AhnLab Cyber Threat Intelligence Report

Unerring Spear:
Cephalus Ransomware Analysis

Dec 2025

Table of Contents

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Summary

Cephalus Information

- A new ransomware group that first appeared in mid-June 2025
- Describes itself as operating with a purely financial motive
- Performs double extortion by leaking targeted organizational data and then encrypting it
- Gains entry by stealing RDP accounts that do not have multi-factor authentication (MFA) enabled
- Targets various countries and industries, including the eastern United States, Japan, the United Kingdom, and sectors such as legal, finance, IT, and government agencies

About the Ransomware

- Developed in Go
- Disrupts analysis by using a fake AES key-generation routine
- Applies techniques to prevent encryption keys from being exposed in memory or on disk
- Appends the .sss extension after encrypting files and creates a ransom note named recover.txt
- Stops services related to backups (Veeam) and databases (MSSQL, MongoDB)
- Modifies Windows Defender settings (diagnostic exclusions, disabling real-time protection, etc.)

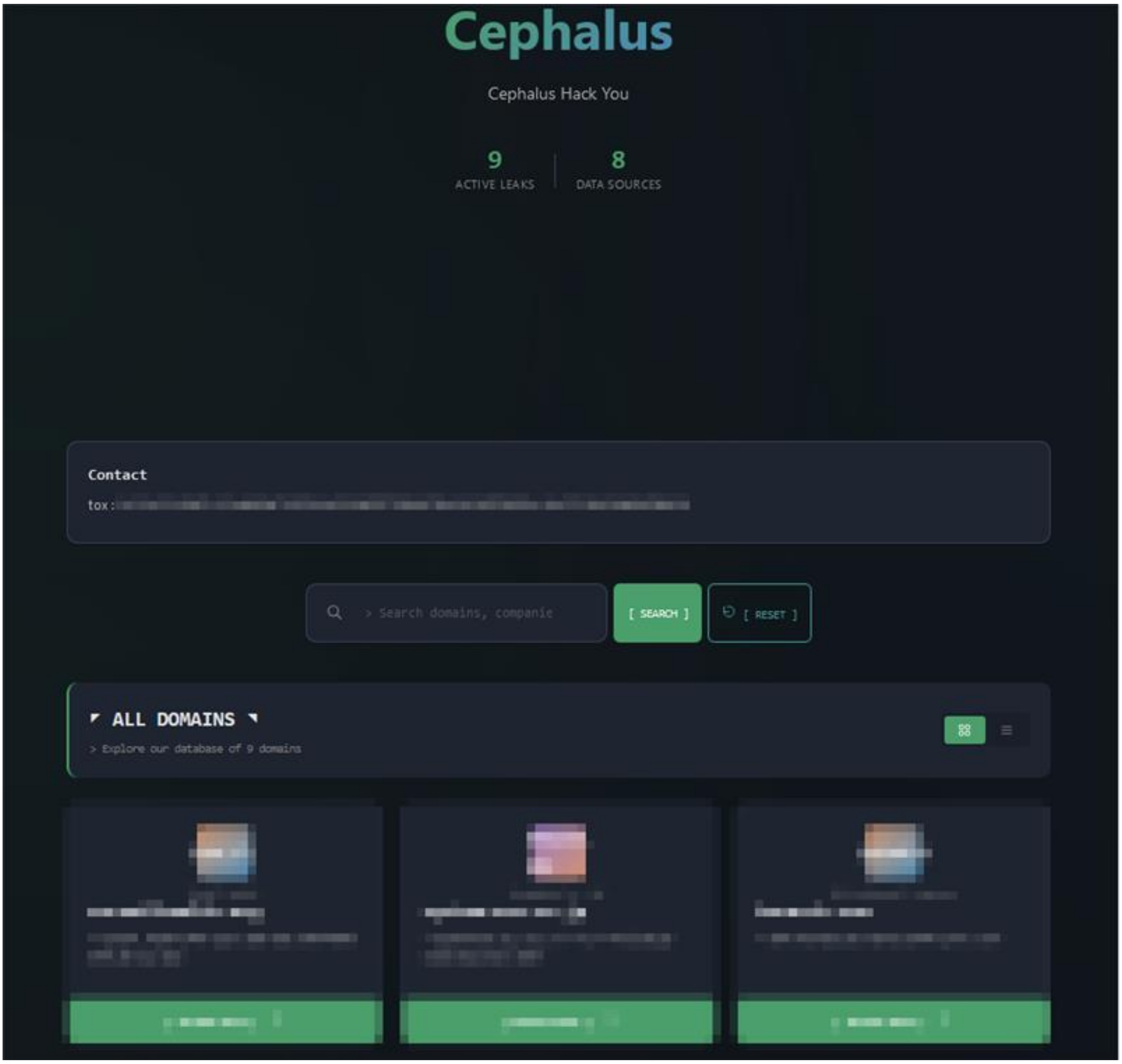
Overview

Cephalus

Cephalus is a new ransomware group that first appeared in mid-June 2025. The group claims that they are motivated 100% by financial gain. Their main method of breaching organizations is by stealing credentials through Remote Desktop Protocol (RDP) accounts that do not have multi-factor authentication (MFA) enabled. Their operation is unique in that they have a form of customized ransomware that targets specific organizations, breaches them, exfiltrates their data, and then encrypts it. As of now, it is not yet known if they operate as Ransomware as a Service (RaaS) or if they have formed alliances with other ransomware groups. The name of the group comes from Cephalus, a character in Greek mythology who received an "unerring" spear from Artemis. This is seen as a sign of the group's confidence in their success rate.

There is currently no information available on the rebranding history of the group or their clear and direct connection with other ransomware groups. There is also no information available on the existence of new strains or subgroups. Upon breaching the system, the group openly states their presence and previous cases of damage in their ransom notes to pressure the victims. They also use tactics such as proving the data breach by providing a link to a GoFile repository.

The cases identified so far are concentrated primarily in the United States. Organizations targeted include law firms in the eastern states such as New Jersey and Virginia, as well as architecture offices, financial companies, marketing and PR firms, and local government agencies. Cases have also been reported outside the United States—such as Japanese IT companies and healthcare service providers in the United Kingdom—showing that the group is targeting a wide range of regions and industries.



