H0lyGh0st - North Korean Threat Group Strikes Back With New Ransomware

picussecurity.com/resource/h0lygh0st-north-korean-threat-group-strikes-back-with-new-ransomware

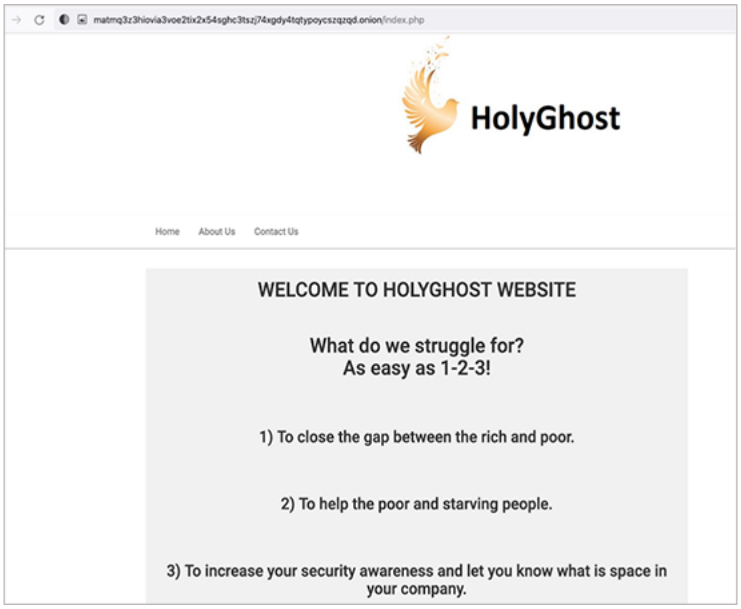
Huseyin Can YUCEEL

H0lyGh0st is a North Korea-based threat actor group, and they have been actively using and developing malware in the wild since June 2021. Like other ransomware groups, H0lyGh0st is a cyber extortion group with financial motives and objectives. In September 2021, they launched successful attacks on many small-to-midsize industries like banks, manufacturers, schools, and event and meeting planning organizations worldwide [1]. Even though H0lyGh0st is not a new threat actor, the group started using a new, improved, and more persistent variant in April 2022. This blog explained what the H0lyGh0st group has improved regarding its TTPs (Tactics, Techniques, and Procedures).

Picus Labs added attack simulations for H0lyGh0st ransomware attacks to the Picus Threat Library, and you can test your security controls against H0lyGh0st attacks.

The H0lyGh0st Extortion Group

The H0lyGh0st is a North Korea-based cyber extortion threat group known for developing malware payloads and performing ransomware attacks since June 2021. The ransomware group is also known as HolyGhost and DEV-0530. In September 2021, they launched many successful attacks. Victim statistics show that they mainly target small-to-midsize industries like financial services, manufacturing, education, and entertainment organizations with weak security infrastructures [1].


matmq3z3hiovia3voe2tix2x54sghc3tszj74xgdy4tqtypoycszqzqd.onion/index.php
HolyGhost
Home
About Us
Contact Us

WELCOME TO HOLYGHOST WEBSITE

What do we struggle for?
As easy as 1-2-3!

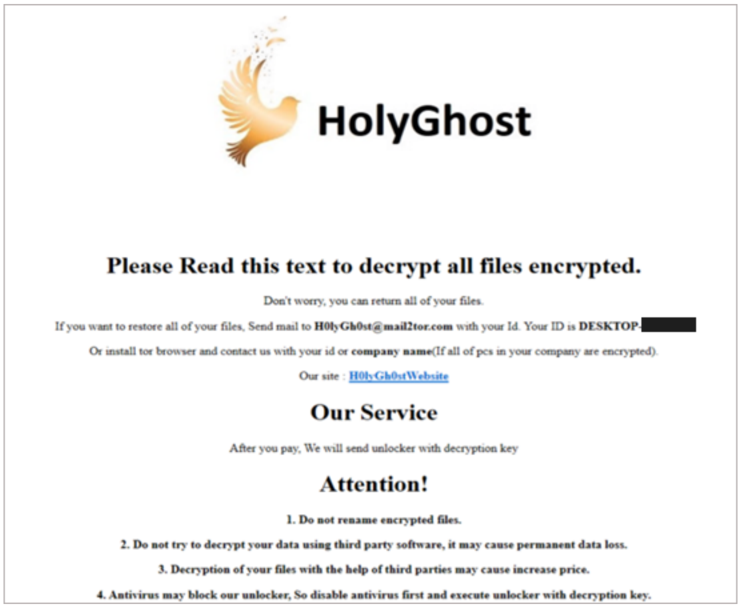
1) To close the gap between the rich and poor.

