Arete

Malware Spotlight: **Fog Ransomware**

Executive Summary

Since April 2024, Arete's Incident Response (IR) team has responded to multiple engagements attributed to the Fog ransomware group. Engagements attributed to this group have been trending up since mid-June and through July 2024, accounting for nearly 20% of Arete's ransomware and extortion engagements in July. The Fog ransomware group is especially noteworthy as it is one of the few threat actors specifically targeting one industry: education. Since April, Arete has observed that 70% of Fog victims have been education organizations. This spotlight explores the ransomware group's observed behavior, background information on the threat actor, and statistics from Incident Response engagements, along with a technical analysis of Fog's ransomware executable. Finally, we discuss security recommendations to better defend against this evolving cyber threat and mitigate the risk of financial and reputation losses.

Incident Response Data on the Fog Ransomware Group

The information below is based on Fog ransomware incidents investigated by Arete since April 2024. Our IR, Threat Intelligence, and Data Analytics teams work together to analyze key data points during every ransomware engagement and form real-time threat actor (TA) insights.

- The median initial demand is $220,000.
- The median ransom payment facilitated is $100,000.
- 36% of engagements involved data exfiltration, often using tools like MEGAsync and Filezilla.
- Common initial access vectors include brute force attacks against remote desktop protocol (RDP) and compromised virtual private network (VPN) credentials.
- Tools observed during investigations include CobaltStrike, Mimikatz, ngrok, WinRAR, AnyDesk, Advanced Port Scanner, and GMER, among others. The group demonstrates distinct skill in evading common anti-malware defenses.
- The ransom note file name is commonly "readme.txt" and includes a link to a TOR site used for negotiations.
- The group operates a data leak site (DLS) self-proclaimed as "The Fog Blog."

Background

Fog ransomware was a prominent newcomer in the second quarter (Q2) of 2024 and demonstrated a noticeable trend of attacking entities in the education sector. Arete engagements involving Fog ransomware more than doubled during July 2024 compared to previous months.

Technical Analysis

Malware analysis revealed that Fog ransomware:

- Supports multiple command-line arguments.
- Encrypts files on the system and mounted shares.
- Adds the following extensions to encrypted files: .fog, .ffog, or .flocked (e.g., file.docx.flocked).
- Creates a ransom note with the following filename: readme.txt.
- Self-identifies the group as Fog in the ransom note.
- References a data leak site in the ransom note that, when accessed, self-identifies the group as Fog.
- Kills a list of processes and services.
- Maintains a list of whitelisted files and directories to make sure it will not render the system unusable, preventing recovery when running a decryptor.
- Attempts to prevent system recovery by deleting the system's volume shadow copies.
- Creates a mutex during execution.
- Creates a log file named DbgLog.sys.

Execution Pattern/Arguments

Fog ransomware needs command line arguments to execute and encrypt files in the system. Command line arguments supported:

Command line argument	Description
-id	Key to decrypt ransomware configuration.
-nomutex	Skip mutex check.
-target	Specific location to encrypt files.
-console	Creates a new console window for output.
-size	File size threshold to encrypt.
-log	Log the ransomware activity.
-procoff	Presently unknown.
-uncoff	Presently unknown.

The ransomware will not execute in the system without the “-id” argument followed by a 6-character value that is unique in each engagement.

Execution of ransomware to encrypt files:

```
Fog.exe -id [6-characters]

Example:
Fog.exe -id A9p3RZ
```

```
lea eax,dword ptr ss:[ebp-3EC]
cmp dword ptr ds:[eax],440049                eax:L"ID"
jne locker.40570D
movzx eax,word ptr ds:[eax+4]                eax:L"ID"
test ax,ax
jne locker.40570D
inc dword ptr ss:[ebp+8]
```

Figure 1. Code in the ransomware to check command line argument "-ID"

The ransomware uses the "-id" argument followed by a 6-character value to decrypt a JSON-based ransomware configuration information at runtime. Decrypted JSON field name and descriptions:

Name	Description
RSAPubKey	Public key used in the file encryption process.
LockedExt	Extension added to encrypted files.
NoteFileName	Ransom note name.
PathStopList	Excludes listed directories.
FileMaskStopList	Excludes listed file extensions.
ShutdownProcesses	Terminates list of processes.
ShutdownServices	Terminates list of services.