Cephalus

Cephalus Hack You

9 ACTIVE LEAKS

8 DATA SOURCES

Contact

tox : [redacted]

ALL DOMAINS

> Explore our database of 9 domains

[redacted]

Figure 1. Cephalus leak site (DLS)

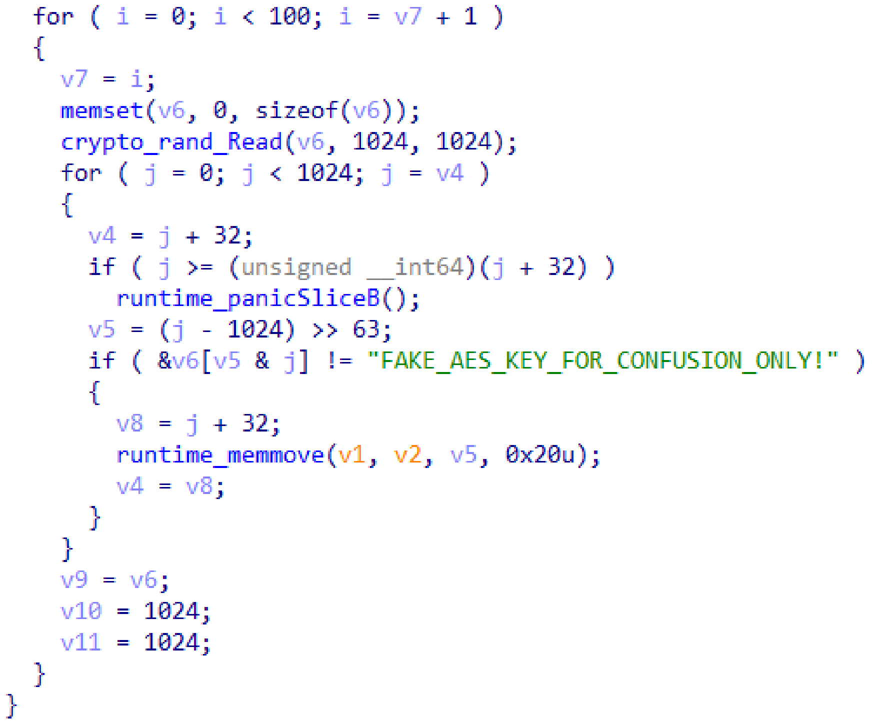
Analysis Details

Cephalus is a ransomware strain developed in Go. It disrupts dynamic analysis by generating a fake AES key. Upon execution, it disables Windows Defender's real-time protection, deletes VSS backups, and stops key services such as Veeam and MSSQL to increase its encryption success rate and decrease the chances of recovery. Cephalus uses a single AES-CTR key for encryption, and this key is managed to minimize exposure on the disk and in memory. Finally, the AES key is encrypted using an embedded RSA public key, ensuring that only threat actors with the corresponding RSA private key can decrypt the key.

Initial Routine

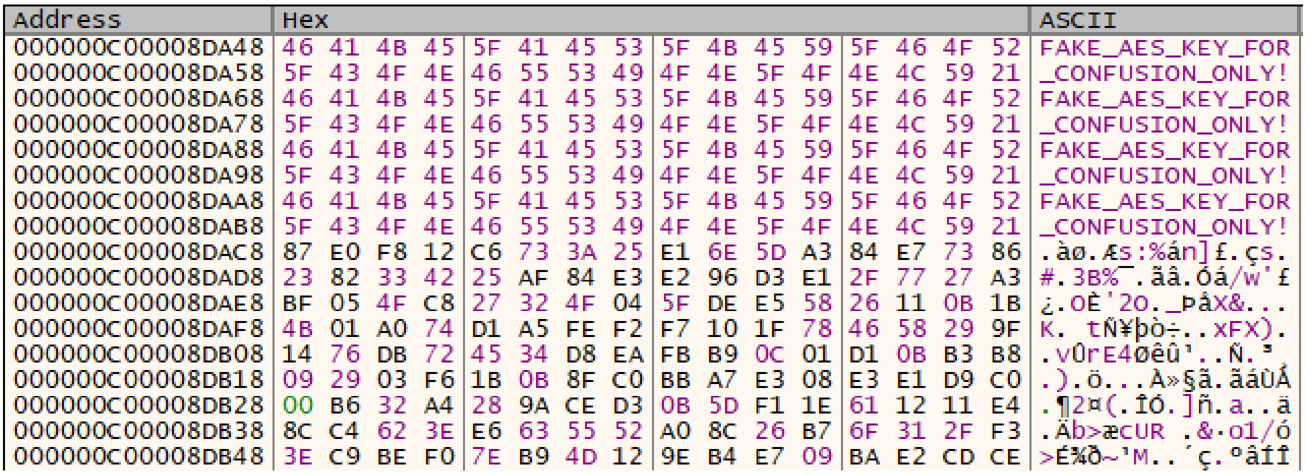
Fake AES Key Generation

Cephalus has a feature that aims to disrupt analysis and conceal the AES key that will be used for encryption. When the ransomware is executed, it generates a 1,024-byte random buffer using crypto_rand.Read(). It then overwrites this buffer with a 32-byte string that reads "FAKE_AES_KEY_FOR_CONFUSION_ONLY!" —a process that is repeated 100 times. Because this process causes many 32-byte memory accesses from the perspective of dynamic analysis tools or systems examining the ransomware, it appears to be intentionally designed so that "FAKE_AES_KEY_FOR_CONFUSION_ONLY!" is mistaken for the real AES key.



```
  for ( i = 0; i < 100; i = v7 + 1 )
  {
    v7 = i;
    memset(v6, 0, sizeof(v6));
    crypto_rand_Read(v6, 1024, 1024);
    for ( j = 0; j < 1024; j = v4 )
    {
      v4 = j + 32;
      if ( j >= (unsigned __int64)(j + 32) )
        runtime_panicSliceB();
      v5 = (j - 1024) >> 63;
      if ( &v6[v5 & j] != "FAKE_AES_KEY_FOR_CONFUSION_ONLY!" )
      {
        v8 = j + 32;
        runtime_memmove(v1, v2, v5, 0x20u);
        v4 = v8;
      }
    }
    v9 = v6;
    v10 = 1024;
    v11 = 1024;
  }
}
```

