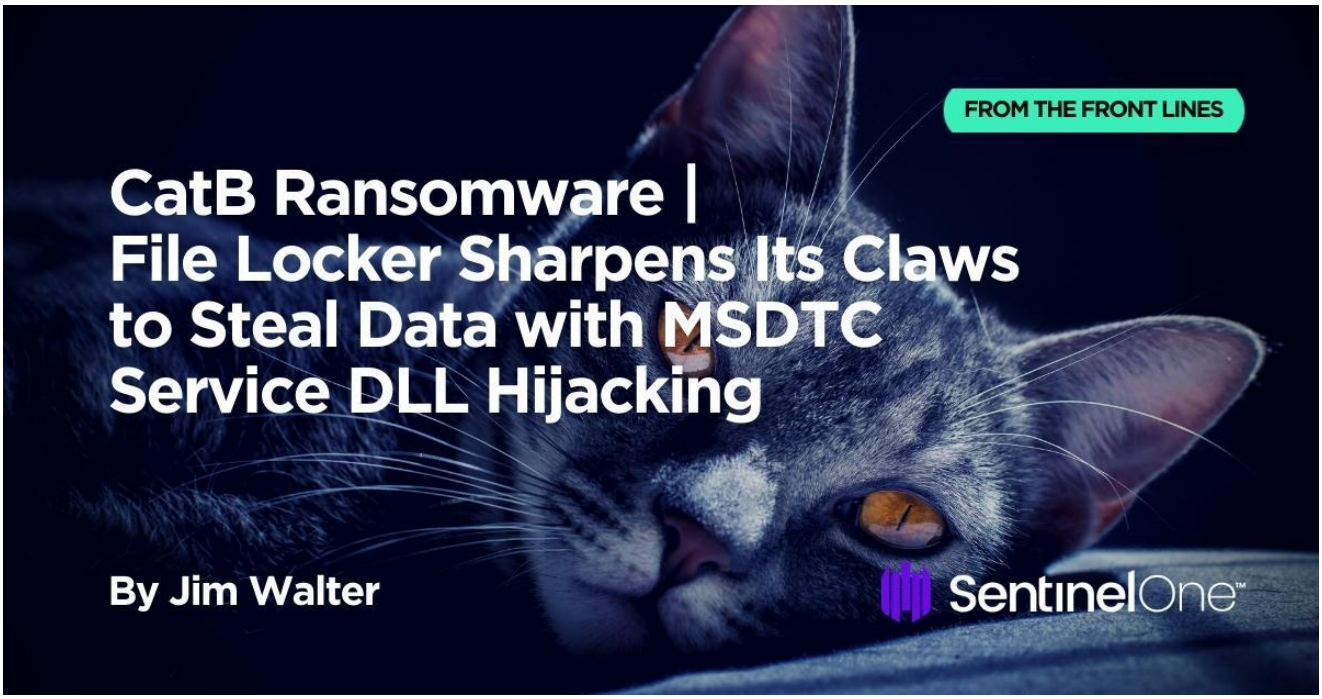
sentinelone.com/blog/decrypting-catb-ransomware-analyzing-their-latest-attack-methods/

March 13, 2023

The CatB ransomware family, sometimes referred to as CatB99 or Baxtoy, was first observed in late 2022, with campaigns being observed steadily since November. The group's activities have gained attention due to their ongoing use of DLL hijacking via Microsoft Distributed Transaction Coordinator (MSDTC) to extract and launch ransomware payloads.

