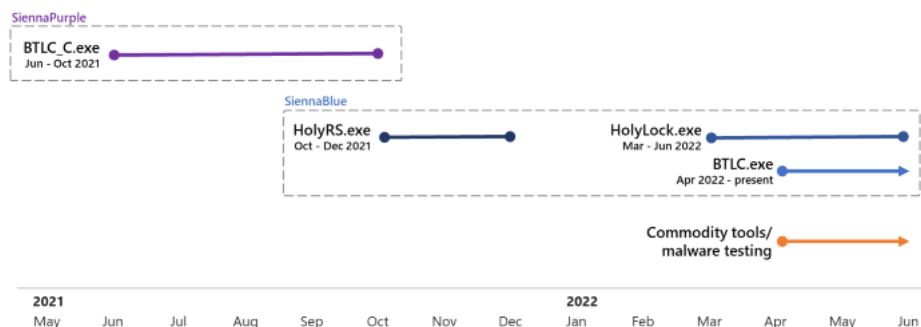


North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware

: 7/14/2022

DEV-0530 ransomware payloads over time



A group of actors originating from North Korea that Microsoft Threat Intelligence Center (MSTIC) tracks as DEV-0530 has been developing and using ransomware in attacks since June 2021. This group, which calls itself H0lyGh0st, utilizes a ransomware payload with the same name for its campaigns and has successfully compromised small businesses in multiple countries as early as September 2021.

Along with their H0lyGh0st payload, DEV-0530 maintains an *.onion* site that the group uses to interact with their victims. The group's standard methodology is to encrypt all files on the target device and use the file extension *.h0lyenc*, send the victim a sample of the files as proof, and then demand payment in Bitcoin in exchange for restoring access to the files. As part of their extortion tactics, they also threaten to publish victim data on social media or send the data to the victims' customers if they refuse to pay. This blog is intended to capture part of MSTIC's analysis of DEV-0530 tactics, present the protections Microsoft has implemented in our security products, and share insights on DEV-0530 and H0lyGh0st ransomware with the broader security community to protect mutual customers.

MSTIC assesses that DEV-0530 has connections with another North Korean-based group tracked as PLUTONIUM (aka DarkSeoul or Andariel). While the use of H0lyGh0st ransomware in campaigns is unique to DEV-0530, MSTIC has observed communications between the two groups, as well as DEV-0530 using tools created exclusively by PLUTONIUM.

As with any observed nation-state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the information they need to secure their accounts. Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing MSTIC to track it as a unique set of information until we reach high confidence about the origin or identity of the actor behind the activity.

Who is DEV-0530?

DEV-0530 primarily operates ransomware campaigns to pursue financial objectives. In MSTIC's investigations of their early campaigns, analysts observed that the group's ransom note included a link to the *.onion* site *https://matmq3z3hiovvia3voe2tix2x54sghc3tszj74xgdy4tqtypoicszqzqd[.]onion*, where the attackers claim to "close the gap between the rich and poor". They also attempt to legitimize their actions by claiming to increase the victim's security awareness by letting the victims know more about their security posture.



Figure 1. A H0lyGh0st ransom note linked to the attackers' .onion site.

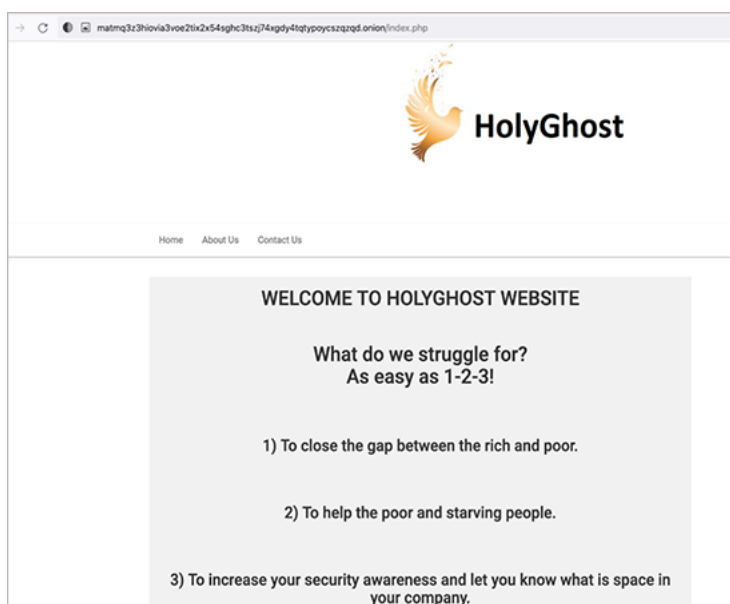


Figure 2. DEV-0530 attackers publishing their claims on their website.