2) To help the poor and starving people.

3) To increase your security awareness and let you know what is space in your company.

Figure 1: H0lyGh0st group's welcoming message on their web page [1]

The group hosts a .onion web page to maintain communication with their victims. On their homepage, they rationalize their cyberattacks and malicious actions by claiming to be "Robin Hood" however, the H0lyGh0st ransomware group does not target large organizations with robust security infrastructure. In fact, H0lyGh0st can be called an opportunistic threat group that preys on small businesses with a weak security posture.



HolyGhost

Please Read this text to decrypt all files encrypted.

Don't worry, you can return all of your files.

If you want to restore all of your files, Send mail to **H0lyGh0st@mail2tor.com** with your Id. Your ID is **DESKTOP-**[redacted]

Or install tor browser and contact us with your id or **company name**(If all of pcs in your company are encrypted).

Our site : [H0lyGh0stWebsite]

Our Service

After you pay, We will send unlocker with decryption key

Attention!

1. Do not rename encrypted files.

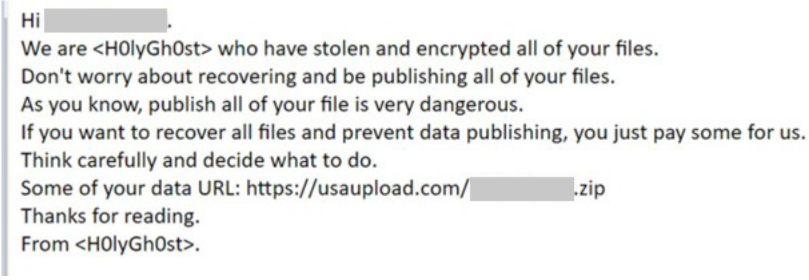
2. Do not try to decrypt your data using third party software, it may cause permanent data loss.

3. Decryption of your files with the help of third parties may cause increase price.

4. Antivirus may block our unlocker, So disable antivirus first and execute unlocker with decryption key.

Figure 2: Instructions given by H0lyGh0st on their web page. [1]

After gaining initial access to their victim's network, the threat actors move laterally across the network and exfiltrate sensitive data. After exfiltration, H0lyGh0st encrypts the victim's data and leaves the instructions for a ransom payment in Figure 2. The ransomware group uses the double extortion method and threatens to release stolen sensitive information on social media or anonymous document-sharing platforms like Pastebin unless ransom is paid.



Hi [redacted].
We are <H0lyGh0st> who have stolen and encrypted all of your files.
Don't worry about recovering and be publishing all of your files.
As you know, publish all of your file is very dangerous.
If you want to recover all files and prevent data publishing, you just pay some for us.
Think carefully and decide what to do.
Some of your data URL: https://usaupload.com/[redacted].zip
Thanks for reading.
From <H0lyGh0st>.

Figure 3: An email sent by H0lyGh0st [1]

The threat actor sends a piece of stolen data back to their victim as proof and demands ransom for the decryption key. Demanded ransoms vary from 1.2 to 5 BTC. However, some victims were able to negotiate and make a discount of up to ⅓ of the initial ransom [2].

Affiliated APT Group - PLUTONIUM

According to Microsoft Threat Intelligence Center (MSTIC), H0lyGh0st is not following a hundred percent unique and independent approach from other ransomware groups. There are some overlapping points between H0lyGh0st and another North Korean-based APT group, PLUTONIUM.