Figure 2. Fake AES key generation process



```
Address          Hex                                               ASCII
000000C00008DA48 46 41 4B 45 5F 41 45 53 5F 4B 45 59 5F 46 4F 52  FAKE_AES_KEY_FOR
000000C00008DA58 5F 43 4F 4E 46 55 53 49 4F 4E 5F 4F 4E 4C 59 21  _CONFUSION_ONLY!
000000C00008DA68 46 41 4B 45 5F 41 45 53 5F 4B 45 59 5F 46 4F 52  FAKE_AES_KEY_FOR
000000C00008DA78 5F 43 4F 4E 46 55 53 49 4F 4E 5F 4F 4E 4C 59 21  _CONFUSION_ONLY!
000000C00008DA88 46 41 4B 45 5F 41 45 53 5F 4B 45 59 5F 46 4F 52  FAKE_AES_KEY_FOR
000000C00008DA98 5F 43 4F 4E 46 55 53 49 4F 4E 5F 4F 4E 4C 59 21  _CONFUSION_ONLY!
000000C00008DAA8 46 41 4B 45 5F 41 45 53 5F 4B 45 59 5F 46 4F 52  FAKE_AES_KEY_FOR
000000C00008DAB8 5F 43 4F 4E 46 55 53 49 4F 4E 5F 4F 4E 4C 59 21  _CONFUSION_ONLY!
000000C00008DAC8 87 E0 F8 12 C6 73 3A 25 E1 6E 5D A3 84 E7 73 86  .àø.Æs:%án]£.çs.
000000C00008DAD8 23 82 33 42 25 AF 84 E3 E2 96 D3 E1 2F 77 27 A3  #.3B%¯.ãâ.Óá/w'£
000000C00008DAE8 BF 05 4F C8 27 32 4F 04 5F DE E5 58 26 11 0B 1B  ¿.OÈ'2O._ÞåX&...
000000C00008DAF8 4B 01 A0 74 D1 A5 FE F2 F7 10 1F 78 46 58 29 9F  K. tÑ¥þò÷..xFX).
000000C00008DB08 14 76 DB 72 45 34 D8 EA FB B9 0C 01 D1 0B B3 B8  .vÛrE4Øêû¹..Ñ.³¸
000000C00008DB18 09 29 03 F6 1B 0B 8F C0 BB A7 E3 08 E3 E1 D9 C0  .).ö...À»§ã.ãáÙÀ
000000C00008DB28 00 B6 32 A4 28 9A CE D3 0B 5D F1 1E 61 12 11 E4  .¶2¤(.ÎÓ.]ñ.a..ä
000000C00008DB38 8C C4 62 3E E6 63 55 52 A0 8C 26 B7 6F 31 2F F3  .Äb>æcUR .&·o1/ó
000000C00008DB48 3E C9 BE F0 7E B9 4D 12 9E B4 E7 09 BA E2 CD CE  >É¾ð~¹M..´ç.ºâÍÎ
```

Figure 3. Fake AES key generation process (Memory)

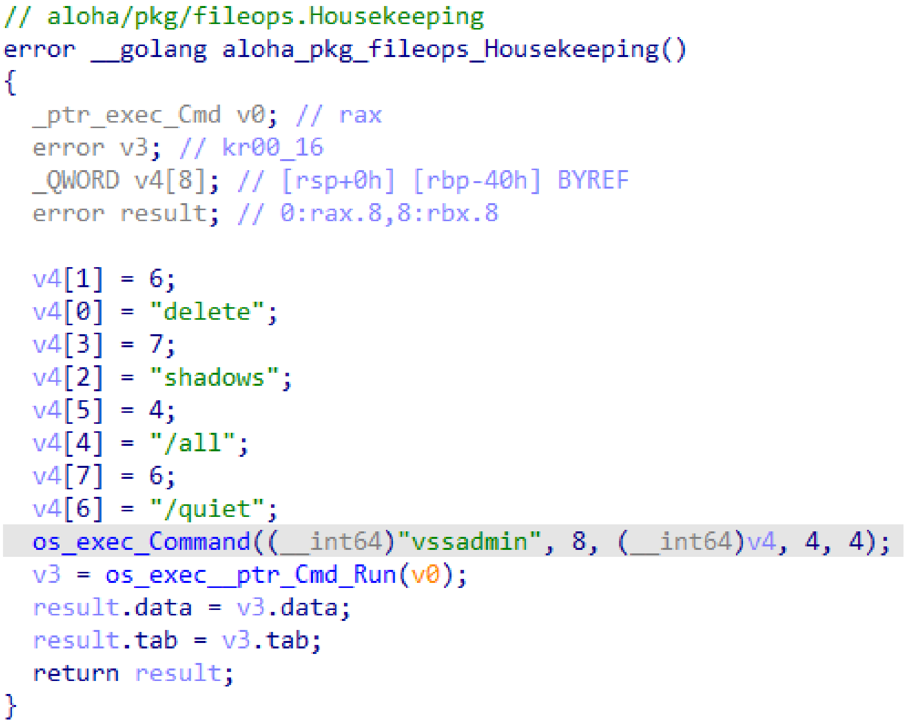
Windows Defender Option Modification

To ensure the malware operates smoothly, the settings of Windows Defender are modified to exclude the malware or disable security features. Its features are as follows:

- Uses PowerShell commands to exclude the ransomware process from detection
- Uses PowerShell commands to exclude the folder where the ransomware resides from detection
- Uses PowerShell commands to exclude the ".sss", ".tmp", ".dat", and ".cache" extensions from detection
- Modifies the registry to exclude the path where the ransomware resides from detection
- Modifies the registry to disable real-time protection
- Uses PowerShell commands to disable real-time monitoring
- Uses PowerShell commands to forcibly stop the Windows Defender service

Backup Data Deletion

Through the Housekeeping() method, it deletes all backup data stored in Volume Shadow Copy Service (VSS), preventing victims from restoring data through system restore features.

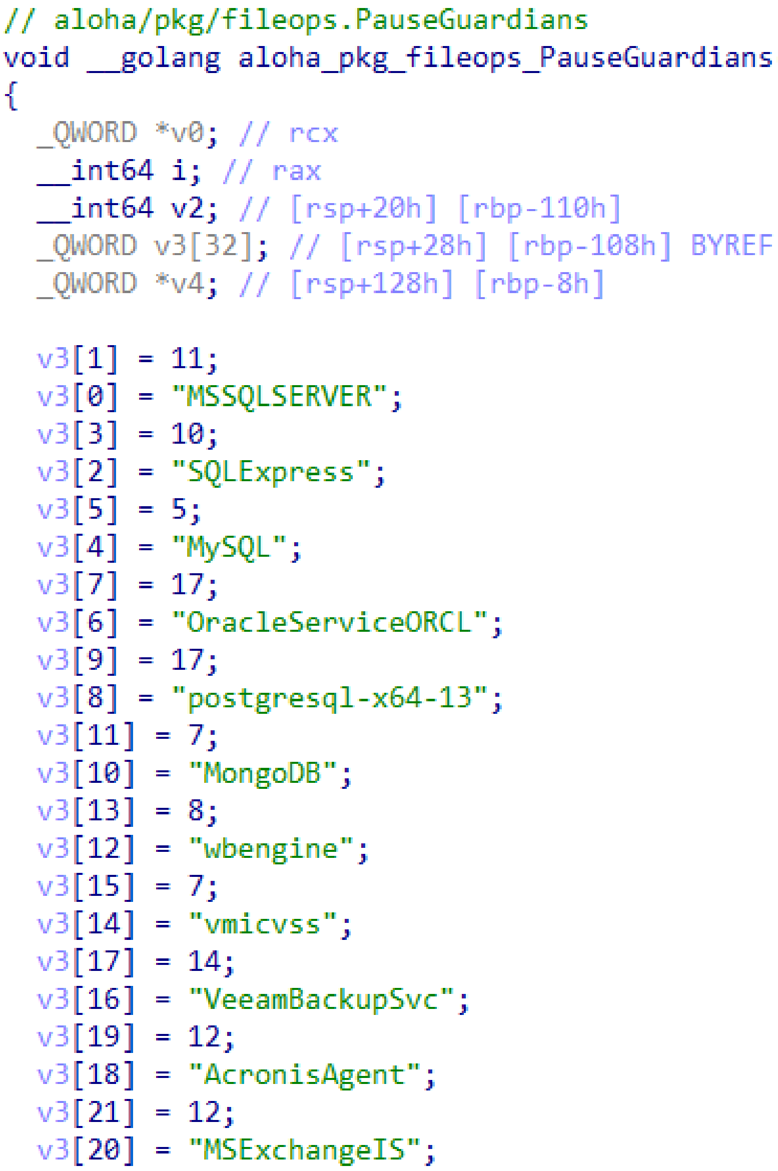


```
// aloha/pkg/fileops.Housekeeping
error __golang aloha_pkg_fileops_Housekeeping()
{
  _ptr_exec_Cmd v0; // rax
  error v3; // kr00_16
  _QWORD v4[8]; // [rsp+0h] [rbp-40h] BYREF
  error result; // 0:rax.8,8:rbx.8

  v4[1] = 6;
  v4[0] = "delete";
  v4[3] = 7;
  v4[2] = "shadows";
  v4[5] = 4;
  v4[4] = "/all";
  v4[7] = 6;
  v4[6] = "/quiet";
  os_exec_Command((__int64)"vssadmin", 8, (__int64)v4, 4, 4);
  v3 = os_exec__ptr_Cmd_Run(v0);
  result.data = v3.data;
  result.tab = v3.tab;
  return result;
}
```