Like many other ransomware actors, DEV-0530 notes on their website's privacy policy that they would not sell or publish their victim's data if they get paid. But if the victim fails to pay, they would publish everything. A contact form is also available for victims to get in touch with the attackers.

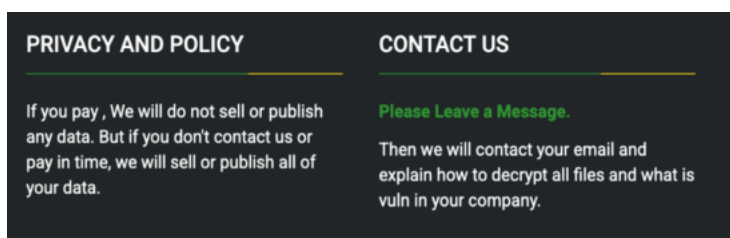


Figure 3. Privacy policy and contact us information on the H0lyGh0st website.

Affiliations with other threat actors originating from North Korea

MSTIC assesses there is likely some overlap between DEV-0530 and PLUTONIUM. PLUTONIUM is a North Korean threat actor group affiliated with clusters of activity that are also known as DarkSeoul and Andariel. Active since at least 2014, PLUTONIUM has primarily targeted the energy and defense industries in India, South Korea, and the United States using a variety of tactics and techniques.

MSTIC has observed known DEV-0530 email accounts communicating with known PLUTONIUM attacker accounts. MSTIC has also observed both groups operating from the same infrastructure set, and even using custom malware controllers with similar names.

To further assess the origin of DEV-0530 operations, MSTIC performed a temporal analysis of observed activity from the group. MSTIC estimates that the pattern of life of DEV-0530 activity is most consistent with the UTC+8 and UTC+9 time zones. UTC+9 is the time zone used in North Korea.

Despite these similarities, differences in operational tempo, targeting, and tradecraft suggest DEV-0530 and PLUTONIUM are distinct groups.

Why are North Korean actors using ransomware?

Based on geopolitical observations by global experts on North Korean affairs and circumstantial observations, Microsoft analysts assess the use of ransomware by North Korea-based actors is likely motivated by two possible objectives.

The first possibility is that the North Korean government sponsors this activity. The weakened North Korean economy has become weaker since 2016 [due to sanctions](#), [natural disasters](#), [drought](#), and the North Korean government's COVID-19 [lockdown from the outside world](#) since early 2020. To offset the losses from these economic setbacks, the North Korean government could have sponsored cyber actors stealing from [banks and cryptocurrency wallets](#) for more than five years. If the North Korean government is ordering these ransomware attacks, then the attacks would be yet another tactic the government has enabled to offset financial losses.

However, state-sponsored activity against cryptocurrency organizations has typically targeted a much broader set of victims than observed in DEV-0530 victimology. Because of this, it is equally possible that the North Korean government is not enabling or supporting these ransomware attacks. Individuals with ties to PLUTONIUM infrastructure and tools could be moonlighting for personal gain. This moonlighting theory might explain the often-random selection of victims targeted by DEV-0530.

Although Microsoft cannot be certain of DEV-0530's motivations, the impact of these ransomware attacks on our customers raises the importance of exposing the underlying tactics and techniques, detecting and preventing attacks in our security products, and sharing our knowledge with the security ecosystem.