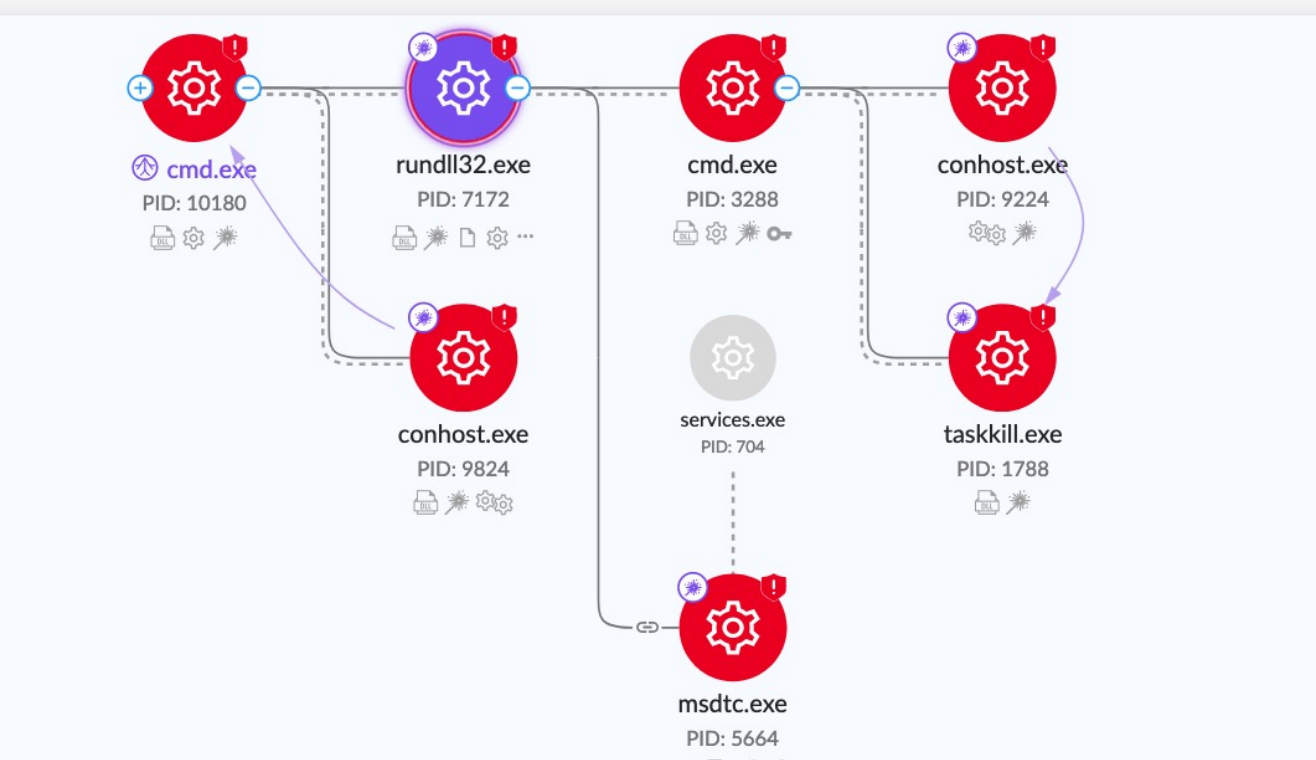
String similarities in the ransom notes as well as modifications left by the ransomware payloads suggest that CatB may be either an evolution or direct rebrand of the Pandora ransomware, which was active in early to mid-2022 and targeted the automotive industry.

In this post, we offer a technical analysis of the CatB ransomware and its abuse of the legitimate MSDTC service, describing its evasion tactics, encryption behavior, and its attempts to steal credentials and browser data.



CatB Ransomware Technical Information

CatB payloads are distributed as a two DLL set. A dropper DLL is responsible for initial evasive environmental checks as well as dropping and launching the second DLL, which serves the ransomware payload.

