Halcyon Identifies New Ransomware Operator Volcano Demon Serving Up LukaLocker

By Halcyon RISE Team

Published: 2024-07-01 · Archived: 2026-04-05 22:20:30 UTC

Halcyon has encountered a new ransomware organization our researchers are tracking as Volcano Demon following several attacks in the past two weeks.

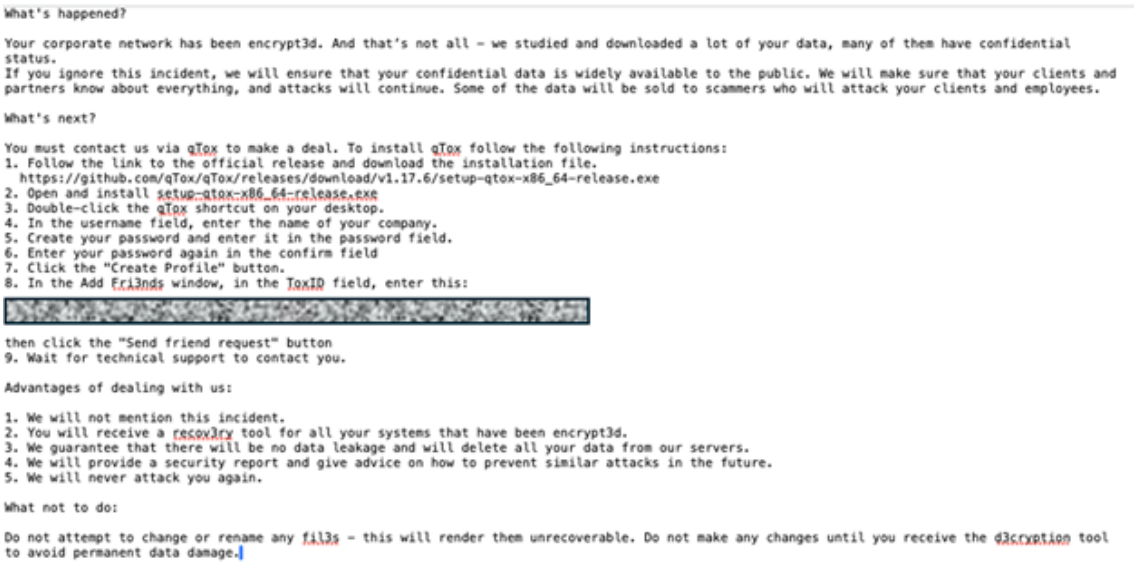
The following encryptor sample dubbed LukaLocker was identified encrypting victim files with the .nba file extension. In addition, multiple attack tools were identified with IOCs noted in the table below. A linux version of LukaLocker was also identified on the victim's network.

Volcano Demon was successful in locking both Windows workstations and servers after utilizing common administrative credentials harvested from the network. Prior to the attack, data was exfiltrated to C2 services for double extortion techniques.

Logs were cleared prior to exploitation and in both cases, a full forensic evaluation was not possible due to their success in covering their tracks and limited victim logging and monitoring solutions installed prior to the event.

During both cases, the threat actor features no leak site and uses phone calls to leadership and IT executives to extort and negotiate payment. Calls are from unidentified caller-ID numbers and can be threatening in tone and expectations.

Ransom Note



```
What's happened?

Your corporate network has been encrypt3d. And that's not all - we studied and downloaded a lot of your data, many of them have confidential
status.
If you ignore this incident, we will ensure that your confidential data is widely available to the public. We will make sure that your clients and
partners know about everything, and attacks will continue. Some of the data will be sold to scammers who will attack your clients and employees.

What's next?

You must contact us via qTox to make a deal. To install qTox follow the following instructions:
1. Follow the link to the official release and download the installation file.
  https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.exe
2. Open and install setup-qtox-x86_64-release.exe
3. Double-click the qTox shortcut on your desktop.
4. In the username field, enter the name of your company.
5. Create your password and enter it in the password field.
6. Enter your password again in the confirm field
7. Click the "Create Profile" button.
8. In the Add Fri3nds window, in the ToxID field, enter this:
[redacted]
then click the "Send friend request" button
9. Wait for technical support to contact you.

Advantages of dealing with us:

1. We will not mention this incident.
2. You will receive a recov3ry tool for all your systems that have been encrypt3d.
3. We guarantee that there will be no data leakage and will delete all your data from our servers.
4. We will provide a security report and give advice on how to prevent similar attacks in the future.
5. We will never attack you again.

What not to do:

Do not attempt to change or rename any fil3s - this will render them unrecoverable. Do not make any changes until you receive the d3cryption tool
to avoid permanent data damage.
```

Volcano Demon Ransomware Note

Indicators of Compromise

The following artifacts were associated with Volcano Demon. At the time of publishing, all were uploaded to VT with multiple being flagged:

Name	Description	SHA256 Hash	On VirusTotal
Protector.exe	Trojan	f83abe3d9717238755f1276c87b3b320d8c30421984a897099ce3741d9143906	Yes; 38/73
Locker.exe	Encryptor	4e58629158a6c46ad420f729330030f5e0b0ef374e9bb24cd203c89ec3262669	Yes; 7/68
Linux locker.bin	Linux Encryptor	ac08ab5bfc5f2cfa0703115a0e2b61decc5158ec0d8a99ebc0824da2b4c3d25	No; 0/64
Reboot.bat	Command line scripts as precursors to encryption event	ed32ebb15d4abe262a34e54408ebb0680b62dc975bf6c02652d28006f45fca14	No; 0/64

Encryptor Overview

The LukaLocker sample analyzed in this report was discovered on 15 June 2024. The ransomware is an x64 PE binary written and compiled using C++. LukaLocker ransomware employs API obfuscation and dynamic API resolution to conceal its malicious functionalities -- evading detection, analysis and reverse engineering:

Command Line Options

Command-Line Arguments	Description
-p <path>	Encrypt target path then exit
-m <mode>	Encrypt modes can be any of the following: default is set to 'all' • all • local • net • backups
-l <log_file>	Output to logfile
-s <int>	Unknown, possibly a debugging flag
-no-mutex	Skip creating process mutex
--sd-killer-off	Skip terminating processes and services
--exit-safe-boot	Remove safe-mode option then restart computer
-v / --verbose	Detailed verbose logging.

Note that some of these command-line options are not functional since there is no code implemented by the ransomware author to support these. These are:

- -l <log_file>: although it creates a specified log file, nothing is written to it and remains at 0 bytes.
- Modes “net” and “backups”: unsupported modes and does nothing. Inferring from the names, these options are used to target network shares and backup files for encryption.
- -s <int>: unknown command-line option, no code implemented. Possibly a debugging switch.

Evasion Tactics

Service Stop

Upon execution, unless “--sd-killer-off” is specified, LukaLocker immediately terminates some services similar to and possibly copied from Conti ransomware. The services include the following:

Antivirus and Endpoint Protection

- Sophos
- Symantec
- McAfee
- Avast
- Defender
- Malwarebytes
- Windows Defender
- BitDefender
- Spyhunter
- Kaspersky
- SentinelOne

Backup and Recovery

- Acronis
- Symantec
- Veeam
- SQL Safe

Databases

- Microsoft SQL Server
- MySQL

- IBM DB2
- Oracle

E-Mail Servers

- Microsoft Exchange

Virtualization and Cloud

- VMWare
- BlueStripe
- ProLiant

Remote Access and Monitoring

- Alerter
- Eventlog
- UI0Detect
- WinVNC4

Process Stop

Upon execution, unless “--sd-killer-off” is specified, LukaLocker immediately terminates some processes. The processes include the following:

Antivirus and Security Software

- Symantec/Norton
- McAfee
- AVG
- Kaspersky
- Bitdefender
- Trend Micro
- Malware Bytes

System Monitoring and Management

- VMware
- Proficy
- Microsoft
- IBM

- BMC

Database and Storage Services

- Microsoft SQL Server
- Oracle
- MySQL

Cloud and Remote Access Tools

- TeamViewer
- VNC
- Google

Web Browsers

- Firefox
- Chrome

Office and Productivity Software

- Microsoft Office

File Selection

The following directories are avoided during encryption:

Directories
tmp
temp
winnt
thumb
$Recycle.Bin
$RECYCLE.BIN
System Volume Information
Boot
Windows
Trend Micro
perflogs

The following extensions are avoided, all others are included:

readme.txt
NBA_LOG.txt
.NBA
.exe
.dll
.lnk
.sys
.msi
.bat

File Encryption

The Chacha8 cipher is used for bulk data encryption. The Chacha8 key and nonce are randomly-generated, with the key generated through the Elliptic-curve Diffie–Hellman (ECDH) key agreement algorithm over Curve25519. The ECDH file public key and the nonce are stored in the footer.

The file itself allows for full encryption or partial supporting 100%, 50%, 20%, or 10% of the file data being encrypted. The following is the footer that is used by the ransomware:

Offset	**Length (bytes)**	**Description**
0x00	32	File public key
0x20	8	Chacha Nonce
0x28	1	Encryption Mode byte code 0x24 – Whole file 0x25 – Intermittent
0x29	1	Encrypt Percentage • 0x64 – 100% • 0x32 – 50% • 0x14 – 20% • 0xA – 10%
0x2A	14	Padding
0x38	8	Last encrypted byte in file offset
0x40	8	Original File Size

Offset	Length (bytes)	Description
0x48	16	Magic bytes

Halcyon.ai is the leading anti-ransomware company. Global 2000 companies rely on the Halcyon platform to defeat ransomware with minimal business disruption through built-in bypass and evasion protection, key material capture, automated decryption, and data exfiltration and extortion prevention – talk to a Halcyon expert today to find out more. Halcyon also publishes a quarterly RaaS (Ransomware as a Service) and extortion group reference guide, Power Rankings: Ransomware Malicious Quartile, and check out the Recent Ransomware Attacks resource site.