Ransomware developed by DEV-0530

Between June 2021 and May 2022, MSTIC classified H0lyGh0st ransomware under two new malware families: *SiennaPurple* and *SiennaBlue*. Both were developed and used by DEV-0530 in campaigns. MSTIC identified four variants under these families – BTLC_C.exe, HolyRS.exe, HolyLock.exe, and BLTC.exe – and clustered them based on code similarity, C2 infrastructure including C2 URL patterns, and ransom note text. BTLC_C.exe is written in C++ and is classified as *SiennaPurple*, while the rest are written in Go, and all variants are compiled into .exe to target Windows systems. Microsoft Defender Antivirus, which is built into and ships with Windows 10 and 11, detects and blocks BTLC_C.exe as *SiennaPurple* and the rest as *SiennaBlue*, providing protection for Windows users against all known variants the H0lyGh0st malware..

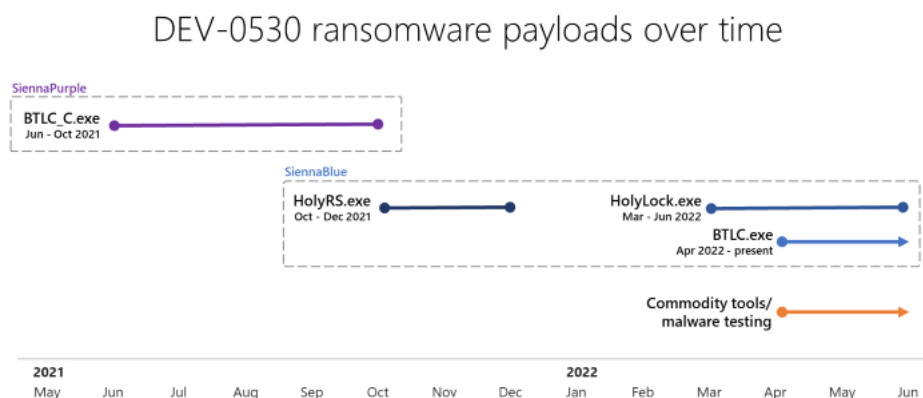


Figure 4. Timeline of DEV-0530 ransomware payloads.

SiennaPurple ransomware family: BTLC_C.exe

BTLC_C.exe is a portable ransomware developed by DEV-0530 and was first seen in June 2021. This ransomware doesn't have many features compared to all malware variants in the SiennaBlue family. Prominently, if not launched as an administrative user, the BTLC_C.exe malware displays the following hardcoded error before exiting:

```
"This program only execute under admin privilege".
```

The malware uses a simple obfuscation method for strings where 0x30 is subtracted from the hex value of each character, such that the string "aic^ef^bi^abc0" is decoded to 193[.]56[.]29[.]123. The indicators of compromise (IOCs) decoded from the BTLC_C.exe ransomware are consistent with all malware variants in the SiennaBlue family, including the C2 infrastructure and the HTTP beacon URL structure `access.php?order=AccessRequest&cmn`. The

BTLC_C.exe sample analyzed by MSTIC has the following PDB path: *M:\ForOP\attack(utils)\attack tools\Backdoor\powershell\btlc_C\Release\btlc_C.pdb*.

SiennaBlue ransomware family: HolyRS.exe, HolyLocker.exe, and BTLC.exe

Between October 2021 and May 2022, MSTIC observed a cluster of new DEV-0530 ransomware variants written in Go. We classified these variants as SiennaBlue. While new Go functions were added to the different variants over time, all the ransomware in the SiennaBlue family share the same core Go functions.

A deeper look into the Go functions used in the SiennaBlue ransomware showed that over time, the core functionality expanded to include features like various encryption options, string obfuscation, public key management, and support for the internet and intranet. The table below demonstrates this expansion by comparing the Go functions in HolyRS.exe and BTLC.exe:

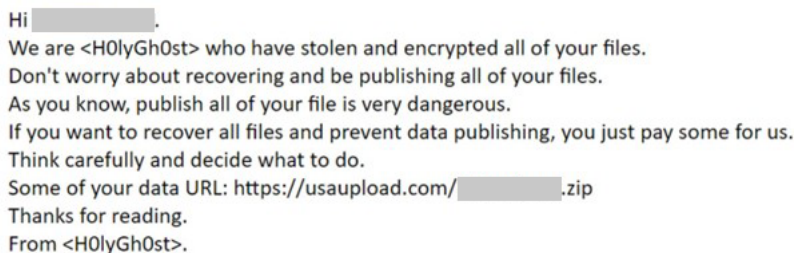
HolyRS.exe [2021]	BTLC.exe [2022]
<i>main_main</i>	<i>main_main</i>
<i>main_init_0</i>	<i>main_init_0</i>
<i>main_IsAdmin</i>	<i>main_IsAdmin</i>
<i>main_encryptFiles</i>	<i>main_encryptFiles</i>
<i>HolyLocker_RsaAlgorithm_GenerateKeyPair</i>	<i>main_DeleteSchTask</i>
<i>HolyLocker_RsaAlgorithm_Encrypt</i>	<i>main_DisableNetworkDevice</i>
<i>HolyLocker_CryptoAlogrithm__ptr_File__EncryptRSA</i>	<i>main_encryptString</i>
<i>HolyLocker_CryptoAlogrithm__ptr_File__EncryptAES</i>	<i>main_decryptString</i>
<i>HolyLocker_utilities_GenerateRandomANString</i>	<i>main_cryptAVPass</i>
<i>HolyLocker_utilities_StringInSlice</i>	<i>main_SelfDelete</i>
<i>HolyLocker_utilities_SliceContainsSubstring</i>	<i>HolyLocker_RsaAlgorithm_GenerateKeyPair</i>
<i>HolyLocker_utilities_RenameFile</i>	<i>HolyLocker_RsaAlgorithm_Encrypt</i>
<i>HolyLocker_Main_init</i>	<i>HolyLocker_CryptoAlogrithm__ptr_File__EncryptRSA</i>
<i>HolyLocker_communication_New</i>	<i>HolyLocker_CryptoAlogrithm__ptr_File__EncryptAES</i>
<i>HolyLocker_communication__ptr_Client__GetPubkeyFromServer</i>	<i>HolyLocker_utilities_GenerateRandomANString</i>
<i>HolyLocker_communication__ptr_Client__Do</i>	<i>HolyLocker_utilities_StringInSlice</i>
<i>HolyLocker_communication__ptr_Client__SendEncryptedPayload</i>	<i>HolyLocker_utilities_SliceContainsSubstring</i>
<i>HolyLocker_communication__ptr_Client__SendFinishRequest</i>	<i>HolyLocker_utilities_RenameFile</i>
<i>HolyLocker_communication__ptr_Client__AddNewKeyPairToIntranet</i>	<i>HolyLocker_Main_init</i>
<i>HolyLocker_communication__ptr_Client__AddNewKeyPair</i>	<i>HolyLocker_communication_New</i>
	<i>HolyLocker_communication__ptr_Client__GetPubkey</i>
	<i>HolyLocker_communication__ptr_Client__Do</i>
	<i>HolyLocker_communication__ptr_Client__SendEncry</i>
	<i>HolyLocker_communication__ptr_Client__SendFinis</i>
	<i>HolyLocker_communication__ptr_Client__AddNewKe</i>
	<i>HolyLocker_communication__ptr_Client__AddNewKe</i>

MSTIC assesses DEV-0530 successfully compromised several targets in multiple countries using HolyRS.exe in November 2021. A review of the victims showed they were primarily small-to-midsized businesses, including manufacturing organizations, banks, schools, and event and meeting planning companies. The victimology indicates that these victims are most likely targets of opportunity. MSTIC suspects that DEV-0530 might have exploited vulnerabilities such as [CVE-2022-26352](#) (DotCMS remote code execution vulnerability) on public-facing web applications and content management systems to gain initial access into target networks. The SiennaBlue malware variants were then dropped and executed. To date, MSTIC has not observed DEV-0530 using any 0-day exploits in their attacks.

