

Revealing the Abyss Ransomware

 idanmalihi.com/revealing-the-abyss-ransomware/



[Skip to content](#)

Idan Malihi

Security Researcher

Executive Summary

Abyss Ransomware emerged in early 2023, and it was immediately clear to the global security community that it posed a dangerous new threat. Therefore, a thorough examination is required of its features and consequences. It is typically spread through phishing emails and then infiltrates targeted systems. Once it has gained access, Abyss encrypts critical files in the victim's network using lateral movement techniques and advanced cryptographic algorithms, posing a significant risk to the affected organization.

In this report, I will provide a detailed analysis of Abyss Ransomware's tactics, techniques, and procedures. Additionally, I will include the MITRE ATT&CK matrix at the end of the report, which outlines the ransomware's tactics, techniques, and procedures (TTPs).

Technical Analysis

File Name: Abyss.exe

File Type: Portable Executable

Architecture: 64-bit

Size: 216KB

MD5: 5620e71084c3bdc87a2522d4f5ad548a

SHA256: 837b3ddaaa7f209aac10480b43c248c20caaea2154ea13ef707e675a50bb2747

Ransomware Execution Diagram

Static Analysis

The ransomware is a portable executable 64-bit architecture, and the ransomware was programmed in C++ programming language.

Compilation Time

The compilation date of the ransomware is May 15, 2023.

Strings

Based on the output provided by the string extraction, we can expect a ransom note to appear after the execution of the program. This note will provide crucial information about the threat actors, including their identity, motives, negotiation tactics, and terms of the ransom. A

detailed analysis of the ransom note will be included in the dissection section.

During Abyss ransomware execution, a new log file may be created, and logs may be written to it.

The ransomware will destroy the contents of files and then change their extension to .XPbS1.

The ransomware executes specific commands to delete shadow copies, making it difficult to restore data from backups.

```
/c vssadmin.exe delete shadows /all /quiet  
/c wmic SHADOWCOPY DELETE
```

The ransomware executes the following commands to prevent the system from entering recovery mode.

```
/c bcdedit / set{ default } recoveryenabled No  
/c bcdedit / set{ default } bootstatuspolicy ignoreallfailures
```

When the ransomware is executed, it attempts to infect any external drives present in the system and creates an autorun file.

The ransomware will create two files in the system — a JPG file and a TXT file.

The Abyss ransomware will attempt to perform lateral movement techniques within the local network by searching for SMB shares, external drives, and other accessible resources.

DLL File Usage

The ransomware executes multiple DLL files during execution:

Dissecting the Ransomware

The ransomware initiates its operation by producing a log file named 'work.log' through the `CreateFileW` function, which records its operations, such as the encryption process, targeted files, and errors. This log can be helpful for the threat actors to determine the success or failure of the ransomware execution.

When the ransomware creates the 'work.log' file, it adds the file to an exclusion list. The ransomware loads the effective address of the 'work.log' string into the `rax` register. Then, it moves the `rax` register content to the 'cs:qword_140033CA0' memory location, which indicates an exclusions list.

The 'cs:qword_140033CA0' content:

Additionally, the ransomware loads the effective address of the '.XPbS1' string into the rax register. Then, it moves the rax register content to the 'cs:qword_140033A60' memory location, which indicates an exclusion list with files' extensions.

The 'cs:qword_140033A60' content:

The ransomware uses the GetTickCount function to obtain the number of milliseconds since the system started. This technique is used to avoid detection in sandboxes or virtual machines. Additionally, the ransomware establishes a connection with the Windows Service Control Manager using the OpenSCManagerA function. It then goes through a list of service names, which are pointed to off_140009990, and tries to open each service using the OpenServiceA function.

Then, for each service, it queries the service status using the QueryServiceStatusEx function. The ransomware checks the service state using the 'Buffer.dwCurrentState -1'.

The ransomware targets services related to security products, such as Windows Defender and Sophos. Also, the ransomware targets services of database management systems, for example, MSSQLServer, MySQL, and corporate software such as IBM Domino and QuickBooks. These services and software are usually targeted because they contain valuable data. Furthermore, the ransomware disables critical services in the organization, such as Microsoft Exchange and SharePoint, and data backup and recovery services, such as Veeam, and Acronis.

Therefore, if the service is not in a 'running' state, it attempts to start the service using the ControlService function and waits for the service to start. The ransomware uses the Sleep function to pause execution for a specific duration between service control operations.

The ransomware uses the CreateToolhelp32Snapshot function to create a snapshot of current processes running on the host system. It then compares the list of running processes with an executable names list, which is pointed to an item named 'off_140009E90', using the Process32FirstW and Process32NextW functions. If a match is found, the malware uses the OpenProcess function to open and handle the process and the TerminateProcess function to terminate the process.