PLUTONIUM is known as DarkSeoul or Andariel in the wild and is a sub-group under the Lazarus umbrella. PLUTONIUM is infamous for attacking energy and defense industries in many countries like South Korea, the USA, and India. The observed mail communications between PLUTONIUM and H0lyGh0st and the use of similar custom malware controllers indicate an affiliation between the two groups.

The first malware developed by the H0lyGh0st ransomware group was named BTLC_C.exe, and it was first observed back in Jun 2021. BTLC_C.exe is classified under the SiennaPurple malware family and was written in C++.

Shortly after, the threat group switched to the Go language and built new ransomware variants. These new variants, HolyRs.exe, HolyLock.exe, and BLTC.exe, are classified under the SiennaBlue malware family.

Since all these variants use the similar C2 URL and code patterns, ransom notes and instructions, MSTIC attributed these ransomware to H0lyGh0st aka DEV-0530.

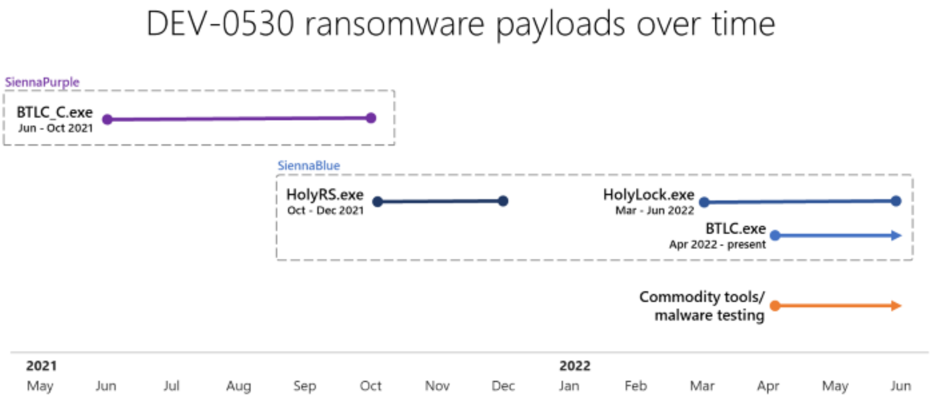


Figure 4: Timeline of the Payloads Developed and Used by H0lyGh0st [1]

BTLC_C.exe Under the SiennaPurple Family

BTLC_C.exe is the first malware developed by the H0lyGh0st ransomware group. BTLC_C.exe is not a sophisticated malware payload and has few distinguishable features compared to its successors HolyRs.exe, HolyLock.exe, and BLTC.exe.

BLTC_C.exe requires administrator-level privileges for execution, otherwise, a hard-coded error message pops up saying that *the program requires an admin user*.

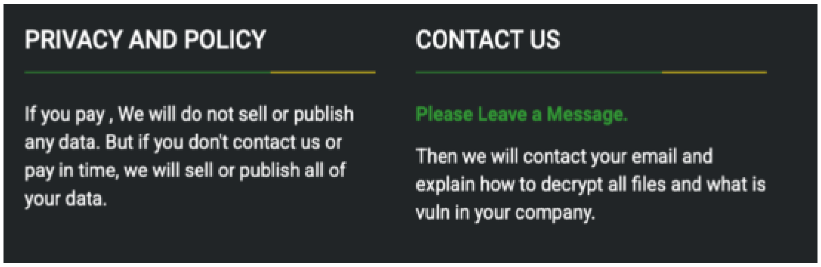
This malware uses a pretty basic string obfuscation technique: It substructs "0x30" from the hex value of each character in a string. For instance, the hard-coded C2 IP address, 193[.]56[.]29[.]123*,* of the main_ServerBaseURL: *hxxp://193[.]56[.]29[.]123:8888* is encoded as *"*aic^ef^bi^abc0" [1]. Apart from that, it is seen that IoCs found in decoded malware are highly correlated to other variants in the SiennaBlue family in terms of C2 infrastructure and TTP beacon URL structure *access.php?order=AccessRequest&cmn* [1].

HolyRS.exe, HolyLock.exe, and BLTC.exe Under the SienneBlue Family

As it was mentioned previously, malware payloads under the SiennaBlue family are written in Go language; thus, they share core Go functions including *multiple encryption options*, *public-key management*, *internet and intranet support*, *string obfuscation*.