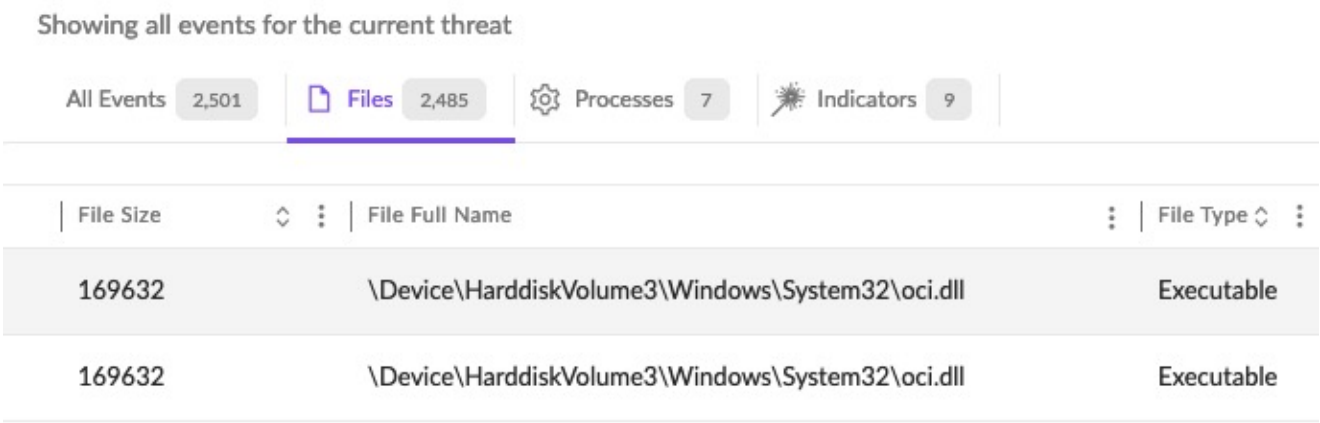


CatB Ransomware Process Graph

First, the dropper is distributed in the form of a UPX-packed DLL (`versions.dll`). This dropper deposits the second DLL payload (`oci.dll`) onto the target host. The dropper DLL is responsible for any sandbox evasion techniques required by the threat actor. Sandbox evasion inhibits the analysis process and ultimately leads to more time in the target environment for the attacker.

CatB performs three primary checks in an attempt to determine if the payload is being executed within a virtual environment. These are direct checks for type and size of physical RAM, type and size of physical hard disks, and checking for odd or anomalous combinations of processors and cores.

Upon execution, CatB payloads rely on DLL search order hijacking to drop and load the malicious payload. The dropper (`versions.dll`) drops the payload (`oci.dll`) into the System32 directory.



Oci.dll payloads in System32 (view from Singularity™ Console)

The malware then abuses the MSDTC service, manipulating the permissions and startup parameters. As a result, the system will inject the malicious `oci.dll` into the service's executable (`msdtc.exe`) when the MSDTC service is restarted. `Taskill.exe` is used to terminate the msdtc.exe process once the service configuration changes have been made.

```
                    u_/c_taskkill_/f_/im_msdtc.exe_1800166a0        XREF[1,5]:   versions:1800012cd(R),
                    u_ill_/f_/im_msdtc.exe_1800166b0                             versions:1800012bf(R),
                    u_im_msdtc.exe_1800166c0                                     versions:1800012d7(R),
                    u_.exe_1800166d0                                             versions:1800012f3(R),
                    u__1800166d8                                                 versions:1800013le(R),
                    u_cmd.exe_/c_taskkill_/f_/im_msdtc_180016690                 versions:18000133d(R)
0016690 63 00 6d        unicode     u"cmd.exe /c taskkill /f /im msdtc.exe"
        00 64 00
```

Msdtc.exe termination syntax

CatB ransomware excludes the following files and extensions from the encryption process: `.msi`, `.dll`, `.sys`, `.iso` and `NTUSER.DAT`.

```
if (((byte)local_8b8[0] & 0x10) == 0) {
  pwVar3 = wcsstr(local_894,L".msi");
  if (((((pwVar3 == (wchar_t *)0x0) &&
         (pwVar3 = wcsstr(local_894,L".exe"), pwVar3 == (wchar_t *)0x0)) &&
        (pwVar3 = wcsstr(local_894,L".dll"), pwVar3 == (wchar_t *)0x0)) &&
       ((pwVar3 = wcsstr(local_894,L".sys"), pwVar3 == (wchar_t *)0x0 &&
        (pwVar3 = wcsstr(local_894,L".iso"), pwVar3 == (wchar_t *)0x0)))) &&
      (pwVar3 = wcsstr(local_894,L"NTUSER.DAT"), pwVar3 == (wchar_t *)0x0)) {
    FUN_180005100((undefined (*) [16])local_688,0,0x20a);
```

