Hive Pro

Threat Level

Amber

THREAT ADVISORY

ACTOR REPORT

North Korean hacker group targets victims globally with H0lyGh0st Ransomware

Date of Publication

July 19, 2022

Admiralty code

A1

TA Number

TA2022151

Summary

The H0lyGh0st ransomware group, also tracked as DEV-0530 have been using ransomware payloads to compromise several small to mid-sized organizations across the world.

CVE Table

CVE	NAME	PATCH
CVE-2022-26352	DotCMS remote code execution vulnerability	✓

Actor Map

Potential MITRE ATT&CK TTPs

T1059.003 Windows Command Shell	**T1133** External Remote Services	**T1049** System Network Connections Discovery	**T1082** System Information Discovery
T1083 File and Directory Discovery	**T1486** Data Encrypted for Impact	**T1057** Process Discovery	**T1033** System Owner/User Discovery
T1135 Network Share Discovery	**T1106** Native Application Programming Interface (API		

Technical Details

#1

A financially motivated North Korean state-sponsored actor known as H0lyGh0st successfully compromised multiple small-to-mid-sized industries including schools, banks, manufacturing, and event and meeting planning organizations. The group also has connections with PLUTONIUM (aka DarkSeoul or Andariel) North Korea threat actor group.

#2

DEV-0530 used two custom-developed malware families SiennaPurple and SiennaBlue since they began using ransomware in June 2021 until May 2022. The group also identified four variants under these families – BTLC_C.exe (Jun-Oct 2021), HolyRS.exe (Oct-Dec 2021), HolyLock.exe (Mar-Jun 2022), and BLTC.exe Apr 2022-Present).

#3

The latest variant of H0lyGh0st, BTLC.exe maintains the persistence using lockertask used for either creating or deleting a scheduled task and can be configured to connect to a network share using the default username, password, and intranet URL hardcoded in the malware if the ServerBaseURL is not accessible from the device. Once the ransomware is successfully launched as an administrator, it tries to connect to the default ServerBaseURL hardcoded in the malware, attempts to upload a public key to the C2 server, and encrypts all files on the target device using the file extension '.h0lyenc'.

#4

The ransomware group also maintains an .onion site to interact with its victims. If any victim interacts with the site, the ransomware encrypts files on the victim's targeted device and sends them a sample of the files as proof that it has been stolen. Once received, it demands payment in Bitcoin to restore their access to the files, else, threatens to publish the victim's data publicly or send it to their customers.

#5

The threat actor group might have exploited vulnerabilities such as CVE-2022-26352 (DotCMS remote code execution vulnerability) on public-facing web applications and content management systems, which helps them gain initial access to the target victim's networks. The malware variants were then dropped and executed as mentioned above.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	99fc54786a72f32fd44c7391c2171ca31e72ca52725c68e2dde94d04c286fccdf8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e675d9f40af
File Path	C:\FOR_DECRYPT.html
Command line	cmd.exe /Q /c schtasks /create /tn **lockertask** /tr [File] /sc minute /mo 1 /F /ru system 1> \\127.0.0.1\ADMIN$__[randomnumber] 2>&1
C2	193[.]56[.]29[.]123
Email	H0lyGh0st@mail2tor[.]com

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONS	TARGET INDUSTRIES
H0lyGh0st	North Korea	Financial Gain	Worldwide	Banks, schools, manufacturing organisations, event and meeting planning companies

References

https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 19, 2022 • 6:37 AM

More at www.hivepro.com