To gain initial access, new variants of H0lyGh0st ransomware search for vulnerabilities in the public-facing web applications and content management systems of their target. DotCMS RCE (CVE-2022-26352) vulnerability is one of the vulnerabilities exploited by the ransomware group.

After successfully encrypting the victim's files, the ransomware encodes the file names in Base64 and appends the file with the .h0lyenc extension. Then, the ransomware leaves a file called "FOR_DECRYPT.html" that contains contact information.



PRIVACY AND POLICY

If you pay , We will do not sell or publish any data. But if you don't contact us or pay in time, we will sell or publish all of your data.

CONTACT US

Please Leave a Message.

Then we will contact your email and explain how to decrypt all files and what is vuln in your company.

Figure 5: "Contact Us" Section on the H0lyGh0st Web Page [1]

The latest variant, BLTC.exe, has a hardcoded intranet URL and ServerBaseUrl in the malware. BLTC.exe can be configured to connect to a network share using the default credentials and the intranet URL if the victim device cannot reach the ServerBaseUrl. Unlike its predecessors, BLTC.exe establishes persistence by creating and deleting a scheduled task called lockertask.

After being executed with administrator privileges, the ransomware payload tries to connect to the ServerBaseUrl. If the connection is successful, it downloads a public key to the C2 server in order to encrypt the victim's all files.

How Picus Helps Simulate H0lyGh0st Attacks?

Using the Picus Continuous Security Validation Platform, you can test your security controls against the H0lyGh0st attacks. We advise you to simulate H0lyGh0st ransomware attacks and determine whether your security controls can prevent them or not. Picus Threat Library includes the following threats to simulate attacks and malicious tools used by the H0lyGh0st group.

Threat ID	Action Name	Attack Module
20076	H0lyGh0st Ransomware Malware Download Threat	Network Infiltration
41450	H0lyGh0st Ransomware Malware Email Threat	Email Infiltration (Phishing)
97451	DEV-0530 Threat Group Campaign Malware Download Threat	Network Infiltration
75946	DEV-0530 Threat Group Campaign Malware Email Threat	Email Infiltration (Phishing)

MITRE ATT&CK Techniques Used by H0lyGh0st Group

Initial Access

T1133 External Remote Services

T1190 Exploit Public-Facing Application

Execution

T1059.003 Windows Command Shell

Persistence

T1133 External Remote Services

Privilege Escalation

T1134.001 Token Impersonation/Theft

Defense Evasion

T1027.002 Software Packing

T1134.001 Token Impersonation/Theft

Credential Access

T1056.004 Credential API Hooking

Discovery

T1012 Query Registry

T1033 System Owner/User Discovery

T1049 System Network Connections Discovery

T1057 Process Discovery

T1082 System Information Discovery

T1083 File and Directory Discovery

T1135 Network Share Discovery

Collection

T1056.004 Credential API Hooking

T1114 Email Collection

Command and Control

T1571 Non-Standard Port

T1573 Encrypted Channel

Impact

T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

SHA-256	MD5	SHA-1
99fc54786a72f32fd44c7391c2171ca31e72ca52725c68e2dde94d04c286fccd	54ca404d16db18d233c606b48c73d66f	d7d472bfc62bd6f52e3
f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86	a2b371eea0aee7cf57e23b5f0f4668c7	d1ddbe96ef37c38b4d9
bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e675d9f40af	eec15f3648f8bc8684e67ac7cf9813ea	4dade34d55256981a4

Reference

[1] Microsoft Threat Intelligence Center (MSTIC) and Microsoft Digital Security Unit (DSU), "North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware," *Microsoft Security Blog*, Jul. 14, 2022. [Online]. Available: https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/. [Accessed: Jul. 27, 2022]

[2] H. Pro, "North Korean hacker group targets victims globally with Holy Ghost ransomware," *Hive Pro*, Jul. 20, 2022. [Online]. Available: https://www.hivepro.com/north-korean-hacker-group-targets-victims-globally-with-holy-ghost-ransomware/. [Accessed: Jul. 27, 2022]