Stop Services and Processes

Before file encryption, the ransomware terminates a pre-determined list of processes and services to encrypt as many files as possible.

Process names:

"notepad.exe", "calc.exe", "*sql*"

Service names:

Code in the ransomware showing this operation:

"Dhcp", "Dnscache", "*sql*"

```
do
{
  if ( pe.th32ProcessID != CurrentProcessId )
  {
    v6 = 0;
    if ( *(int *)(a1 + 956) > 0 )
    {
      while ( !sub_407490(pe.szExeFile, *(_DWORD *)(*(_DWORD *)(a1 + 960) + 4 * v6)) )
      {
        if ( ++v6 >= *(_DWORD *)(a1 + 956) )
          goto LABEL_14;
      }
      v7 = OpenProcess(1u, 0, pe.th32ProcessID);
      v8 = v7;
      if ( v7 )
      {
        TerminateProcess(v7, 0);
        v11 = v8;
        v9 = CloseHandle;
        CloseHandle(v11);
```

Figure 2. Process termination decompiled code

```
                goto LABEL_13;
            }
            v11 = OpenServiceA(hSCObject, v9->lpServiceName, 0x20u);
            if ( !v11 )
            {
              v9->ServiceStatus.dwCurrentState = 0;
              GetLastError();
              sub_406020("[-] call OpenServiceA(%s) failed, error %d\n", (char)v9->lpServiceName);
LABEL_13:
              v8 = v22;
              goto LABEL_14;
            }
            sub_406020("[!] Send SERVICE_CONTROL_STOP to Svc [%s]\n", (char)v9->lpServiceName);
            if ( !ControlService(v11, 1u, &ServiceStatus) )
```

Figure 3. Service termination decompiled code

File and Directory Exclusions

The ransomware excludes system-related files and folders, ransomware-related files, and whitelisted extensions during encryption.

Excluded file extensions:

```
"*.exe", "*.dll", "*.lnk", "*.sys"
```

Excluded directories:

```
"tmp", "winnt", "Application Data", "AppData", "temp", "thumb", "$Recycle.Bin", "System Volume Information", "Windows", "Boot"
```

Inhibit System Recovery

Windows operating systems contain features that can help fix corrupted system files, including shadow copies, which are backups of files created by the Volume Shadow Copy Service (VSS). By deleting shadow copies, the ransomware can prevent victims from restoring files from backups, making it more difficult for them to recover their data without paying the ransom.

The ransomware deletes volume shadow copies before file encryption by starting the following process:

```
cmd.exe /c vssadmin delete shadows /all /quiet
```

System Network Connections Discovery

Fog ransomware can enumerate network-mounted shares by scanning the network interfaces.

Data Encrypted for Impact

The ransomware initially finds available drives and then loads the files one by one using the Windows API FindFirstFileW and FindNextFileW. The ransomware generates random AES keys to encrypt the files, and after encrypting them, the keys are encrypted using a public RSA key. The resulting key is again encrypted and placed at the end of the file.

