# Avast finds compromised Philippine Navy certificate used in remote access tool

By Threat Research TeamThreat Research Team

Archived: 2026-04-05 17:43:42 UTC

Avast Threat Intelligence Team has found a remote access tool (RAT) actively being used in the wild in the Philippines that uses what appears to be a compromised digital certificate belonging to the Philippine Navy. This certificate is now expired but we see evidence it was in use with this malware in June 2020.

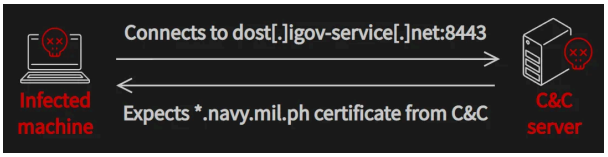
Based on our research, we believe with a high level of confidence that the threat actor had access to the private key belonging to the certificate.

We got in touch with CERT-PH, the National Computer Emergency Response Team for the Philippines to help us contact the navy. We have shared with them our findings. The navy security team later let us know that the incident has been resolved and no further assistance was necessary from our side.

Because this is being used in active attacks now, we are releasing our findings immediately so organizations can take steps to better protect themselves. We have found that this sample is now available on VirusTotal.

## Compromised Expired Philippine Navy Digital Certificate

In our analysis we found the sample connects to `dost[.]igov-service[.]net:8443` using TLS in a statically linked OpenSSL library.



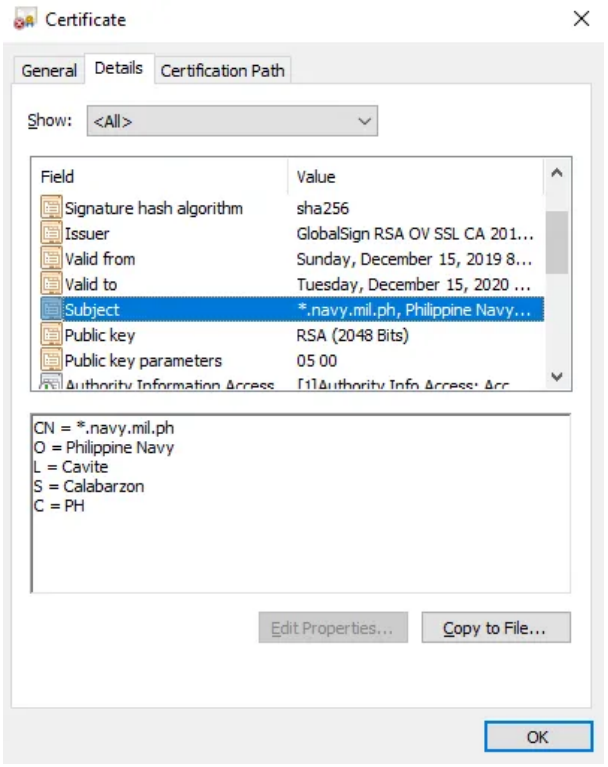

A WHOIS lookup on the C&C domain gave us the following:

Whois Lookup

```
Create date: 2019-12-09
Domain name: igov-service.net
Domain registrar id: 146
Domain registrar url: http://registrar.godaddy.com
Expiry date: 2021-12-09
Name server 1: ns01.domaincontrol.com
Name server 2: ns02.domaincontrol.com
Query time: 2019-12-10 17:42:29
Registrant address: 3267309318f7846c
Registrant city: 3267309318f7846c
Registrant company: 3267309318f7846c
Registrant country: United States
Registrant email: 3267309318f7846cs@
Registrant fax: 3267309318f7846c
Registrant name: 3267309318f7846c
Registrant phone: 3267309318f7846c
Registrant state: 40840a16fcb405fc
Registrant zip: 3267309318f7846c
Update date: 2019-12-09
```

The digital certificate was pinned so that the malware requires the certificate to communicate.