Figure 4. Volume shadow data deletion

Service Suspension

The ransomware forcibly stops key services to block recovery attempts and increase the success rate of encryption. It stops backup services such as VeeamBackupSvc, wbengine (Windows Backup Engine), and AcronisAgent through the PauseGuardians() method. It also terminates database-related services such as MSSQLSERVER, SQLExpress, and MongoDB, releasing any file locks these services may hold and allowing the malware to carry out encryption successfully.



```
// aloha/pkg/fileops.PauseGuardians
void __golang aloha_pkg_fileops_PauseGuardians()
{
  _QWORD *v0; // rcx
  __int64 i; // rax
  __int64 v2; // [rsp+20h] [rbp-110h]
  _QWORD v3[32]; // [rsp+28h] [rbp-108h] BYREF
  _QWORD *v4; // [rsp+128h] [rbp-8h]

  v3[1] = 11;
  v3[0] = "MSSQLSERVER";
  v3[3] = 10;
  v3[2] = "SQLExpress";
  v3[5] = 5;
  v3[4] = "MySQL";
  v3[7] = 17;
  v3[6] = "OracleServiceORCL";
  v3[9] = 17;
  v3[8] = "postgresql-x64-13";
  v3[11] = 7;
  v3[10] = "MongoDB";
  v3[13] = 8;
  v3[12] = "wbengine";
  v3[15] = 7;
  v3[14] = "vmicvss";
  v3[17] = 14;
  v3[16] = "VeeamBackupSvc";
  v3[19] = 12;
  v3[18] = "AcronisAgent";
  v3[21] = 12;
  v3[20] = "MSExchangeIS";
```

Figure 5. Some of the services targeted for suspension

Preparing for Encryption

The ransomware excludes specific files and folders from encryption to maintain system stability. Major directories required for system operation, such as Windows and Program Files, as well as execution-related files such as .exe, .dll, and .sys, are excluded. Also, files that are already encrypted (*.sss) and the ransom note (recover.txt) that provides instructions for paying the decryption fee are excluded from encryption.

Targets Excluded from Encryption
Extensions: .sys, .exe, .dll, .com, .scr, .bat, .vbs, .ps1, .lnk, .inf, .reg, .msi, .ini, .sss *(extensions of files encrypted by the ransomware)* File names: boot.ini, bootmgr, bcd, desktop.ini, config.sys, autoexec.bat, recover.txt *(ransom note)*, pic.bmp Path: Windows, Users, Program Files, Program Files (x86), ProgramData, $Recycle.Bin, System Volume Information

Table 1 Targets excluded from encryption

Users Excluded from Encryption
All Users, Default, Default User, DefaultAccount, Public

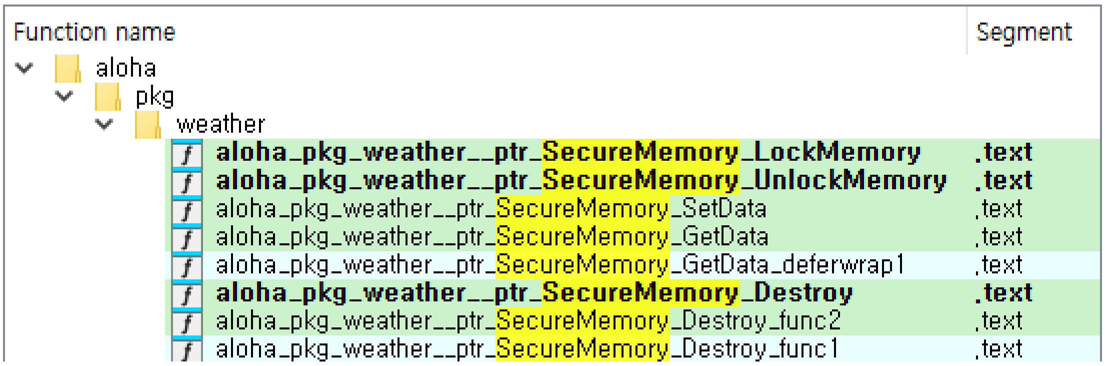
Table 2. Users excluded from encryption

Although the "Users" directory appears in the excluded paths listed in Table 1, encryption is still carried out on user-created accounts that do not fall under Table 2. For these accounts, the subdirectories Desktop, Downloads, Documents, Pictures, Music, and Videos are encrypted. In addition, any detected drives other than the C: drive have all paths included as encryption targets.

File Encryption

The AES-CTR symmetric key encryption algorithm is used for file encryption. The key is generated by applying the SHA-256 function 10,000 times to a random 32-byte value generated using crypto/rand.Read(). A single AES-CTR key is reused across all files, rather than generating a different key for each file.

Therefore, since a single AES-CTR key can decrypt every encrypted file, keeping that key confidential is critical for the threat actor. To prevent it from being exposed, the threat actor implemented a custom SecureMemory structure and related methods that control how the key is stored, used, and destroyed, minimizing any chance of the key leaking.



Function name	Segment
aloha	
pkg	
weather	
aloha_pkg_weather__ptr_SecureMemory_LockMemory	**.text**
aloha_pkg_weather__ptr_SecureMemory_UnlockMemory	**.text**
aloha_pkg_weather__ptr_SecureMemory_SetData	.text
aloha_pkg_weather__ptr_SecureMemory_GetData	.text
aloha_pkg_weather__ptr_SecureMemory_GetData_deferwrap1	.text
aloha_pkg_weather__ptr_SecureMemory_Destroy	**.text**
aloha_pkg_weather__ptr_SecureMemory_Destroy_func2	.text
aloha_pkg_weather__ptr_SecureMemory_Destroy_func1	.text

Figure 6. SecureMemory structure and related methods

The following features are designed to reduce the risk of key exposure.