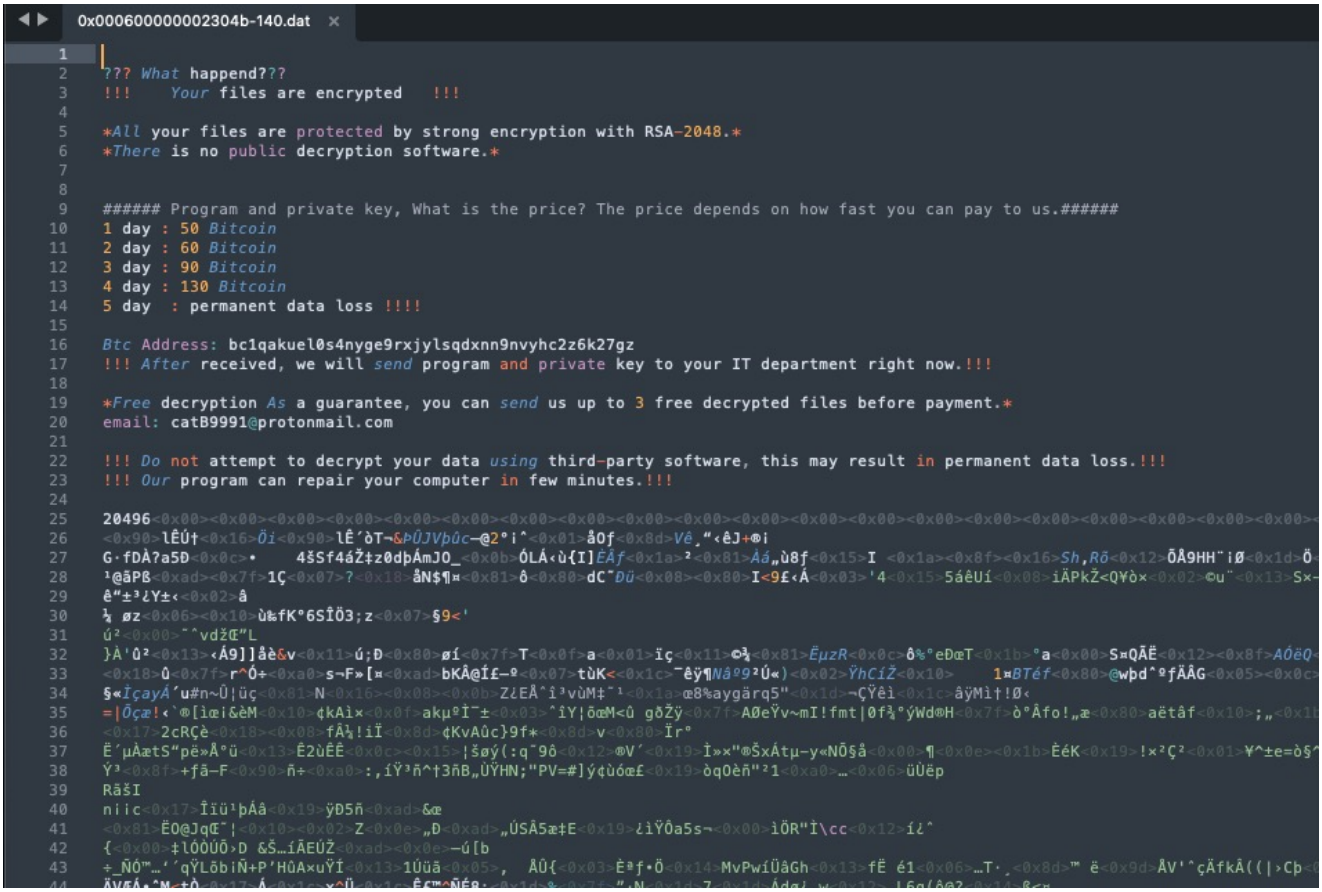
Encryption exclusions in payload DLL

In addition to the hardcoded exclusions, the local disk volumes to be encrypted are also configured in a similar manner. By default, the `oci.dll` payload will attempt to encrypt `C:\users` (crawl whole tree), `I:`, `H:`, `G:`, `F:`, `E:`, and `D:`.

```
    FUN_1800036b0(&DAT_180022f08,auStack1352,(uint *)auStack1368,auStack1048,(uint)uStack2024);
    FUN_1800036b0(&DAT_180022f10,auStack1352,(uint *)auStack1368,auStack1048,(uint)uStack2024);
    FUN_1800036b0(&DAT_180022f18,auStack1352,(uint *)auStack1368,auStack1048,(uint)uStack2024);
    FUN_1800036b0(&DAT_180022f20,auStack1352,(uint *)auStack1368,auStack1048,(uint)uStack2024);
    FUN_1800036b0(&DAT_180022f28,auStack1352,(uint *)auStack1368,auStack1048,(uint)uStack2024);
    FUN_1800036b0(&DAT_180022f30,auStack1352,(uint *)auStack1368,auStack1048,(uint)uStack2024);
    FUN_1800036b0(L"C:\\Users\\",auStack1352,(uint *)auStack1368,auStack1048,(uint)uStack2024);
}
```

Local encryption targets in *oci.dll*

The lack of post-encryption alterations is a trait that sets CatB apart from other contemporaries. Once encrypted, there is no blatant indicator – no separate ransom note dropped, no change to the desktop wallpaper, and no antagonizing file extensions. Instead, what could be considered the ransom note is inserted into the beginning of each encrypted file.