The processes list (off_140009E90):

After the ransomware actions, it executes four commands using the ShellExecuteW function. The goal of these commands is to prevent the victim from entering recovery mode and to remove shadow copies to prevent data restoration from backups.

```
/c vssadmin.exe delete shadows /all /quiet  
/c wmic SHADOWCOPY DELETE  
/c bcdedit / set{ default } recoveryenabled No  
/c bcdedit / set{ default } bootstatuspolicy ignoreallfailures
```

Then, it sets up a semaphore (hSemaphore) and a handle (hHandle) for thread synchronization. Before the synchronization, the ransomware uses the GetSystemInfo function to retrieve information about the system and the number of processors. Based on the number of processors, the ransomware adjusts the number of threads (nCount) and initializes several handles for synchronization.

The subroutine 'sub_14001A4F0' uses semaphore thread synchronization and calls the CreateSemaphoreA function.

The ransomware creates multiple threads using the CreateThread API to execute the 'sub_14001C870' subroutine concurrently. These threads appear to be assigned tasks related to network shares and paths.

The ransomware performs network share searches in the 'sub_14001CB80' subroutine.

In the 'sub_14001CB80' subroutine code, the ransomware uses the NetShareEnum function to search through the network shares and disk devices present in the host. The ransomware disregards any hidden administrative shares (ADMIN\$) and records the paths of the detected

network shares in the 'sub_14001A240' subroutine.

The ransomware uses several functions to enumerate and determine the type of drives in the system.

In the 'sub_14001A740' subroutine, the ransomware iterates through the predefined drive letters and checks the drive type using the `GetDriveTypeW` function. It enumerates fixed and removable drives on the system. For each drive with drive type 1 (`DRIVE_FIXED`), it attempts to assign a corresponding drive letter to the volume using the `SetVolumeMountPointW` function.

Also, in the 'sub_14001CD20' subroutine, the ransomware constructs the drive path in the format \\?\X: where 'X' is the drive letter. It uses GetDriveTypeW to determine the type of the drive, whether it's removable, fixed, or network. If the drive type is 1 (root path), 2 (removable drive), or 3 (fixed drive), it logs information and processes the drive path further.

After the ransomware enumerates network shares and logical drives, it starts the encryption operation. The ransomware uses the FindFirstFileW and FindNextFileW functions to go through every file in every directory and sub-directory.

The CreateFileW function is used in a loop to create the WhatHappened.txt file in the file system and write the ransom note content using the WriteFile function.

Ransom Note Analysis

The threat group, known as Abyss, informs the victim about the situation:

The threat actors state that they can restore the files on the file system. They claim their motive is purely financial and open to negotiation.

The threat actors offer two options to the victim. The first option is to seek help from authorities, but the threat actors threaten to cause the company to face fines, legal actions, and reputational damage if they try to help with the decryption. The second option is to negotiate with the threat actors, pay the ransom, and receive the decryption. Importantly, the victim's privacy will be maintained, and no one will know about the incident.

The attackers instruct the company to access a specific URL using the TOR browser to initiate negotiations.

The Full Ransom Note

The ransomware uses the GetTempPathW function to acquire the temporary path, where it creates the file 'readme.bmp' using CreateFileW and writes content using the WriteFile API function.

BMP is short for bitmap, and it is an image file that contains bitmap graphics data.

The BMP content is the ransom note that the ransom spread in the file system earlier.

The ransomware opened the 'HKEY_CURRENT_USER\Control Panel\Desktop' registry path using the RegOpenKeyExW function. It edited the 'WallpaperStyle' and 'TileWallpaper' entries to 0 using the RegSetValueExW API.

As a result, the Desktop wallpaper is changed to the ransom note.

Conclusion

The emergence of Abyss Ransomware, which was unknown before March 2023, is a significant and dynamic threat that requires organizations to maintain a vigilant and adaptive cybersecurity posture. Its intricate infiltration tactics, combined with its potent encryption mechanisms and lateral movement techniques, make proactive measures critically important. Although its attribution remains elusive, and little is known behind the threat group promulgating the ransomware, the motive behind this threat is clearly financial gain, underscoring the organized and profit-driven nature of the threat.

Appendix: Technical Details

Indicators of Compromise (IoCs)

1. .XPbS1
2. 5620e71084c3bdc87a2522d4f5ad548a
3. 837b3ddaaa7f209aac10480b43c248c20caaea2154ea13ef707e675a50bb2747
4. %temp%\readme.bmp
5. WhatHappend.txt

MITRE ATT&CK Matrix

Yara Rule

Detection