After successfully compromising a network, DEV-0530 exfiltrated a full copy of the victims' files. Next, the attackers encrypted the contents of the victim device, replacing all file names with Base64-encoded versions of the file names and renaming the extension to *.h0lyenc*. Victims found a ransom note in *C:\FOR_DECRYPT.html*, as well as an email from the attackers with subject lines such as:

```
!!!!We are <H0lyGh0st>. Please Read me!!!!
```

As seen in the screenshot below, the email from the attackers let the victim know that the group has stolen and encrypted all their files. The email also included a link to a sample of the stolen data to prove their claim, in addition to the demand for payment for recovering the files.



```
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 5. Ransom note left by DEV-0530 attackers.

BTLC.exe is the latest DEV-0530 ransomware variant and has been seen in the wild since April 2022. BTLC.exe 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. One notable feature added to BTLC.exe is a

persistence mechanism in which the malware creates or deletes a scheduled task called *lockertask*, such that the following command line syntax can be used to launch the ransomware:

```
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
```

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 in the victim's drive.

HolyRS.exe/HolyLocker.exe C2 configuration

```
main_ServerBaseURL:
hxxp://193[.]56[.]29[.]123:8888
main_IntranetURL: 10[.]10[.]3[.]42
main_Username: adm-karsair
```

BTLC.exe C2 configuration