When we checked the digital certificate used for the TLS channel we found the following information:




Some important things to note:

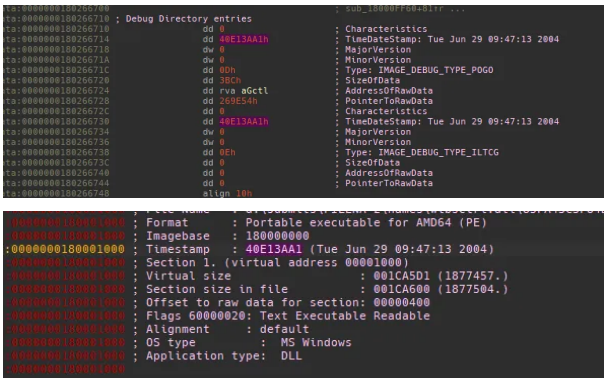
- The certificate is a valid certificate with a subject of `*.navy.mil.ph`, the Philippine Navy.
- The certificate has recently expired: it was valid for one year, from Sunday December 15, 2019 until Tuesday December 15, 2020.
- Our research shows that Censys saw this certificate employed by the actual navy.mil.ph website

Based on our research, we believe with a high level of confidence that the threat actor had access to the private key belonging to the certificate.

While the digital certificate is now expired we see evidence it was in use with this malware in June 2020.

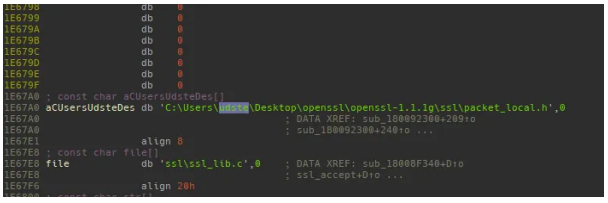
The malicious PE file was found with filename: `C:\Windows\System32\wlbsctrl.dll` and its hash is: `85FA43C3F84B31FBE34BF078AF5A614612D32282D7B14523610A13944AADAACB`.

In analyzing that malicious PE file itself, we found that the compilation timestamp is wrong or was edited. Specifically, the `TimeDateStamp` of the PE file was modified and set to the year 2004 in both the PE header and Debug Directory as shown below:




However, we found that the author used OpenSSL 1.1.1g and compiled it on April 21, 2020 as shown below:


The username of the author was probably `udste`. This can be seen in the debug information left inside the used OpenSSL library.




We found that the malware supported the following commands:

- run shellcode
- read file
- write file
- cancel data transfer
- list drives
- rename a file
- delete a file

- list directory content

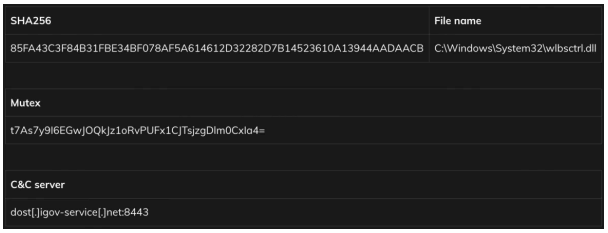

Some additional items of note regarding the malicious PE file:

- All configuration strings in the malware are encrypted using `AES-CBC` with the exception of the mutex it uses.That mutex is used as-is without decryption: `t7As7y9I6EGwJOQkJz1oRvPUFx1CJTsjzgDlm0CxIa4=`.
- When this string is decrypted using the hard-coded key it decrypts to `QSR_MUTEX_zGKwWAejTD9sDitYcK`. We suspect that this is a failed attempt to disguise this malware as the infamous Quasar RAT malware. But this cannot be the case because this sample is written in C++ and the Quasar RAT is written in C#.

Avast customers are protected against this malware.

## Indicators of Compromise (IoC)

- Repository: https://github.com/avast/ioc/tree/master/Philippine-Navy-Certificate




A group of elite researchers who like to stay under the radar.

---

Source: https://decoded.avast.io/threatintel/avast-finds-compromised-philippine-navy-certificate-used-in-remote-access-tool/