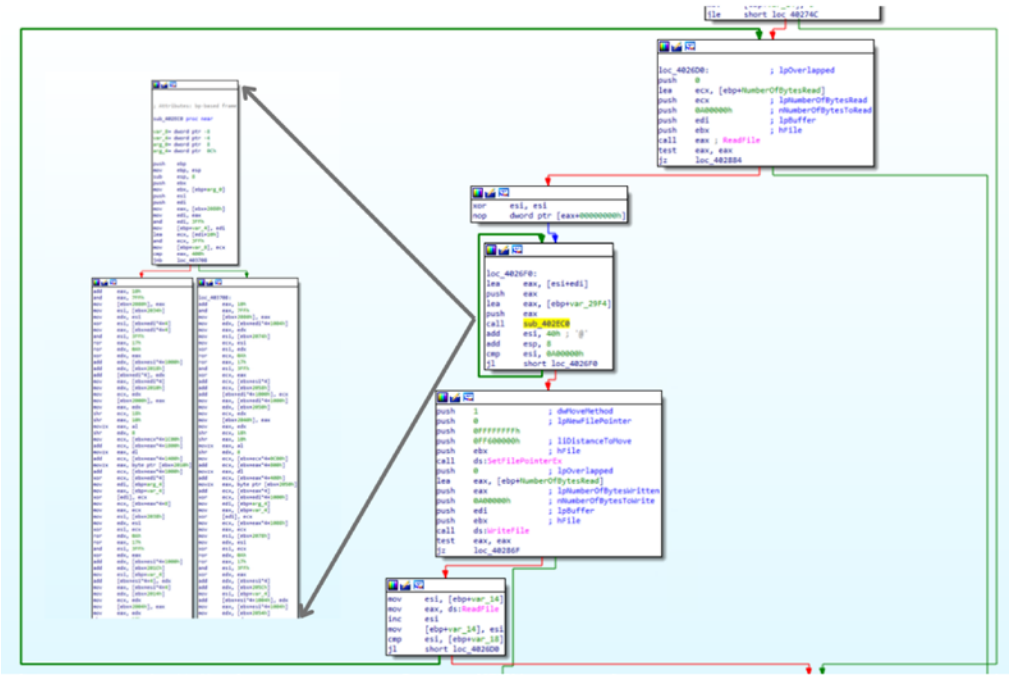


Figure 4. Data encryption code

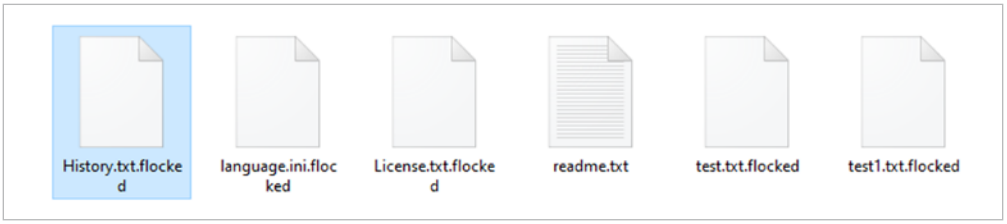


Figure 5. Extension added to the encrypted files

contributors.md.flocked

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000570  DB 83 1B AD A0 A2 D0 01 E3 E2 20 0A 4E 2E 36 B3  Ûƒ.. ¢Ð.ãâ .N.6³
00000580  02 8E E0 BE 5C 1B 55 2B 1F 16 70 96 DD 2F C3 2B  .Žà¾\.U+..p–Ý/Ã+
00000590  26 6E 3A CF EA F1 CF B8 90 7D 52 8D 0F D4 39 65  &n:Ïêñ Ï¸.}R..Ô9e
000005A0  22 7C 7D E0 2C C3 52 D6 4A BC F9 EF 23 46 33 31  "|}à,ÃRÖJ¼ùï#F31
000005B0  B8 78 13 D5 27 A6 F1 3E D5 8F A1 F8 10 52 B7 13  ¸x.Õ'¦ñ>Õ.¡ø.R·.
000005C0  C1 4F EC A6 67 83 FC 04 55 0B 35 19 BC CF 47 08  ÁOì¦gƒü.U.5.¼ÏG.
000005D0  79 46 97 5F 8A 0E EB 08 87 56 3F 8F 18 DD CD 43  yF—_Š.ë.‡V?..ÝÍC
000005E0  0C A5 6A 83 24 62 76 EF 62 22 25 B1 07 6A 76 AF  .¥jƒ$bvïb"%±.jv¯
000005F0  00 E9 A0 EA F9 5A 3F 9B 8C 79 BD 7F 73 64 26 67  .é êùZ?›Œy½.sd&g
00000600  11 D5 6B 6D CE D3 6A 06 DC 69 C2 FF 99 3B 75 AF  .ÕkmÎÓj.ÜiÂÿ™;u¯
00000610  18 9C A5 08 C8 F1 06 7B 59 3C 9B E5 F0 DC 4C 2F  .œ¥.Èñ.{Y<›åðÜL/
00000620  56 C3 E4 C7 FE E1 0E F9 CA CC 4E 72 21 67 4A 89  VÃäÇþá.ùÊÌNr!gJ‰
00000630  52 32 51 47 0A FA 07 8A 81 71 B7 4D 00 BD 73 22  R2QG.ú.Š.q·M.½s"