```
EncryptionKey: HOlyGh0stKey1234
IntranetUrl: 192[.]168[.]168[.]5
Username: atrismsp Scheduledtask name:
lockertask
```

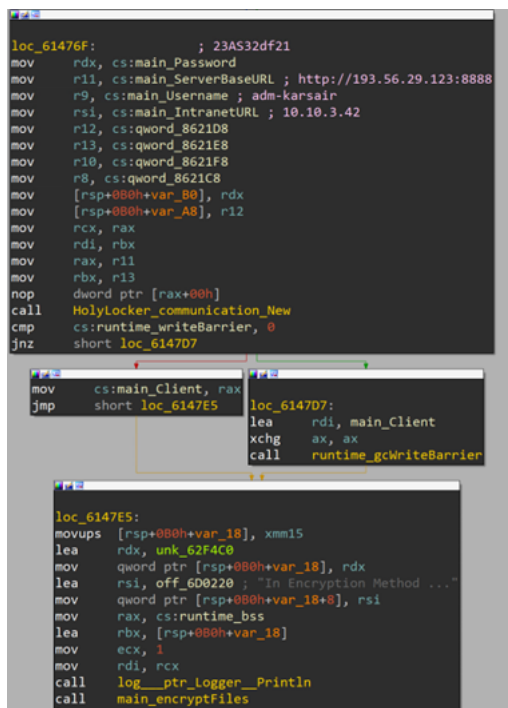


Figure 6. BTLC.exe C2 communication

Based on our investigation, the attackers frequently asked victims for anywhere from 1.2 to 5 Bitcoins. However, the attackers were usually willing to negotiate and, in some cases, lowered the price to less than one-third of the initial asking price. As of early July 2022, a review of the attackers' wallet transactions shows that they have not successfully extorted ransom payments from their victims.

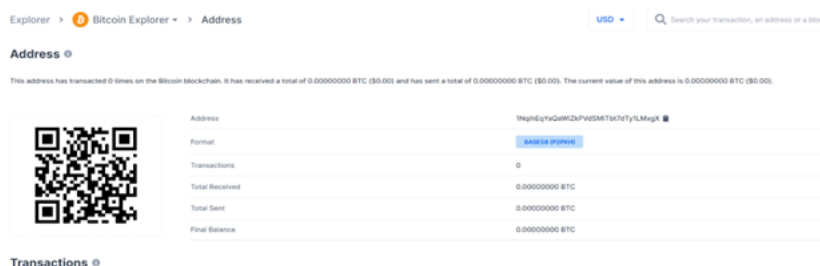


Figure 7. Screenshot of DEV-0530 attackers' wallet

HolyRS.exe/BTLC.exe C2 URL pattern:

- *hxxp://193[.]56[.]29[.]123:8888/access.php?order=GetPubkey&cmn=[Victim_HostName]*
- *hxxp://193[.]56[.]29[.]123:8888/access.php?order=golc_key_add&cmn=[Victim_HostName]&type=1*
- *hxxp://193[.]56[.]29[.]123:8888/access.php?order=golc_key_add&cmn=[Victim_HostName]&type=2*
- *hxxp://193[.]56[.]29[.]123:8888/access.php?order=golc_finish&cmn=[Victim_HostName]&*

Examples of HolyRS.exe/BTLC.exe ransom note metadata:

Attacker email address: *HOlyGh0st@mail2tor[.]com*

Image location: *hxxps://cloud-*

ex42[.]jusaupload[.]com/cache/plugins/filepreviewer/219002/f44c6929994386ac2ae18b93f8270ec9ff8420d528c9e35a878efaa2d38fb94c/110

Report URL: *hxxp://matmq3z3hiovvia3voe2tix2x54sghc3tszj74xgdy4tqtypoycszqzqd[.]jonion*

Microsoft will continue to monitor DEV-0530 activity and implement protections for our customers. The current detections, advanced detections, and indicators of compromise (IOCs) in place across our security products are detailed below.

Recommended customer actions

Microsoft has implemented protections to detect these malware families as SiennaPurple and SiennaBlue (e.g., Ransom:Win32/SiennaBlue.A) via Microsoft Defender Antivirus and Microsoft Defender for Endpoint, wherever these are deployed on-premises and in cloud environments.

Microsoft encourages all organizations to proactively implement and frequently validate a data [backup and restore plan](#) as part of broader protection against ransomware and extortion threats.

The techniques used by DEV-0530 in H0lyGh0st activity can be mitigated by adopting the security considerations provided below:

- Use the included IOCs to investigate whether they exist in your environment and assess for potential intrusion.

Our [blog on the ransomware-as-a-service economy](#) has an exhaustive guide on how to protecting against ransomware threats. We encourage readers to refer to that blog for a comprehensive guide that has a deep dive into each of the following areas:

- Building credential hygiene
- Auditing credential exposure
- Prioritizing deployment of Active Directory updates
- Cloud hardening
 - Implement the [Azure Security Benchmark](#) and general [best practices for securing identity infrastructure](#).
 - Ensure cloud admins/tenant admins are treated with [the same level of security and credential hygiene](#) as Domain Admins.
 - Address [gaps in authentication coverage](#).
- Enforcing MFA on all accounts, remove users excluded from MFA, and strictly [require MFA](#) from all devices, in all locations, at all times.
- Enabling passwordless authentication methods (for example, Windows Hello, FIDO keys, or Microsoft Authenticator) for accounts that support passwordless. For accounts that still require passwords, use authenticator apps like Microsoft Authenticator for MFA.
- Disabling [legacy authentication](#).

For small or midsize companies who use Microsoft Defender for Business or Microsoft 365 Business Premium, enabling each of the features below will provide a protective layer against these threats where applicable. For Microsoft 365 Defender customers, the following checklist eliminates security blind spots:

- Turn on [cloud-delivered protection](#) in Microsoft Defender Antivirus to cover rapidly evolving attacker tools and techniques, block new and unknown malware variants, and enhance attack surface reduction rules and tamper protection.
- Turn on [tamper protection](#) features to prevent attackers from stopping security services.
- Run [EDR in block mode](#) so that Microsoft Defender for Endpoint can block malicious artifacts, even when a non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode also blocks indicators identified proactively by Microsoft Threat Intelligence teams.
- Enable [network protection](#) to prevent applications or users from accessing malicious domains and other malicious content on the internet.
- Enable [investigation and remediation](#) in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches.
- Use [device discovery](#) to increase visibility into the network by finding unmanaged devices and onboarding them to Microsoft Defender for Endpoint.
- [Protect user identities and credentials](#) using Microsoft Defender for Identity, a cloud-based security solution that leverages on-premises Active Directory signals to monitor and analyze user behavior to identify suspicious user activities, configuration issues, and active attacks.

Indicators of compromise

This list provides IOCs observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

Indicator	Type	Description
99fc54786a72f32fd44c7391c2171ca31e72ca52725c68e2dde94d04c286fccd	SHA-256	Hash of BTLC_C.exe
f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86	SHA-256	Hash of HolyRS.exe
bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e675d9f40af	SHA-256	Hash of BTLC.exe

Indicator	Type	Description
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	Command line	Example of new ScheduledTask to BTLC.exe
193[.]56[.]29[.]123	C2	C2 IP address
H0lyGh0st@mail2tor[.]com	Email	Ransomware payment communication address
C:\FOR_DECRYPT.html	File path	File path of ransom note

NOTE: These indicators should not be considered exhaustive for this observed activity.

Microsoft 365 detections

Microsoft Defender Antivirus

- [Trojan:Win32/SiennaPurple.A](#)
- [Ransom:Win32/SiennaBlue.A](#)
- [Ransom:Win32/SiennaBlue.B](#)

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint customers may see any or a combination of the following alerts as an indication of possible attack.

- DEV-0530 activity group
- Ransomware behavior detected in the file system
- Possible ransomware infection modifying multiple files
- Possible ransomware activity

Advanced hunting queries

Microsoft Sentinel

To locate possible DEV-0530 activity mentioned in this blog post, Microsoft Sentinel customers can use the queries detailed below:

Identify DEV-0530 IOCs

This query identifies a match based on IOCs related to DEV-0530 across various Sentinel data feeds:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/Dev-0530_July2022.yaml

Identify renamed file extension

DEV-0530 actors are known to encrypt the contents of the victim's device as well as rename the file and extension. The following query detects the creation of files with *.h0lyenc* extension:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/Dev-0530_FileExtRename.yaml

Identify Microsoft Defender Antivirus detection related to DEV-0530

This query looks for Microsoft Defender AV detections related to DEV-0530 and joins the alert with other data sources to surface additional information such as device, IP, signed-in on users, etc.

<https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SecurityAlert/Dev-0530AVHits.yaml>

Yara rules