Paging Prevention - SecureMemory.LockMemory()/UnlockMemory()

Windows carries out internal page-out operations, which move old or infrequently used memory pages to the disk when memory becomes scarce. This creates a risk where the encryption key may be written to the disk file (page file) in plaintext and become exposed. The Cephalus malware uses the LockMemory() method to prevent this. This method internally calls the Windows API VirtualLock,[1] ensuring the encryption key is excluded from page-out operations. This prevents the key from ever appearing on the disk.

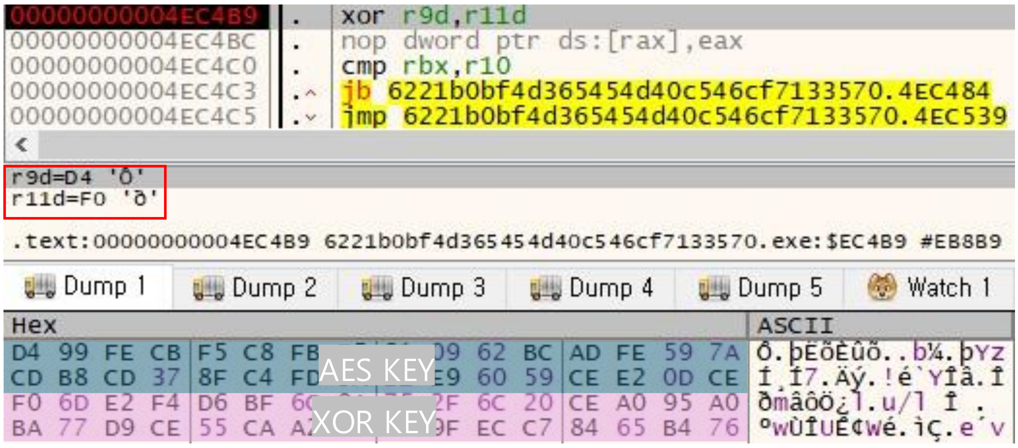
XOR-based Key Storage/Recovery – SecureMemory.SetData()/GetData()

Cephalus is designed not only to prevent the encryption key from being left behind on disk through paging, but also to reduce the chance of the key being exposed in memory. All access

[1] https://learn.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-virtuallock

to the key is handled through the SetData() and GetData() methods.

The SetData() method for storing keys does not save the encryption key as-is. Instead, it first performs an XOR operation with a randomly generated XOR key before storing it. As a result, in a typical memory dump scenario, only the AES key in its masked state after the XOR operation exists. As shown in Figure 7 below, you can see the AES key starting with 0xD4 being XORed with the XOR key starting with 0xF0.



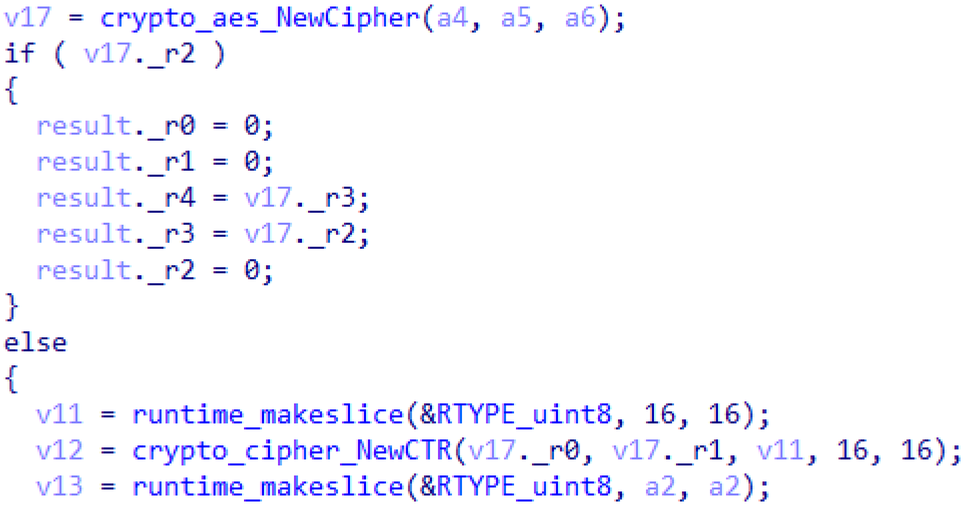
```
000000000004EC4B9 | .   | xor r9d,r11d
000000000004EC4BC | .   | nop dword ptr ds:[rax],eax
000000000004EC4C0 | .   | cmp rbx,r10
000000000004EC4C3 | .^  | jb 6221b0bf4d365454d40c546cf7133570.4EC484
000000000004EC4C5 | .v  | jmp 6221b0bf4d365454d40c546cf7133570.4EC539

r9d=D4 'Ô'
r11d=F0 'ð'

.text:000000000004EC4B9 6221b0bf4d365454d40c546cf7133570.exe:$EC4B9 #EB8B9
```

```
Hex                                                  ASCII
D4 99 FE CB  F5 C8 FB         09 62 BC  AD FE 59 7A  Ô.þËõÈûõ..b¼.þYz
CD B8 CD 37  8F C4 FD         E9 60 59  CE E2 0D CE  Í¸Í7.Äý.!é`YÎâ.Î
F0 6D E2 F4  D6 BF 6C         2F 6C 20  CE A0 95 A0  ðmâôÖ¿l.u/l Î .
BA 77 D9 CE  55 CA A          9F EC C7  84 65 B4 76  ºwÙÎUÊ¢wé.ìÇ.e´v
```

Figure 7. The process of XORing the original key

When the original AES key is needed for encrypting files, the GetData() method uses the same XOR key that was applied during storage to restore the original key, which is then used for encryption. Since this design limits the exposure of the real key in memory to the brief moment when GetData() is called, acquiring the original key through forensic analysis or recovery becomes extremely difficult.