Ransom note appended to head of encrypted file (catb991 variation)

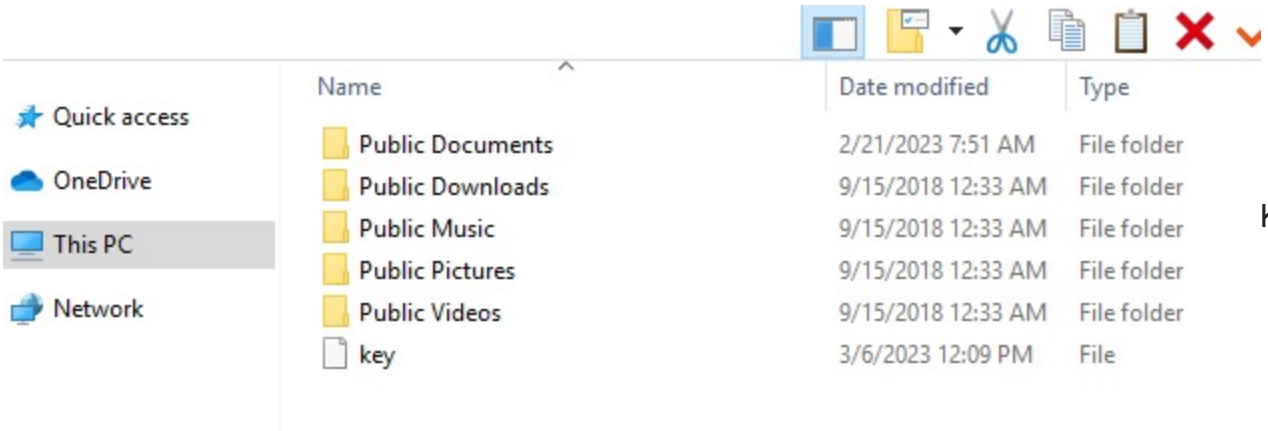
Per the ransom note, the only way to engage the threat actor is via email at the provided catB9991 protonmail address. Beyond that, a single Bitcoin (BTC) address is provided for payment submissions. The ransom price is set to increase each day for five days and, following the fifth day, there will be “permanent data loss” if the victim does not comply.

Based on observations, there is no evidence to indicate that CatB operators are generating payment wallets for each victim as the Bitcoin address provided is not unique to each sample.

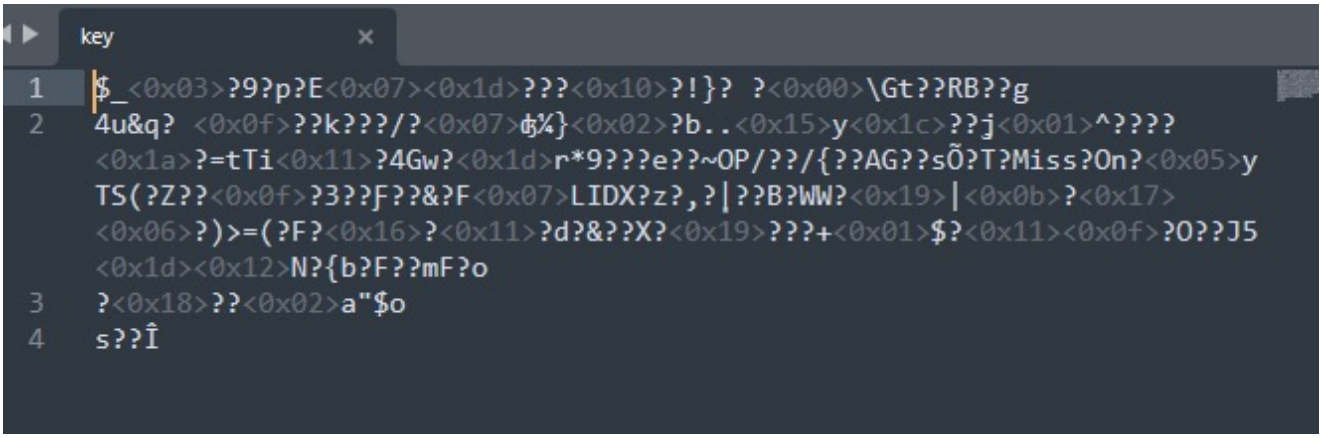
```
140027c0c 00              ??         00h
140027c0d 00              ??         00h
140027c0e 00              ??         00h
140027c0f 00              ??         00h

                     s_c:\users\public\key_140027c10                 XREF[1
140027c10 63 3a 5c        ds         "c:\\users\\public\\key"
          75 73 65
          72 73 5c ...
```

Generation of unique key file

A key file is deposited onto each infected host in `c:\users\public\`. This file must be included in email correspondence with the attackers as it is, ideally, a unique identifier for each victim or host.