```
rule SiennaPurple
{
    meta:
        author = "Microsoft Threat Intelligence Center (MSTIC)"
        description = "Detects PDB path, C2, and ransom note in DEV-0530 Ransomware SiennaPurple samples"
        hash =
            "99fc54786a72f32fd44c7391c2171ca31e72ca52725c68e2dde94d04c286fccd"
        strings:
            $s1 = "ForOP\\attack(utils)\\attack
            tools\\Backdoor\\powershell\\btlc_C\\Release\\btlc_C.pdb"
```

```

        $s2 = "matmq3z3hiovia3voe2tix2x54sghc3tszj74xgdy4tqtypoycszqzqd.onion"
        $s3 = "H0lyGh0st@email2tor.com"
        $s4 = "We are <HolyGhost>. All your important files are stored and
encrypted."
        $s5 = "aic^ef^bi^abc0"
        $s6 = "-----3819074751749789153841466081"

        condition:
            uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
            filesize < 7MB and filesize > 1MB and
            all of ($s*)
    }

rule SiennaBlue
{
    meta:
        author = "Microsoft Threat Intelligence Center (MSTIC)"
        description = "Detects Golang package, function, and source file names
observed in DEV-0530 Ransomware SiennaBlue samples"
        hash1 =
"f8fc2445a9814ca8cf48a979bfff7f182d6538f4d1fff438cf259268e8b4b76f86"
        hash2 =
"541825cb652606c2ea12fd25a842a8b3456d025841c3a7f563655ef77bb67219"
        strings:
            $holylocker_s1 =
"C:/Users/user/Downloads/development/src/HolyLocker/Main/HolyLock/locker.go"
            $holylocker_s2 = "HolyLocker/Main.EncryptionExtension"
            $holylocker_s3 = "HolyLocker/Main.ContactEmail"
            $holylocker_s4 = "HolyLocker/communication.
(*Client).GetPubkeyFromServer"
            $holylocker_s5 = "HolyLocker/communication.
(*Client).AddNewKeyPairToIntranet"

            $holyers_s1 =
"C:/Users/user/Downloads/development/src/HolyGhostProject/MainFunc/HolyRS/HolyRS.go"
            $holyers_s2 = "HolyGhostProject/MainFunc.ContactEmail"
            $holyers_s3 = "HolyGhostProject/MainFunc.EncryptionExtension"
            $holyers_s4 = "HolyGhostProject/Network.(*Client).GetPubkeyFromServer"
            $holyers_s5 = "HolyGhostProject/Network.
(*Client).AddNewKeyPairToIntranet"
            $s1 = "Our site : <b><a href=%s>H0lyGh0stWebsite"
            $s2 = ".h0lyenc"
            $go_prefix = "Go build ID:"
        condition:
            uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and
            filesize < 7MB and filesize > 1MB and
            $go_prefix and all of ($s*) and (all of ($holylocker_*) or all of
($holyers_*))
    }
}

```