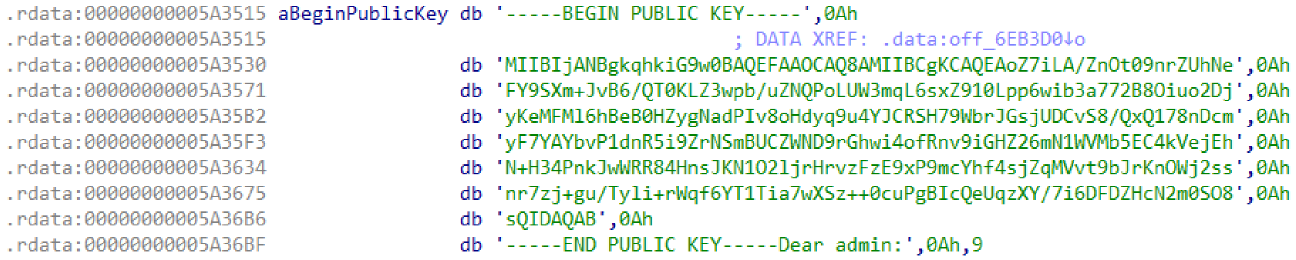
Afterward, it creates an encryption object configured for CTR mode, as shown in Figure 8, and uses it to encrypt files.



```
v17 = crypto_aes_NewCipher(a4, a5, a6);
if ( v17._r2 )
{
  result._r0 = 0;
  result._r1 = 0;
  result._r4 = v17._r3;
  result._r3 = v17._r2;
  result._r2 = 0;
}
else
{
  v11 = runtime_makeslice(&RTYPE_uint8, 16, 16);
  v12 = crypto_cipher_NewCTR(v17._r0, v17._r1, v11, 16, 16);
  v13 = runtime_makeslice(&RTYPE_uint8, a2, a2);
```

Figure 8. Creation of AES-CTR encryption object

From the threat actor's perspective, they must know the AES key in order to decrypt the encrypted files. To achieve this, Cephalus encrypts the AES key using the RSA public-key algorithm. The RSA public key embedded in the malware is encoded in PEM format and is restored through the process of the Go library's encoding/pem.Decode() and crypto/x509.ParsePKIXPublicKey() functions.



```
.rdata:00000000005A3515 aBeginPublicKey db '-----BEGIN PUBLIC KEY-----',0Ah
.rdata:00000000005A3515                                         ; DATA XREF: .data:off_6EB3D0↓o
.rdata:00000000005A3530                 db 'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoZ7iLA/ZnOt09nrZUhNe',0Ah
.rdata:00000000005A3571                 db 'FY9SXm+JvB6/QT0KLZ3wpb/uZNQPoLUW3mqL6sxZ910Lpp6wib3a772B8Oiuo2Dj',0Ah
.rdata:00000000005A35B2                 db 'yKeMFMl6hBeB0HZygNadPIv8oHdyq9u4YJCRSH79WbrJGsjUDCvS8/QxQ178nDcm',0Ah
.rdata:00000000005A35F3                 db 'yF7YAYbvP1dnR5i9ZrNSmBUCZWND9rGhwi4ofRnv9iGHZ26mN1WVMb5EC4kVejEh',0Ah
.rdata:00000000005A3634                 db 'N+H34PnkJwWRR84HnsJKN1O2ljrHrvzFzE9xP9mcYhf4sjZqMVvt9bJrKnOWj2ss',0Ah
.rdata:00000000005A3675                 db 'nr7zj+gu/Tyli+rWqf6YT1Tia7wXSz++0cuPgBIcQeUqzXY/7i6DFDZHcN2m0SO8',0Ah
.rdata:00000000005A36B6                 db 'sQIDAQAB',0Ah
.rdata:00000000005A36BF                 db '-----END PUBLIC KEY-----Dear admin:',0Ah,9
```

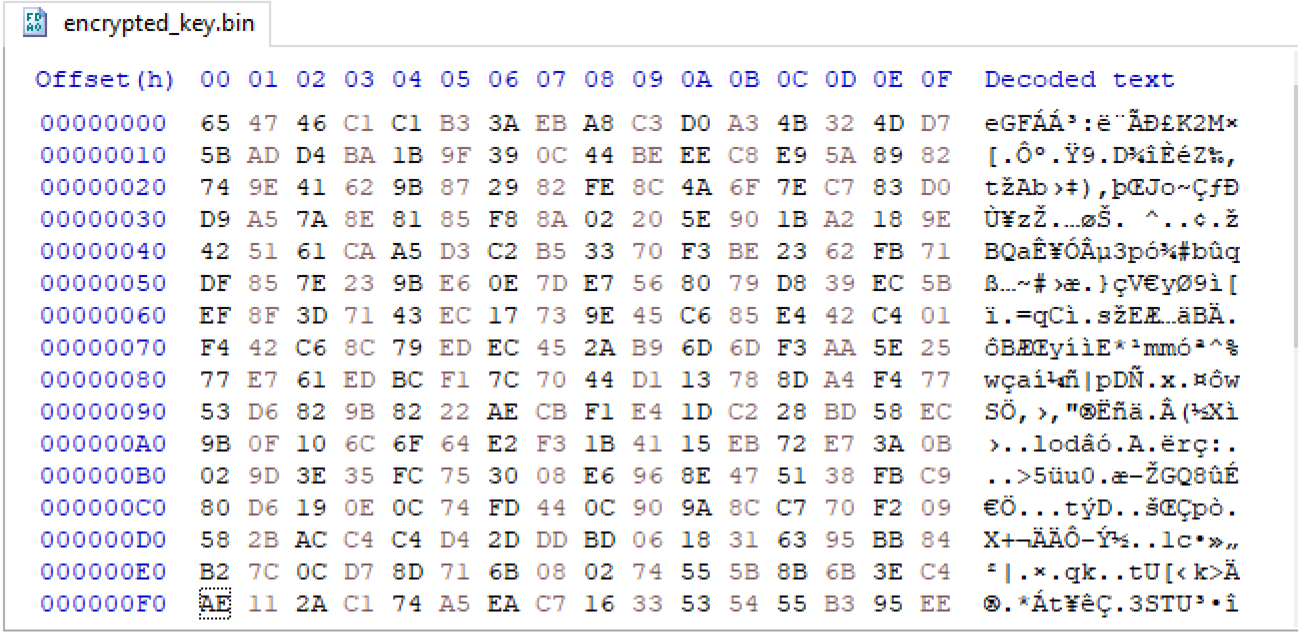
Figure 9. Threat actor's RSA public key

Once the AES-CTR key is encrypted with the threat actor's RSA public key, only the threat actor with the corresponding RSA private key can decrypt it.

Key Storage

The AES key encrypted with the RSA public key is stored redundantly in the following three locations rather than a single path.

