Data used at startup
Web server directories
Device les, drivers
RANSOMWARE
System information, including PID les; cleared on each reboot
Virtual lesystem used by Linux to store runtime system information like PIDs, mounted
Interface to the kernel; similar to /proc
LINUX MALWARE

Indicators of Compromise
an IBM Aspera vulnerability.
actors turn to exploiting application vulnerabilities, as the IceFire operator demonstrated by deploying payloads through
This evolution for IceFire forties that ransomware targeting Linux continues to
Conclusion
targeting Windows.
The Linux version's Onion hostname matches the hostname that ransomware trackers tie to

Notable Findings
including:

ICEFIRE

ICEFIRE Linux Payload Delivery & Infrastructure
IceFire payloads are hosted on a DigitalOcean droplet at 159.65.217.216 with the following URL format:
recently patched vulnerability in IBM's Aspera Faspex le sharing software.

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

SHA-1: b676c38d5c309b64ab98c2cd82044891134a9973

The IceFire Linux version (SHA-1: b676c38d5c309b64ab98c2cd82044891134a9973) is a 2.18 MB, 64-bit ELF binary

IceFire skipped the les with ".sh" and ".cfg" extensions.

In observed intrusions, the Linux version was deployed against CentOS hosts running a vulnerable version of IBM

The following le extensions are targeted for encryption:

.AES .bat .bash .bat .bin .c .com .conf .cpp .csh .cshrc .crt .d .db .db .dc.

.......-...-..-.......

A le with the CPP extension that was encrypted by IceFire

In observed intrusions, the IceFire developers employed the following excisions in the kept paths and kee extensions:

user and shared directories (e.g.,

During our analysis, the user prole directory at

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

i F i r e

le extension is associated with known reports of IceFire, a ransomware family noted

BlackBasta
Hive

Function for writing a log le to user Jhone's Desktop

In a cryptographic logging function, the binary contains an embedded path referencing the Desktop for a user named

.cnf extension potentially refers to a conguration le. The relic was near the end of the OpenSSL

Enterprise Networks
IceFire Ransomware Returns | Now Targeting Linux

groups
their focus to include Linux. This strategic shift is a signicant move that aligns them with

@malwrhunterteam
@demonslay335
"hard" it seems...
countries in the past < 40 hours, so they started
Already seen victim companies from multiple

Extension: .iFire

©2023 SentinelOne, All Rights Reserved.