Key file dropped for each victim



Example CatB ‘key’ file

Credential and Browser Data Theft

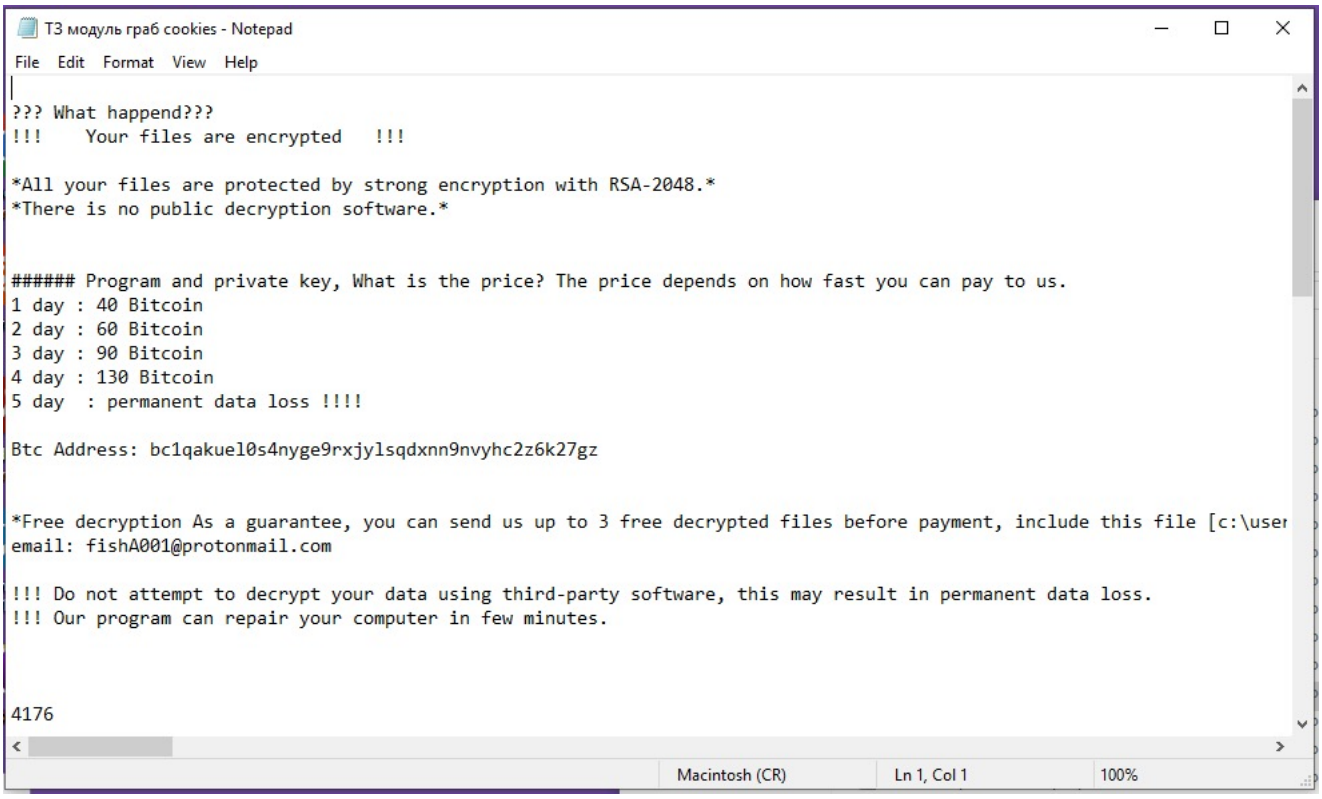
In addition to file encryption and obfuscation, the CatB malware will attempt to gather specific, sensitive information from targeted systems. This includes browser session and credential data.