- %TEMP%\encrypted_key.bin
- %APPDATA%\.system_cache
- %LOCALAPPDATA%\temp.dat



encrypted_key.bin

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  65 47 46 C1 C1 B3 3A EB A8 C3 D0 A3 4B 32 4D D7  eGFÁÁ³:ë¨ÃÐ£K2M×
00000010  5B AD D4 BA 1B 9F 39 0C 44 BE EE C8 E9 5A 89 82  [.Ôº.Ÿ9.D¾îÈéZ‰‚
00000020  74 9E 41 62 9B 87 29 82 FE 8C 4A 6F 7E C7 83 D0  tžAb›‡)‚þŒJo~ÇƒÐ
00000030  D9 A5 7A 8E 81 85 F8 8A 02 20 5E 90 1B A2 18 9E  Ù¥zŽ.…øŠ. ^..¢.ž
00000040  42 51 61 CA A5 D3 C2 B5 33 70 F3 BE 23 62 FB 71  BQaÊ¥ÓÂµ3pó¾#bûq
00000050  DF 85 7E 23 9B E6 0E 7D E7 56 80 79 D8 39 EC 5B  ß…~#›æ.}çV€yØ9ì[
00000060  EF 8F 3D 71 43 EC 17 73 9E 45 C6 85 E4 42 C4 01  ï.=qCì.sžEÆ…äBÄ.
00000070  F4 42 C6 8C 79 ED EC 45 2A B9 6D 6D F3 AA 5E 25  ôBÆŒyíìE*¹mmóª^%
00000080  77 E7 61 ED BC F1 7C 70 44 D1 13 78 8D A4 F4 77  wçaí¼ñ|pDÑ.x.¤ôw
00000090  53 D6 82 9B 82 22 AE CB F1 E4 1D C2 28 BD 58 EC  SÖ‚›‚"®ËñäÂ(½Xì
000000A0  9B 0F 10 6C 6F 64 E2 F3 1B 41 15 EB 72 E7 3A 0B  ›..lodâó.A.ërç:.
000000B0  02 9D 3E 35 FC 75 30 08 E6 96 8E 47 51 38 FB C9  ..>5üu0.æ–ŽGQ8ûÉ
000000C0  80 D6 19 0E 0C 74 FD 44 0C 90 9A 8C C7 70 F2 09  €Ö...týD..šŒÇpò.
000000D0  58 2B AC C4 C4 D4 2D DD BD 06 18 31 63 95 BB 84  X+¬ÄÄÔ-Ý½..1c•»„
000000E0  B2 7C 0C D7 8D 71 6B 08 02 74 55 5B 8B 6B 3E C4  ²|.×.qk..tU[‹k>Ä
000000F0  AE 11 2A C1 74 A5 EA C7 16 33 53 54 55 B3 95 EE  ®.*Át¥êÇ.3STU³•î
```

Figure 10. AES key encrypted with the RSA public key

By collecting the files in these locations and decrypting them with the RSA private key, the threat actor can obtain the AES key and use it to decrypt the encrypted files.

Ransom Note

Figure 11 shows the screen infected by Cephalus ransomware. The desktop background remains unchanged. The ransom note is named "recover.txt" and is created in every path where encryption has finished.

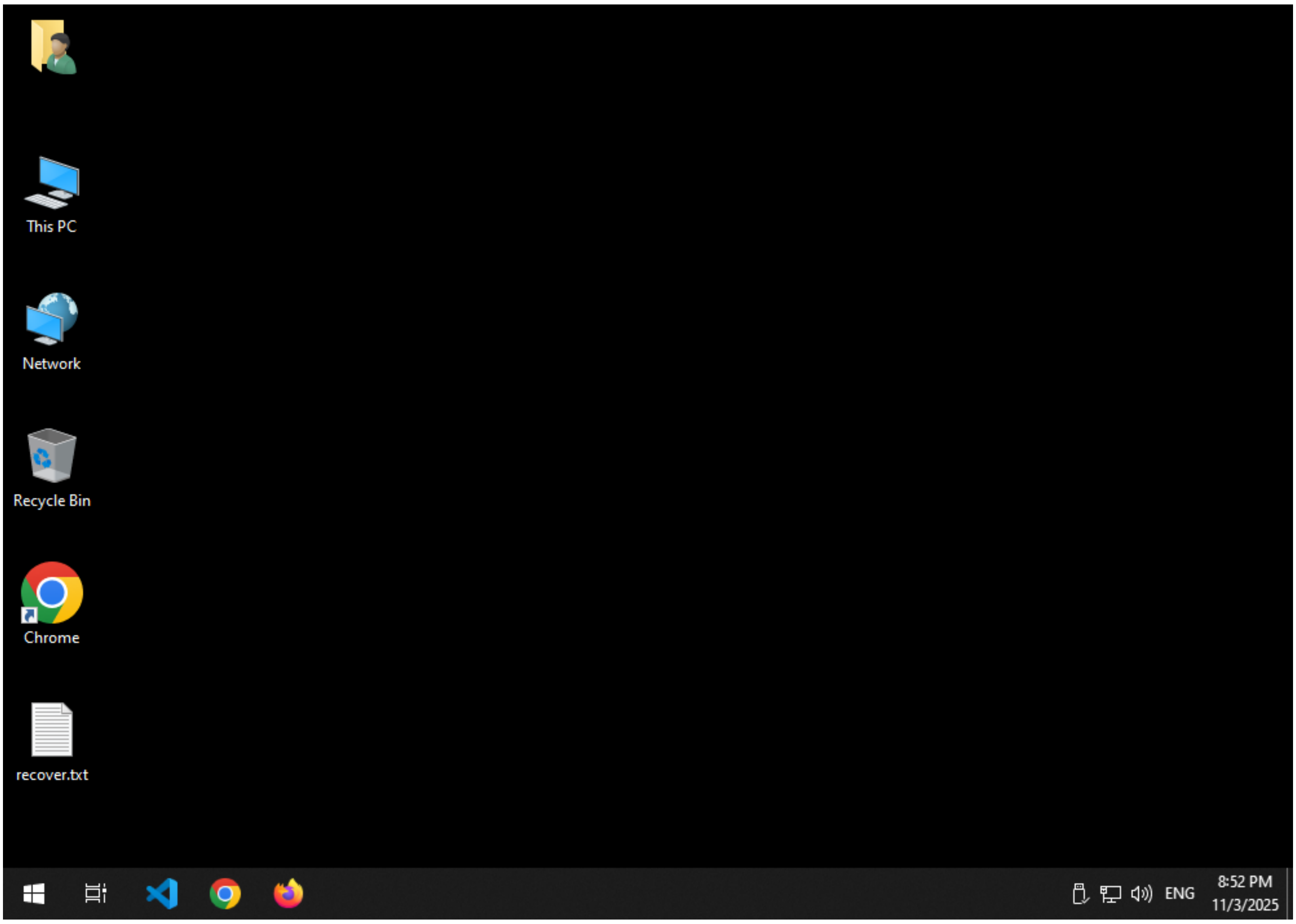
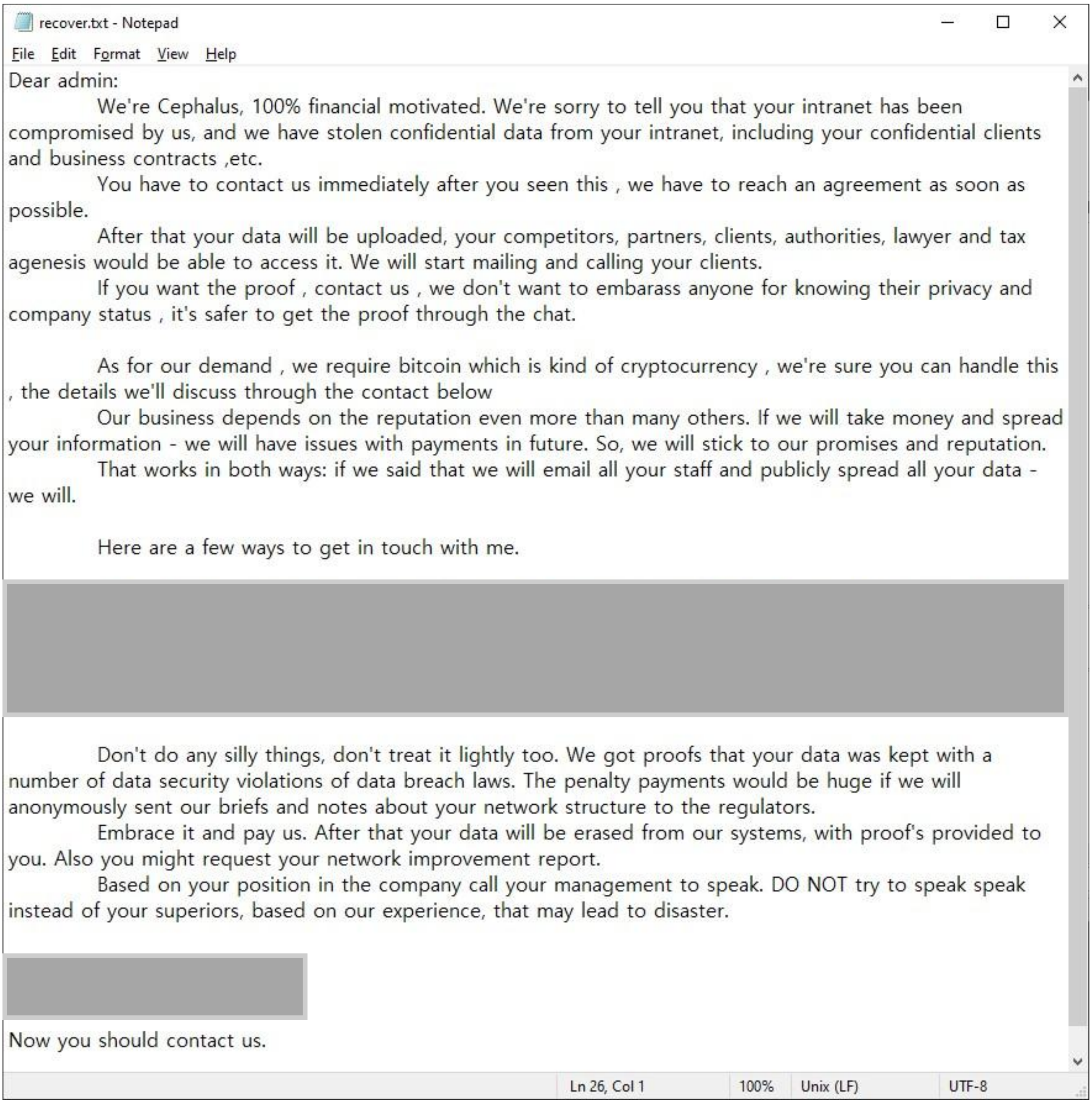


Figure 11. After encryption is completed

The ransom note alerts the victim that their data has been both encrypted and exfiltrated, applying pressure to them. The threat actor warns that if the victim does not contact them within the specified deadline, the stolen data will be leaked to competitors or business partners. They also claim that the victim's current data management practices violate security regulations, and that reporting the incident to authorities could result in immediate fines. Finally, the threat actor emphasizes that their motive is purely financial.



Dear admin:

We're Cephalus, 100% financial motivated. We're sorry to tell you that your intranet has been compromised by us, and we have stolen confidential data from your intranet, including your confidential clients and business contracts ,etc.

You have to contact us immediately after you seen this , we have to reach an agreement as soon as possible.

After that your data will be uploaded, your competitors, partners, clients, authorities, lawyer and tax agenesis would be able to access it. We will start mailing and calling your clients.

If you want the proof , contact us , we don't want to embarass anyone for knowing their privacy and company status , it's safer to get the proof through the chat.

As for our demand , we require bitcoin which is kind of cryptocurrency , we're sure you can handle this , the details we'll discuss through the contact below