00000640  B5 A7 0A 23 18 EE 3A 0D E6 38 3C 13 0B ED 07 5E  µ§.#.î:.æ8<..í.^
00000650  8F 98 F7 6F 35 E3 5B 4E AD 48 9E 57 3B DF 75 E8  .˜÷o5ã[N.HžW;ßuè
00000660  14 FC AC F5 13 DB 9D 72 68 F0 6B 01 0D B9 F8 9D  .ü¬õ.Û.rhðk..¹ø.
00000670  01 A3 0E 38 45 12 E5 AB B3 DE C1 CD 84 E5 68 48  .£.8E.å«³ÞÁÍ„åhH
00000680  6B AD 7B E9 D3 32 46 9C 59 72 5A 6C 30 50 A4 6D  k.{éÓ2FœYrZl0P¤m
00000690  B3 EA 42 10 AA 63 D6 7F 1E 3B FB 32 99 86 B8 14  ³êB.ªcÖ..;û2™†¸.
000006A0  B5 8B 3A 47 52 F2 6E 8B E8 6F 4E 6B CB 69 69 E1  µ‹:GRòn‹èoNkËiiá
000006B0  B6 0B 2F C5 61 C9 C8 0B 28 8C 54 1C B6 A1 43 03  ¶./ÅaÉÈ.(ŒT.¶¡C.
```

Figure 6. Encrypted AES key appended to encrypted file.

Fog ransomware extensions observed:

```
".FOG", ".FLOCKED", "FFOG"
```

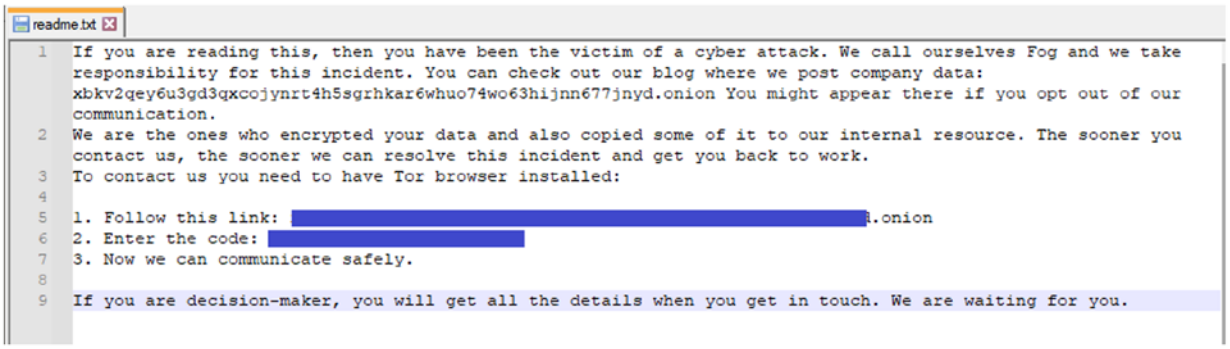
During execution, the ransomware creates a file named DbgLog.sys in the same directory and logs the ransomware activity. If the "-log" argument is used during ransomware execution, the ransomware creates and encrypts a lock_log.txt file under the C:\ProgramData directory. Encrypting the lock_log.txt file created might be an oversight in the ransomware code possibly indicating that the ransomware is still under development.

DbgLog.sys

```
7/18/2024 12:20:28 AM [=] Decrypting json config
7/18/2024 12:20:28 AM [=] Checking mutex...
7/18/2024 12:20:28 AM [=] NoteFileName: readme.txt
7/18/2024 12:20:28 AM [+] JSON config loaded successfully
7/18/2024 12:20:28 AM [=] Init prgn data...
7/18/2024 12:20:29 AM Found disk # 1 (C:\), type: 1
7/18/2024 12:20:29 AM Uknonwn DrvType (5) of root: D:\, skipped
7/18/2024 12:20:29 AM [=] thread 7480 created
7/18/2024 12:20:29 AM [=] thread 8084 created
7/18/2024 12:20:29 AM [-] WnetOpenEnumA failed with error 1222
7/18/2024 12:20:29 AM [-] WnetOpenEnumA failed with error 1222
7/18/2024 12:20:29 AM Find dir: $Recycle.Bin
7/18/2024 12:20:29 AM Find dir: $WinREAgent
7/18/2024 12:20:29 AM Find dir: Scratch
7/18/2024 12:20:29 AM Find dir: Config.Msi
7/18/2024 12:20:29 AM [-] FindFirstFileW(C:\Config.Msi\*) call error, code: 5
7/18/2024 12:20:29 AM Find dir: Documents and Settings
7/18/2024 12:20:29 AM [-] FindFirstFileW(C:\Documents and Settings\*) call error, code: 5
```

Figure 7. Log file created by the ransomware.

Upon successful execution, the ransomware creates ransom notes with the file name readme.txt.


readme.txt

```
1  If you are reading this, then you have been the victim of a cyber attack. We call ourselves Fog and we take
   responsibility for this incident. You can check out our blog where we post company data:
   xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd.onion You might appear there if you opt out of our
   communication.
2  We are the ones who encrypted your data and also copied some of it to our internal resource. The sooner you
   contact us, the sooner we can resolve this incident and get you back to work.
3  To contact us you need to have Tor browser installed:
4
5  1. Follow this link: [redacted].onion
6  2. Enter the code: [redacted]
7  3. Now we can communicate safely.
8
9  If you are decision-maker, you will get all the details when you get in touch. We are waiting for you.
```

Figure 8. Fog ransom note

Ransom note content:

> If you are reading this, then you have been the victim of a cyber attack. We call ourselves Fog and we take responsibility for this incident. You can check out our blog where we post company data: xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd[.]onion You might appear there if you opt out of our communication.
> We are the ones who encrypted your data and also copied some of it to our internal resource. The sooner you contact us, the sooner we can resolve this incident and get you back to work.
> To contact us you need to have Tor browser installed:
>
> 1. Follow this link: <url>.onion
> 2. Enter the code: <code>
> 3. Now we can communicate safely.
>
> If you are decision-maker, you will get all the details when you get in touch. We are waiting for you.

Modify Registry

The ransomware did not perform any registry key modification.

Mutex

The mutex is the fundamental tool for managing shared resources between multiple threads or processes. Typically, ransomware uses a mutex to avoid reinfecting the victim system and causing multiple layers of encryption. The ransomware creates the following mutex value: XDLJgan1TkNkWfrQ78xVrust07YDq45X.

```
pop ebp
jmp vt1.CA6020
push esi
add eax,3042                                  eax:"xDLJgan1TkNkWfrQ78xVrust07YDq45X"
push eax                                      eax:"xDLJgan1TkNkWfrQ78xVrust07YDq45X"
push 0
push 0
call dword ptr ds:[<&CreateMutexA>]
mov esi,eax                                   eax:"xDLJgan1TkNkWfrQ78xVrust07YDq45X"
call dword ptr ds:[<&GetLastError>]
```

Figure 9. Mutex value created while debugging the ransomware

Network Activity

The ransomware did not try to communicate with a remote server other than encrypting data from mounted shares.

Indicators of Compromise

Indicator	Type	Context
B6360765c786cee0eb28bee64709172b4e2e066449968e011390be1afd8f36c5 15edfedab458be0f569fc2bedb6c4139782516d6faf464b4881739e312e9fabb E67260804526323484f564eebeb6c99ed021b960b899ff788aed85bb7a9d75c3 e44c342198e0ad8dd8c0f7bda19d4deb33f0d8355e3e78827505c3b858c82d54	SHA256 hash	Fog ransomware
C:\readme.txt	File path	Fog ransom note
.fog, .flocked, .ffog	Extension	Encrypted files extension
vssadmin delete shadows /all /quiet	Process	Volume Shadow Copy deletion
XDLJgan1TkNkWfrQ78xVrust07YDq45X JBgB4ZHxUhNdJL9mz61WFXxI0GUXPAxw Gxu7w1Hj1ojGy99XUbpyG3JuYVOtwIe2	Mutex	Mutex value object created by the Fog ransomware
xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd[.]onion	URL	TA data leak site (DLS)

Data Leak Site

The ransom note contains a data leak site (DLS) that, when accessed, displayed the following page, self-identifying the group as Fog:

Figure 10. TOR DLS: xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd[.]onion

Detection Mechanisms

Custom Detections and Blocking with Arete's Arsinal

SentinelOne S1QL 1.0 query syntax (STAR rule):

Fog Ransomware

EndpointOS = "Windows" **AND**
((ObjectType = "Process" **AND** SrcProcCmdLine RegExp "\.exe\s{1,3}\-id\s{1,3}[a-zA-Z0-9]{6}") OR (ObjectType = "File" AND EventType In ("File Creation" , "File Scan") AND TgtFilePath Contains Anycase "\DbgLog.sys"))

Volume Shadow Copy Deletion

(EndpointOS = "Windows" **AND** ObjectType = "Process") **AND** (TgtProcCmdLine Contains Anycase " vssadmin " **AND** TgtProcCmdLine Contains Anycase " delete " **AND** TgtProcCmdLine Contains Anycase " shadows" **AND** TgtProcCmdLine Contains Anycase " /all " **AND** TgtProcCmdLine Contains Anycase " /quiet")

Note: These threat hunting queries may need to be tuned for your specific network environment.

Yara

```
rule Fog_ransomware_executable
{
  meta:
    author = "areteir.com"
    description = "Detects the Fog ransomware executable"
    target = "Windows systems"
    file_type = "exe"
    copyright = "Copyright © 2024 by Arete Advisors, LLC."
    distribution = "No re-distribution without Arete Advisors, LLC consent."

  strings:
    $str1 = "Start encrypt file:" nocase
    $str2 = "locked by another process" nocase
    $str3 = "Find file:" nocase
    $str4 = "-nomutex param" nocase
    $str5 = "Decrypting json config" nocase
    $str6 = "CryptStringToBinaryA()" nocase
    $str7 = "JSON config loaded successfully" nocase
    $str8 = "CryptEncrypt()" nocase
    $str9 = "SERVICE_CONTROL_STOP" nocase
    $str10 = "delete shadows" nocase
    $str11 = "error load value:" nocase

  condition:
    ((uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)) and
    (8 of ($str*))
}
```

Recommended Mitigations

- Utilize an endpoint detection and response (EDR) solution with the capability to halt detected processes and isolate systems on the network based on identified conditions.
- Block any known attacker C2s in the firewall.
- Implement multi-factor authentication on RDP and VPN to restrict access to critical network resources.
- Eliminate unnecessary RDP ports exposed to the internet.
- Block a high number of SMB connection attempts from one system to others in the network over a short period of time.
- Perform periodic dark web monitoring to verify if data is available for sale on the black market.
- Perform penetration tests.
- Periodically patch systems and update tools.
- Monitor connections to the network from suspicious locations.
- Monitor downloads and uploads of files to file-sharing services outside standard work hours.
- Monitor file uploads from domain controllers to the internet.
- Monitor network scans from uncommon servers (e.g., RDP server).

Organizations can find the full list of US government recommended ransomware prevention and mitigation guidance here: https://www.cisa.gov/stopransomware/ransomware-guide.

References

Arete Podcast - Unmasking Fog: Ransomware Threats in K-12 Education