The ransomware contains functionality to discover and extract user data from Mozilla Firefox, Google Chrome, Microsoft Edge as well as Internet Explorer. Data extracted from browsers includes bookmarks, blocklists, crash logs, history, user profile data, autofill data, environmental settings, browser session keys, and more.

CatB malware will also attempt to locate and extract sensitive information from Windows Mail profile data (`\AppData\Local\Microsoft\Windows Mail\`).

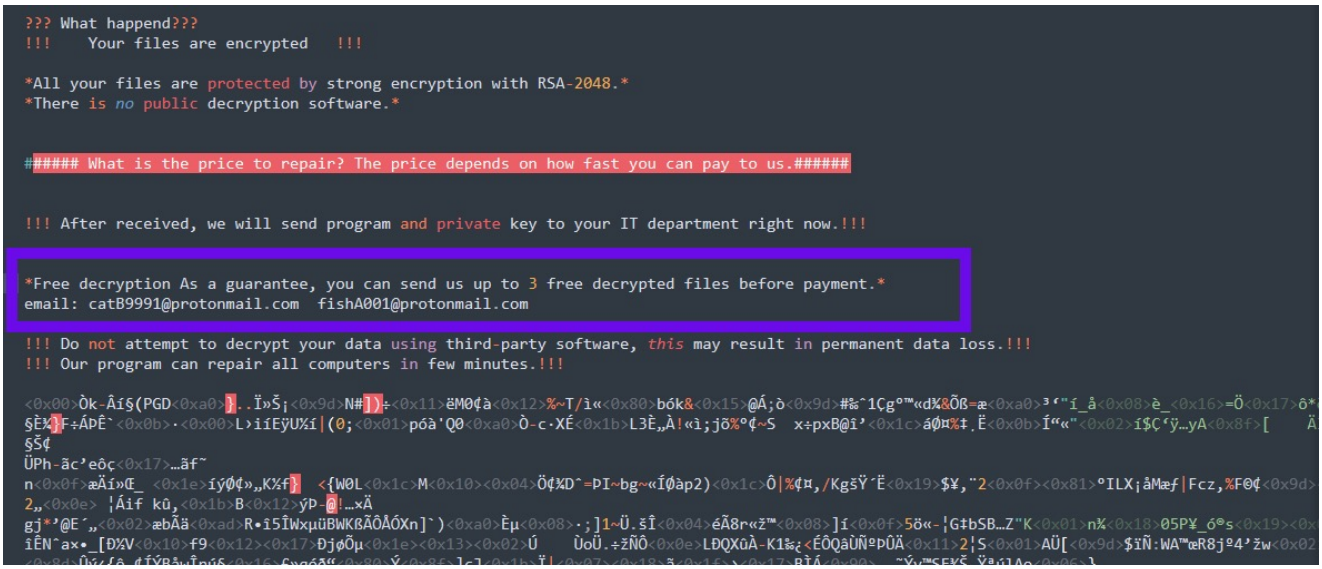
Variations of CatB Threat Campaigns

Samples pulled from a November 2022 campaign feature a different contact email address, `fishA001[@]protonmail.com`. This later changes to the catB9991 protonmail address mentioned above. This is the only difference with regards to the ransom notes. Other details such as payment-per-day breakdowns and the BTC payment address are identical.



Alternate ransom note (fisha001)

We have also encountered variations which include both email addresses. When these ‘double email’ notes are appended to the head of files, it looks as follows:

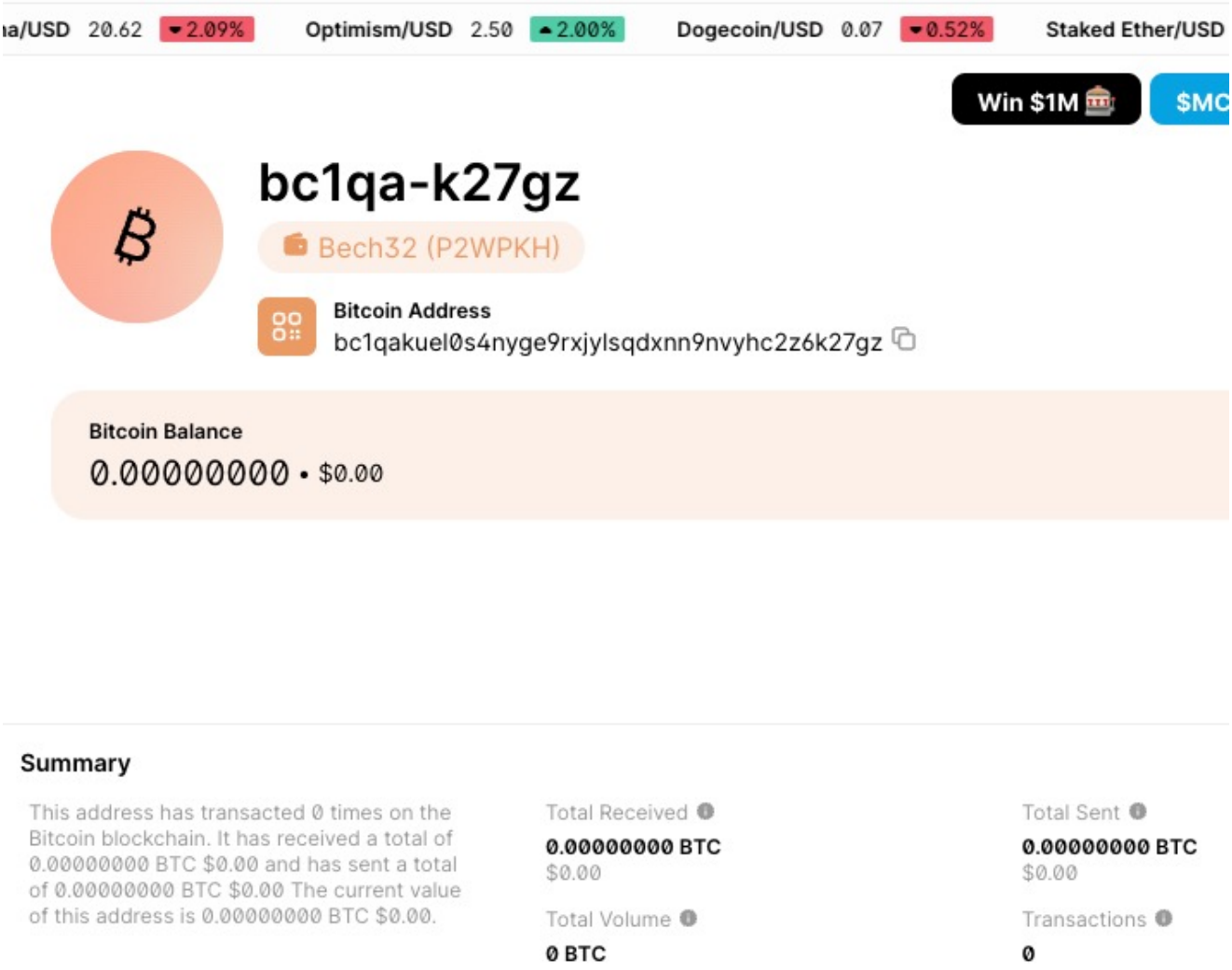


Alternate ransom note (double-email, no BTC)

These ransom notes display all the same features minus the BTC payment address. Also missing is the requirement to submit the key file in `c\users\public\key`. Notes that are missing the key submission feature suggest that they are artifacts of an earlier ‘test’ version of the ransomware.

BTC Payment / Blockchain Status

As the time of writing, the BTC address associated with CatB ransomware have zero transactions and a zero balance.



BTC Balance for Wallet – *bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz*

Conclusion

CatB joins a long line of ransomware families that embrace semi-novel techniques and atypical behaviors such as appending notes to the head of files. These behaviors appear to be implemented in the interest of detection evasion and some level of anti-analysis trickery. For example, many environments rely solely on the appearance of ransom notes to alert them to the potential of a ransomware outbreak. This is not the case with CatB.

Despite that, the threat lacks in overall sophistication, and a modern, properly configured, XDR/EDR solution should alert quickly upon initiation of a CatB attack in the environment.

SentinelOne Singularity™ fully prevents and protects customers against malicious behaviors associated with CatB Ransomware.

Indicators of Compromise

SHA1 CatB Samples

1028a0e6cecb8cfc4513abdbe3b9d948cf7a5567
8c11109da1d7b9d3e0e173fd24eb4b7462073174
951e603af10ec366ef0f258bf8d912efedbb5a4b (early version note example)
db99fc79a64873bef25998681392ac9be2c1c99c
dd3d62a6604f28ebeeec36baa843112df80b0933

Email addresses

catB9991[at]protonmail[.]com
fishA001[at]protonmail[.]com

BTC Wallets

`bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz`