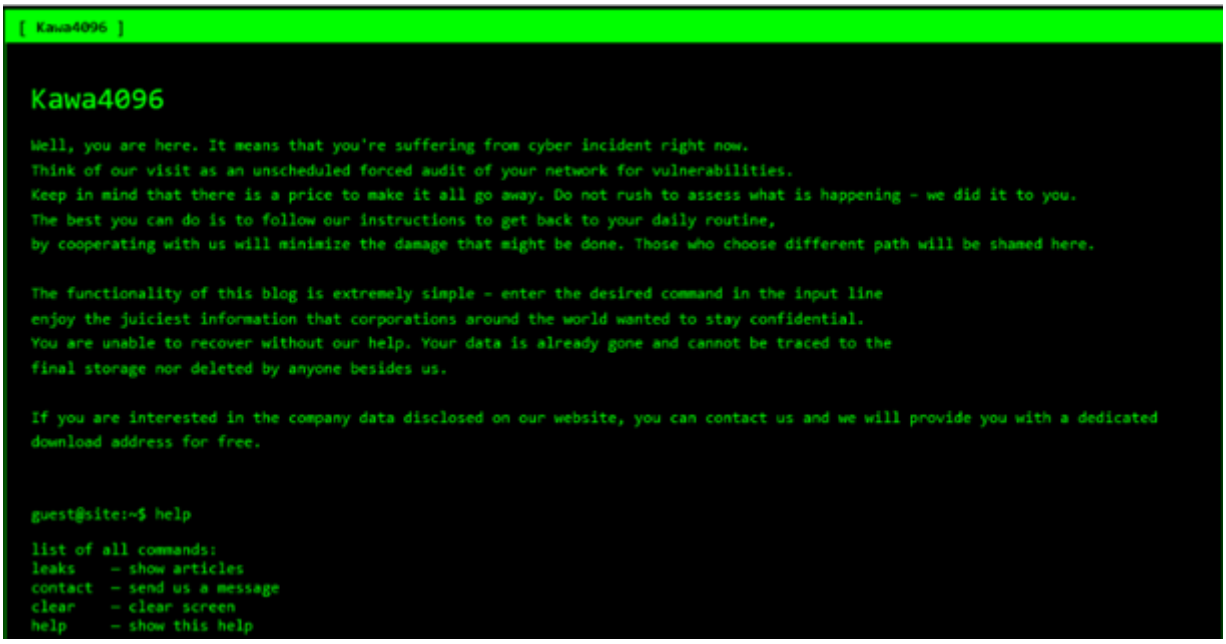
Kawa4096 Ransomware Aimed at Brand Effect through Imitation

⋮ 9/17/2025

In June 2025, a new ransomware group, Kawa4096, appeared. It targets multinational organizations, including Japan and the United States, and is not limited to specific industries, such as finance/education/services. Whether RaaS (Ransomware-as-a-Service) is operational or has not yet been publicly confirmed, but it has attracted attention by attacking organizations in various countries over a relatively short period of time.

1. About

According to the Kawa4096 attack group's operations and features, it operates Tor-based data breach sites and discloses victim information. It appears to use a double extortion method that steals and encrypts data after an attack. In addition, we are managing data access by providing dedicated claim URLs for each victim, suggesting an organized and systematic operating structure. No specific information on the scope of the ransom amount or the manner of the negotiation has yet been made public.



[Fig] Data Leak Site of Kawa4096 Ransomware

2. Analysis

2.1 Early routines

The Kawa4095 ransomware is notable for re-running with the -all argument if there are no -all arguments when running. When re-running with the -all argument, the entire encryption process is performed on the basic encrypted files.

```
132 LABEL_76:
133         printf("-d=directory\n");
134         printf("-all\n");
135         printf("-dump [optional]\n");
136         exit(0);
137       }
138       v24 = 1;
139       v25 = v7 + 1;
140       while ( 1 )
141       {
142         v26 = *v25;
143         if ( *v25 && *v26 == 45 )
144         {
145           do
146             ++v26;
147           while ( *v26 == 45 );
148           v27 = L"all";
149           while ( *v26 && *v27 == *v26 )
150           {
151             ++v27;
152             ++v26;
153             if ( !*v27 )
154               goto LABEL_55;
155           }
```

[Fig] Kawa4096 Ransomware Execution Options

The following activities by encryption options are:

- -d=<directory> : Perform encryption for the specified directory
- -all : Perform encryption for all encrypted files
- -dump : Using the MiniDumpWriteDump API, create a ".dmp" file containing crash information in the folder that ran the ransomware

The Kawa4096 ransomware also creates a mutex named 'SAY_HI_2025' to prevent duplicate execution. If ransomware were executed more than once on the same host, they were concerned that they would encrypt the same files with each other and cause conflicts or slowdowns. Use the CreateMutexA API to create a unique name (SAY_HI_2025) and, if it already exists, terminate the ransomware process immediately so that it is executed only once.

```
84    MutexA = CreateMutexA(0LL, 1, "SAY_HI_2025");
85    a1[196] = MutexA;
86    if ( !MutexA || GetLastError() == 183 )
87      return printf("another instance already running.\n");
88  }
```

[Fig] 'SAY_HI_2025' Mutex Code

This determines the behavior by reading the settings that exist in the resources section inside the executable to the API, such as LoadResource / FindResourceW . The configuration includes a number of fields, including ext/dirs/files, a designated encryption directory, a list of processes and services to be terminated, and so on. I want to explain this in more detail in the next chapter of the "Encryption Preparation" chapter.

2.2 Preparation for encryption

Seventeen fields are identified in the configuration values of the Ransomware Resources section analyzed in the text, where only five items are described. A detailed description of each field can be found in the body of the analysis report.

XML Element	Explanations and examples
	Exclusion rules – Excluding extensions List
skip_exts value	Listed extension files are excluded from the encryption target. It is intended to maintain system stability and accessibility, such as execution, driver, system, and shortcuts. .ani; .cab; .dll; .ico; .lnk; .scr; .sys; .exe; .bat; .cmd and many others
The skip_dirs value	**Exclude encryption rules – list of exclusions from encrypted directories** The directory listed is skipped when recurring. It is encrypted, but it is intended to avoid the destruction of the OS/application itself and to preserve the negotiable state.

	All Users; PerfLogs; Program Files (x86); Program Files; and many others
skip_files value	**Exclude encryption rules – list of non-encrypted file names** The exact file name is excluded from encryption. It is believed that the user profile, boot, auto-run, etc., protected and prevented from booting, were intended to avoid scenarios that could not be booted. boot.ini; desktop.ini; bootmgr; thumbs.db; autorun.inf and many others
specify_dirs enable, value	**Restrict the scope of the encryption target** Option to restrict only specified directories to be encrypted. The option of enable = “0” is disabled, which means that it performs a global (local/network) search. The value itself entered in value represents the possibility of targeting DB data with the SQL Server path, but is currently unused as an option of enable = “0”. <specify_dirs enable=”0″ value=”C:\\Program Files (x86)\\Microsoft SQL Server;C:\\Program Files\\Microsoft SQL Server;" />
kill_process value	**Process Pre-Cleanup Steps – Process End List** Exit for the purpose of unlocking files, interrupting backups, and disrupting surveillance/recovery. sqlservr.exe; excel.exe; firefox.exe; notepad.exe; outlook.exe; powerpnt.exe; winword.exe; wordpad.exe; and many others

[Table] Settings values & descriptions present in the Resources section of Ransomware (partially)

2.3 File encryption

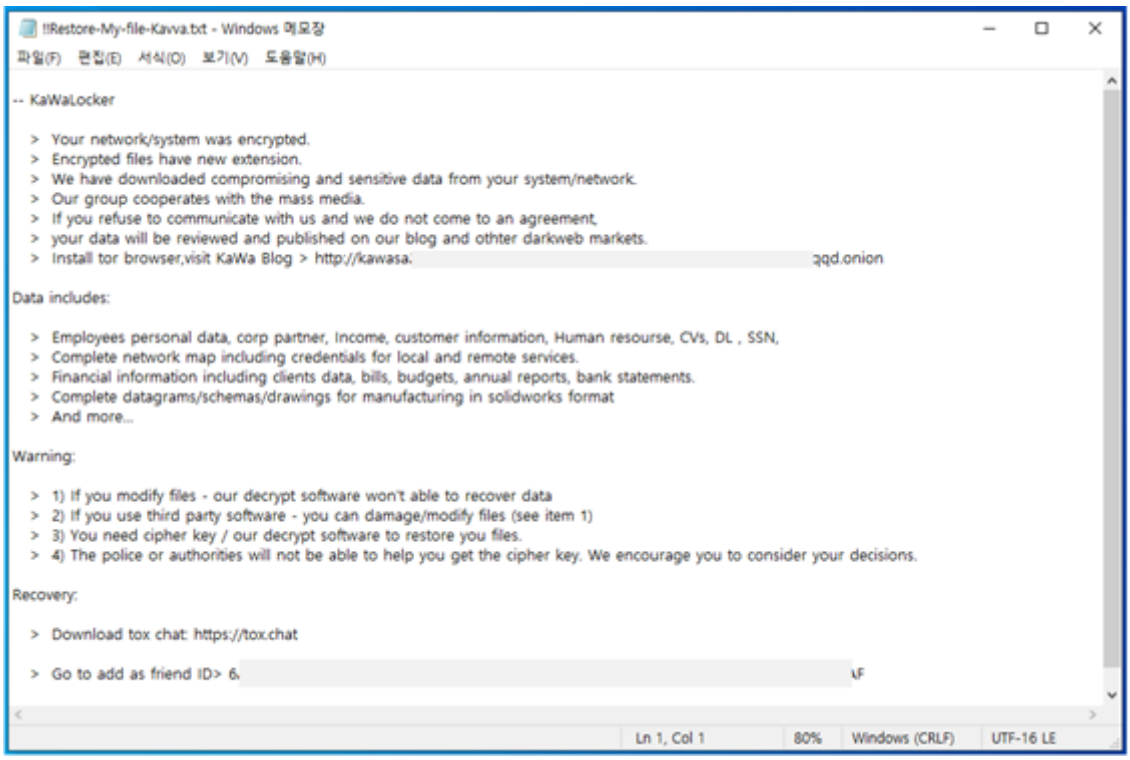
Kawa4096 Ransomware selects the right extension/directory for the configuration during the execution process, and excludes system files and key files from the encryption target. In addition, a partial encryption option method has been adopted. This option, which can be viewed in the configuration file with <partial value=”25” />, aims to greatly increase encryption speed and efficiency by encrypting only a part of each file, not all. If the file size is large, 100% encryption will take a long time. Thus, it is intended to encrypt as many files as possible in a short time by encrypting only a part of the file. In addition, files such as documents/DB/compressed files, such as headers/indexes, are actually not opened or executed by the file itself even if they are broken, such as headers/indexes, and cannot be executed, so even if they are not fully encrypted, the system damage intended to be made is possible.

In the Kawa4096 ransomware, the logic of encrypting chunks was confirmed. For example, after dividing the file into chunks of 64KB (0x10000), only 25% of the chunks are selected to encrypt. In general, partial encryption is applied when the size of a file is greater than 10MB, and if a file smaller than 10MB, a pattern of handling it with full or weak partial encryption is common. Once the number of chunks is determined, the encryption is performed using the Salsa20 stream password, and the encrypted file is <original filename>. "Expansion". It has an extension in the form of a random English language and a combination of numbers of nine characters. It is important to note that exactly how you use it can vary from sample to sample of publicly available malware.

2.4 Ransomnotes

The Kawa4096 ransomware has a high similarity to the ransomware of Qilin Ransomware. The content and format are almost identical to the Qilin Ransomnote, which informs them of the attack, provides data breaches, public threats (double intimidation), and decryption/negotiation contact information.

!! The ransomware note of the Restore-My-file-Kavva.txt file name is created in each encrypted folder and at the root of the system. The contact channel includes the Tor browser-based onion site address and QTOX ID, which leads the victim to attempt to negotiate/pay. In addition, the ransom pressure is applied by listing the types of data stolen from the ransomware note (customer information/employee information/financial data, etc.) or by threatening to disclose the damage. In fact, the case of the customer's information is disclosed as confirmed in the 8p in the body of the report.



[Fig] Kawa4096 Ransomware

2.5 Delete backup data

The Kawa4096 ransomware triggers the run of the process with Win32_Process:Create in WMI to execute

commands related to volume shadow copies. The instructions used in this process are as follows.

- vssadmin.exe Delete Shadows /all /quiet: Delete all shadow copies
- wmic shadowcopy delete /nointerface : Delete a batch of shadow copies via WMIC

```
35  wcscpy(Destination, L"vssadmin.exe dele");
36  memset(&Destination[18], 0, 0xA4uLL);
37  wcscat_s(Destination, 0x64uLL, L"te shadows /all /quiet");
38  sub_140001110(Destination);
39  v10 = 0;
40  v5 = GetModuleHandleA("kernel32.dll");
41  result = GetProcAddress(v5, "IsWow64Process");
```

[Fig] Kawa4096 Ransomware Volume Shadow Copy Deletion Code

This is believed to have completely neutralized the backup recovery method, thus blocking the victim's attempts to recover.

3. Status of Ahn Lab Response

The diagnostic name of the Ahn Lab family and the engine date information are as follows.

3.1 V3 Diagnosis
Ransomware/Win.KawaCrypt.C5774792 (2025.07.02.02)
Ransomware/Win.KawaCrypt.C5783637 (2025.07.30.03)
Ransomware/Win.KawaLocker.C5791069 (2025.08.2.02)
Ransom/MDP.Command.M1026 (2016.04.08.03)
Ransom/MDP.Decoy.M1171 (2016.07.15.02)
Ransom/MDP.Event.M1785 (2017.11.28.00)

3.2 EDR Diagnostics
Suspicious/MDP.Behavior.M1961 (2018.11.06.02)
SystemManipulation/EDR.Event.M2592 (2022.03.31.00)
SystemManipulation/EDR.Event.M2486 (2022.07.09.00)
Ransom/EDR.Decoy.M2470 (2022.09.30.00)
Ransom/DETECT.T1486. M11751 (2024.06.04.02)

MD5

0bf4def902e36cc9174d89c14ec3dcac

64756bf452baa4da411e3a835c08d884

c3ce46d40b2893e30bf00fce72c2e1fa

추가 IoC는 ATIP에서 제공됩니다.