Our business depends on the reputation even more than many others. If we will take money and spread your information - we will have issues with payments in future. So, we will stick to our promises and reputation.

That works in both ways: if we said that we will email all your staff and publicly spread all your data - we will.

Here are a few ways to get in touch with me.

[redacted]

Don't do any silly things, don't treat it lightly too. We got proofs that your data was kept with a number of data security violations of data breach laws. The penalty payments would be huge if we will anonymously sent our briefs and notes about your network structure to the regulators.

Embrace it and pay us. After that your data will be erased from our systems, with proof's provided to you. Also you might request your network improvement report.

Based on your position in the company call your management to speak. DO NOT try to speak speak instead of your superiors, based on our experience, that may lead to disaster.

[redacted]

Now you should contact us.

Figure 12. Ransom note (recover.txt).

AhnLab Response Overview

The detection names and the engine date information of AhnLab products are shown below.

V3

Ransom/MDP.Behavior.M2813 (2021.10.08.00) Ransom/MDP.Decoy.M1171 (2024.09.06.02) Ransom/MDP.Event.M1785 (2024.08.20.03) Ransomware/Win.Cephalus.C5792414 (2025.08.27.04) Ransomware/Win.Cephalus.C5792774 (2025.08.28.02)

EDR

SystemManipulation/EDR.Event.M2486 (2024.04.22.03)

Conclusion

Since emerging in June 2025, the Cephalus ransomware group has carried out financially motivated attacks targeting legal, financial, and government institutions across multiple countries, including the United States and Japan. As shown in this report, Cephalus attempts to block recovery by deleting VSS backups and disabling security features such as Windows Defender. It also applies pressure through ransom notes and implements techniques that minimize exposure of the encryption key, making it significantly harder to recover encrypted files.

Therefore, companies are advised to strictly follow the response guidelines below to protect their key assets and ensure stable operations.

Response Guide

Users should prepare for ransomware by backing up important data to an offsite location separate from the service network, controlling access to backup storage, and regularly practicing recovery. It is essential to go beyond simple backups and take strategic steps to secure the backup system and ensure that recovery is possible.

In addition, companies must strictly follow the security rules below.

- Apply the latest security updates and enable automatic updates for operating systems and software
- Install and use security software, and always keep it up to date
- Back up data regularly and store said data in an offline site or separate network
- Be cautious of websites from unreliable sources and viewing/executing email links and attachments
- Use strong passwords and two-factor authentication (2FA)

IoCs (Indicators of Compromise)

File Hashes (MD5s)

The MD5s of the related files are as follows.

```
6221B0BF4D365454D40C546CF7133570
A16A1228D5276EEC526C21432A403923
```

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
https://www.ahnlab.com | https://asec.ahnlab.com/en

About ASEC

AhnLab SEcurity intelligence Center (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.