← Blog

Anastasia Tikhonova

Global Threat Research Lead

The Art of Cyberwarfare

Chinese APTs attack Russia

August 3, 2021 · min to read · Advanced Persistent Threats

APT China Malware

In mid-May 2021, experts from SOLAR JSOC and the National Computer Incident Response & Coordination Center (NCIRCC) released a joint report on a series of targeted attacks detected in 2020. According to the report, the attackers targeted Russian federal executive authorities.

While analyzing the report, **Anastasia Tikhonova** (Head of APT Research at Group-IB) and **Dmitry Kupin** (Senior Malware Analyst) noticed that they had already come across similar tools in earlier attacks.

Chinese APTs are one of the most numerous and aggressive hacker communities. Several dozen groups conduct attacks in countries all over the world, and Russia is no exception. Hackers mostly target state agencies, industrial facilities, military contractors, and research institutes. The main objective is espionage: attackers gain access to confidential data and attempt to hide their presence for as long as possible. There have been cases when attackers successfully persisted in the victim's network for several years.

Unfortunately, the SOLAR JSOC and NCIRCC report did not provide indicators of compromise, so the experts had to rely on descriptions of the functionality and screenshots of the malicious code. As a result, Group-IB's researchers came up with some interesting conclusions about which **Chinese groups could be behind the attacks against Russian federal executive authorities in 2020**, what tools they used, and how their malware has evolved since.

Key conclusions

The research describes Webdav-O malware detected in attacks against Russian federal executive authorities in 2020.

Group-IB experts detected two versions of the Webdav-O Trojan for x86 and x64 systems.

When comparing parts of the code, the specialists proved that the Webdav-O x64 Trojan was used in attacks against Russian federal executive authorities. The malware has existed since at least 2018.

Group-IB specialists established that Webdav-O has a set of commands similar to a popular Trojan called BlueTraveller (aka RemShell), which was developed in China and has been linked to the hacker group called TaskMasters.

Before that, Sentinel Labs released a report about malware called Mail-O, which was also identified in attacks against Russian federal executive authorities. Mail-O was deemed to be linked to the Chinese hacker group TA428.

Group TA428 is known to use a Trojan called Albaniiutas in their attacks. Group-IB's analysis showed that Albaniiutas is an updated version of BlueTraveller.

Group-IB experts believe that either both Chinese hacker groups (TA428 and TaskMasters) attacked Russian federal executive authorities in 2020 or that there is one united Chinese hacker group made up of different units.

TA428 is a Chinese state-sponsored hacker group that has been operating since 2013. The attackers target a number of government agencies in East Asia that control governmental information technology, domestic and foreign policy, and economic development. **TaskMasters (aka BlueTraveller) is a state-sponsored Chinese hacker group** that allegedly has been active since at least 2010. The group attacks companies based in several countries, but many of their targets are located in Russia and CIS.

The hackers target solid industrial and energy enterprises, government agencies, and transport companies.

Starting point

As the experts put it: "*The report dwells on the analysis of a series of targeted attacks*". Based on this information, we assumed that several hacker groups may be behind the attacks.

The attackers used malware that interacted with management server via the cloud service called Yandex.Disk. The malware was dubbed **Webdav-O**.

Attackers also used malicious software that accessed the cloud service Mail.ru. The malware was dubbed **Mail-O**.

In early June 2021, analysts from the American cybersecurity company Sentinel Labs released a report about Mail-O. The experts wrote that Mail-O is a version of the relatively well-known malware called SManager, which is used by the Chinese hacker group TA428.

Group-IB specialists wanted to make sure that Mail-O is loader, while Smanager and Tmanger are Remote Access Trojans (RAT). However, a part of the code overlaps in the exported functions "Entery" and "ServiceMain" of Mail-O, SManager and Tmanger, which brings us back to TA428. Moreover, hackers from TA428 have already been found to be involved in espionage against Russia, especially Russian state facilities.

To prove the hypothesis that TA428 was behind the attacks against Russian federal executive authorities in 2020, we decided to analyze a sample of Webdav-O. Group-IB Threat Intelligence & Attribution has detected similar malicious behavior before and can now explain why we link it to a specific group. Below we provide an analysis of Webdav-O samples and highlight features that overlap with the points mentioned in the SOLAR JSOC and NCIRCC report.

骑驴找马 [qí lǘ zhǎo mǎ] Verbatim translation: Ride a mule while looking for a horse. **Definition**: Use the tools you have while looking for something better.

Analysis of Webdav-O sample

Name	1.dll
SHA1	c9e03855f738e360d24018e2d203142c7ae6c2ec
Compilation timestamp	2018-07-12 03:08:01
First Submission	2019-11-07 10:34:11
Dll Name	y_dll.dll
Export function	ServiceMain

File "*1.dll*" is an x86 dynamic link library (DLL) that functions as a service in the system.

The analyzed file provides remote access to the command line shell (cmd.exe) and executes various commands originating from C2 on the compromised host.

The legitimate cloud service called Yandex.Disk (webdav.yandex.ru:443) is used as network infrastructure, namely C&C. Network interaction with the cloud is implemented via the Webdav protocol. The authentication method is Basic.

The strings and configuration data are encrypted with the RC4 algorithm using the following key: { **8A 4F 01 47 34 C9 75 F8 2B C8 C1 E9 D2 F3 A5 8B** }. The key size is 16 bytes. The analyzed files can work with 1-7 accounts (in this case only 2 are used, but we will come back to this later).

Features of the sample

1. The exported ServiceMain function uses a random delay before the main code is executed.

2. Yandex.Disk cloud accounts are checked for availability using the query “/?userinfo” (GET).

3. The file "*/test3.txt*" is uploaded from "Yandex.Disk" (GET) and checked for the "*Just A Test!*" line. In case of success, the system checks for batch files in the "*/test" directory of "Yandex.Disk*" (PROFIND).

4. A command file is defined for downloading from the Yandex.Disk cloud (GET). The response from the server is processed. The name of the file with commands is between the tags:

<d:href>[name of the command file]</d:href>

5. In the command file, the contents are encrypted using the RC4 algorithm. After downloading the command file, it is deleted from Yandex.Disk (DELETE).

6. The file "*/test2.txt*" is uploaded to Yandex.Disk (PUT). The file "*/test2.txt*" contains the line "*Just A Test!*". The mechanism is presumably used to check the functioning of a malicious program.

7. The file "*/test2/[0-9]{1,4}[0-9]{1,4}.bin*" is uploaded to "Yandex.Disk" (PUT). The file contains the command results. Data is encrypted using the RC4 algorithm.

Description of the commands

Command	Description
-upload	Uploads the file to Yandex.Disk cloud storage. The file name is specified in the command. The file is saved in the cloud under the following name: "[0-9]{1,4}[0-9]{1,4}.bin". Response format: "##u## %s %s".
-download	Downloads the file from Yandex.Disk cloud storage. The file name is specified in the command. The downloaded file is deleted from Yandex.Disk. Response format: "##d## %s".
-quit	Ends a session (exits the command execution flow).
-setsleep	Sets the waiting interval (in minutes) between command requests. Response format: "##s## %d".

Command	Description
[other	Runs the command in the command line shell (cmd.exe)

Comparison with the sample presented in the SOLAR JSOC and NCIRCC report

When analyzing the code uploaded to VirusTotal, we found many overlapping points with the Trojan described in the SOLAR JSOC and NCIRCC report. Some of the common features can be seen in the screenshot with the malware code, which shows the receipt of the command files list in the test folder:

Comparison of the Webdav-O sample from the report (on the left) to the VirusTotal sample (on the right)

Comparison of Webdav-O samples

Webdav-O sample from the report	Webdav-O x86

Basic authentication and **OAuth**	Basic authentication
List of commands (5): -upload -download -setsleep -quit [other command cmd.exe] **-sleepuntil**	List of commands (4) -upload -download -setsleep -quit [other command cmd.exe]
Command response format: ##u## %s %s (-upload) ##d## %s (-download) ##s## %d (-setsleep) **##l## %s (-sleepuntil)**	Command response format: ##u## %s %s (-upload) ##d## %s (-download) ##s## %d (-setsleep)

* Impossible to verify since there are no indicators (specifying Webdav-O file) in the report.

As you can see from our comparison of the two samples, Webdav-O from the SOLAR JSOC and NCIRCC report looks like a newer, partially improved version of the Trojan that we detected on VirusTotal.

Comparison of Webdav-O with the code of the BlueTraveller (RemShell) sample

> **见风转舵 [jiàn fēng zhuǎn duò] Verbatim translation**: If you feel the wind – change direction. **Meaning**: Change your tactics to avoid difficulties.

Based on a large database of analyzed malicious samples accumulated when searching and responding to cyber threats, Group-IB's specialists linked the detected Webdav-O sample to the **BlueTraveller Trojan**.

To prove our hypothesis, below we present a comparison of the Webdav-O x86 sample and the sample of BlueTraveller (RemShell) (SHA1: 6857BB2C3AE5F9C2393D9F88816BE7A10CB5573F).

Name	netui4.dll
SHA1	6857bb2c3ae5f9c2393d9f88816be7a10cb5573f
Compilation timestamp	2017-03-03 09:13:08
First Submission	2017-07-07 18:33:12
Dll Name	client_dll.dll
Export function	ServiceMain

Fragments of the pseudocode for processing (receiving) the "-upload" command in the samples of Webdav-O

Fragments of the pseudocode for processing (receiving) the "-download" command in the samples of Webdav-O

Fragments of pseudocode for processing (receiving) the "-quit" command in the sample of Webdav-O

Fragments of pseudocode for executing a command in the command line shell (cmd.exe) in the samples of Webdav-O

Original name of DLL **Webdav-O** (DIRECTORY_ENTRY_EXPORT) Dll name: y_**dll.dll**	Original name of DLL **BlueTraveller** (RemShell) (DIRECTORY_ENTRY_EXPORT) Dll name: client_**dll.dll**

Based on the above comparison, we can draw the following conclusions:

1. Similar DLL name (DIRECTORY_ENTRY_EXPORT – original DLL name)
2. Same command names
3. Same principle of command processing
4. Feature allowing to execute commands in the command line shell (cmd.exe)

Accounts, passwords, and attribution

路遥知马力, 日久见人心 [lù yáo zhī mǎ lì rì jiǔ jiàn rén xīn]
Verbatim translation: Having overcome a long distance, you will know a horse's endurance, and after a long time you will know what lies in a person's heart. **Definition**: Time reveals a person's true nature.

Let's go back to the analyzed sample of **Webdav-O x86**. When we decrypted the malware string, we found the following "login:password" for the attacker's accounts used on Yandex.Disk.

The data discovered:

aleshaadams:7ujm!QAZ2wsx

tstrobos:&UJM1qaz2ws

If the account login is known, it is possible to recover the email address as follows:

tstrobos@yandex.ru

aleshaadams@yandex.ru

Attempt to recover the password for aleshaadams@yandex.ru

The screenshots show that both accounts are linked to cellphone numbers in the same region (+86), which is the country code for China.

Analysis of password generation

In 2019, Elmar Nabigaev (Deputy Director of Expert Security Center Positive Technologies) delivered a report entitled "**The TaskMasters APT**" (aka BlueTraveller) and gave examples of passwords discovered when investigating the malware campaign:

The images above show that the passwords to the Webdav-O account were generated using a similar technique as TaskMasters. The only things that changed were the registry and the key row combination.

Blurring the boundaries

Considering all the comparisons made and the information discovered about the accounts, we believe that the Chinese hacker group **TaskMasters** is most likely behind the attacks involving an improved version of the Webdav-O Trojan. The case of TA428, however, is still open to debate. Could both of them be behind the attack against Russian federal executive authorities in 2020? Could there be someone else involved? Or was it the same group?

We will continue our investigation and seek more information for analysis. Let us take a look at the report about TA428 and their new tools, in particular the Trojan called Albaniiutas, which was released by NTT Security Corporation in 2020.

Executing Albaniiutas files, NTT report

The aim of our investigation is to study these two objects. Our reasoning will be presented below.

First and foremost, we discovered some common points in the utility used to launch DLL:

BlueTraveller	**Albaniiutas**
1.exe	vjsc.dll
>6303CCE6747703E81A5A52DEC11A3BA7DB26EA4B	2FE6AF7CE84CB96AE640BB6ED25A7BA
Utility for registering and running DLL as a service in the system and for removing this service.	DLL responsible for registering and runnin service in the system.
Launched in the command line shell (cmd.exe). Receives the following command line arguments: C:\Users\IEUser\Desktop\1.exe Usage: install -i DllPath or install -u ServiceName	Uploaded by the file “Scrpt.exe” (SHA1: BC708ACDF6B8B60577268A0788F1E375 – legitimate signed file “vjc.exe”. Original D “ServiceAdd.dll”.
“-i [DllPath]” – registering and running DLL as a service. “-u [ServiceName]” – deleting the specified service.	

Code parts of both utilities show the similarities in more detail. As can be seen, both samples use XOR encryption, which even displays identical debugging information.

Fragments of code encrypted with XOR and debugging lines in BlueTraveller

Fragments of code of the XOR encrypting function in BlueTraveller

Moreover, there are common points at the stage of establishing persistence in the system. The screenshots below show that the same DLL name randomization occurs. The same description of the service under which this DLL will work is also displayed.

Fragments of code with DLL name randomization in BlueTraveller

Let's continue our comparative analysis and take a look at a sample of BlueTraveller (SHA1:6857BB2C3AE5F9C2393D9F88816BE7A10CB5573F) and a fileless RAT belonging to the Albaniiutas family.

BlueTraveller	**Albaniiutas**
netui4.dll	–
6857BB2C3AE5F9C2393D9F88816BE7A10CB5573F	08645D079ABE05B88201DB0FF1C9B1EC0
DLL is a RAT.	Fileless DLL is a payload in the form of a RAT
Lauched via service (exported function ServiceMain).	Uploaded by the file "XpEXPrint.dll / [a-z]{4}.c (SHA1:

BlueTraveller	Albaniiutas
	AE57D779AAC235E979FAE617599377A099E It is contained in resources in an encrypted f
Original DLL name: “client_dll.dll”.	Original DLL name: “ClientX.dll”.

We also analyzed code parts that look very similar. For example, part of the pseudocode for executing commands in the command line shell (cmd.exe) is shown below.

Fragments of the code in BlueTraveller

Next, we analyzed the code parts of data processing received from the C&C server:

Fragments of the code in BlueTraveller

The parts of code above show that the code in BlueTraveller is less sophisticated, but in both cases the separator “\b” is used three times (the strtok function). Below is an example of the data that Albaniiutas malware receives for each command:

Format of the data received when executing commands (retrieved from the NTT report)

1. If the command is executed multiple times, the command will not be executed unless a value other than the previous one is specified.
2. Separator
3. If the value does not match the value in ③, the command will not be executed.
4. Command identifier and command parameters separated by spaces.

Let's also compare the code fragments for checking and executing the commands received from the C&C server:

Fragments of code in BlueTraveller

It is clear that this part was updated by the hackers, but the commands remain the same:

Command	Options	Description
-exit		Terminates the function for receiving and processing commands (exiting the flow)

Command	Options	Description
-download	Downloads URLs or Path to the storage directory	Downloads a file from the C&C server
-upload	Path to the file on the infected device or Part of path of the URL-address during the upload	Uploads a file to the C&C server
(command)	Command arguments	Executes the command with cmd.exe and returns the result to the C&C server.

In addition, the two Trojans have a similar pattern of communicating with the control server in the protocols of network interaction with the C&C server. Below is an example of network communication with the C&C server, taken from BlueTraveller samples available on VirusTotal.

BlueTraveller	Albaniiutas
http://45.32.188[.]226/0000/1301/0024/4u/i7fr09bGus+Wyt7iyjos=	http://go.vegispaceshop[.]org/l 8QIRN2+6+O3gKV6ODd2mEPI
Template: [IP]/[0000 or 1111]/[0-9]{4}/[0-9]{4}/[base64 data]	Template: [domain]/[dir]/[0-9]{4}

Let's move on to string obfuscation in Albaniiutas. We have established that strings are encrypted using the RC4 algorithm. The encryption key used is **L!Q@W#E$R%T^Y&U*A]}t~k**.

The same encryption key was used in the BlueTraveller server component which stores the log files in the encrypted form:

A fragment of code with a line written to a log file (retrieved from PTSecurity "Operation TaskMasters" 2019)

The conclusion is clear: Albaniiutas is nothing but a logic continuation of the malware belonging to the BlueTraveller family.

And then it dawned on us...

We thought that we had analyzed everything and that we were done with comparisons, when suddenly a sample was uploaded to VirusTotal. We identified it as Webdav-O.

Name	y_dll.dll
SHA1	3ff73686244ca128103e86d8c5aa024e37e7b86d
Compilation timestamp	2018-12-06 11:15:35
First Submission	2021-06-05 04:41:00
Dll Name	y_dll.dll
Export function	ServiceMain

The file “y_dll.dll” is an x64 dynamic link library (DLL) that functions as a service in the system.

As can be seen, this version of Webdav-O was written for a system with a different bitness and compiled later than our sample of Webdav-O x86 (2018-12 and 2018-07, respectively).

The legitimate cloud service Yandex.Disk (webdav.yandex.ru:443) is also used as a network infrastructure, in particular C2. Network interaction with the cloud is carried out via a Webdav protocol.

However, this sample supports two authentication methods instead of one in Webdav-O x86: Basic (with a username and password) and OAuth (using a token).

The strings and configuration data are encrypted using the RC4 algorithm with the following key: { **C3 02 03 04 05 DD EE 08 09 10 11 12 1F D2 15 16** }. The key size is 16 bytes. The analyzed file can work with 1-7 accounts (it works with only one in this case).

This sample seemed even more similar to the one described in the SOLAR JSOC and NCIRCC report: unlike our sample, it has the “-sleepuntil” function.

Unfortunately colleagues at SOLAR JSOC and NCIRCC did not provide any indicators of compromise, so we can only make comparisons based on screenshots and descriptions of the

capabilities of their sample.

Webdav-O sample from the report

Webdav-O sample from the report

The parts of code presented above show that both versions look identical. Group-IB experts also noticed that in Webdav-O x64, the commands and their results are transferred by uploading various files to Yandex.Disk:

Description of files created by **Webdav-O from the report**:

- **test2.txt, test3.txt.** are files used to check the connection
- **test4.txt** contains information about the interval (minutes) between command requests to the server
- **test5.txt** contains the launch date for the malware
- **test7.txt** is uploaded to the server and contains a 16-byte RC4 key that is used to encrypt commands and their results (the
- **key** is also encrypted with a public RSA key)
- **test** is a directory containing files that are downloaded, decrypted, and processed as commands. Malware receives the file list via the PROPFIND request and by parsing the necessary tags: <d:href>complete path to file</d:href>.

Description of the files created by Webdav-O x64:

File/ Directory	Description
test2.txt, test3.txt	Used to verify the connection. Example of “test2.txt” content: “Just A Test!”
test4.txt	Contains the waiting interval (in minutes) between command requests. Example of “test4.txt” content: 15
test5.txt	Contains the date and time until which the malware will be in sleep mode. Format: %d-%d-%d_%d:%d:%d, example of file “test5.txt” content: 2021-03-02_14:30:00
test6.txt	Contains an OAuth token. The content is encrypted using the RC4 algorithm with the following key: { 8A 4F 01 47 34 C9 75 F8 2B C8 C1 E9 D2 F3 A5 8B } (16 bytes). It is noteworthy that this key has already been used by another sample of our Webdav-O x86 to encrypt strings and configuration data.
test7.txt	It is loaded onto the server and contains a RC4 session key (16 bytes), which is used to encrypt commands and their results (the key itself is encrypted with a public RSA key). RC4 session keys are generated using the BCryptGenRandom function;

The data presented above shows that this part is also identical except for the description of test6.txt, which is not presented in the SOLAR JSOC and NCIRCC report.

Based on the comparisons above, Group-IB experts have concluded that this particular Webdav-O sample was most likely used in attacks on Russian federal executive authorities in 2020 and it is the same Trojan as the one described in the SOLAR JSOC and NCIRCC report.

To sum up...

人心齐，泰山移 [rén xīn qí, tài shān yí] **Verbatim translation**: United, people can move even Mount Taishan.
Definition: By working together people can accomplish anything.

Venn diagram showing the common points between the two Trojans (Only data presented in the blog is used in the diagram)

Webdav-O malware is a version of the BlueTraveller (RemShell) Trojan, which is classified as a Chinese APT. Webdav-O was designed for both x86 and x64 systems.

Webdav-O may have been used by the Chinese APT TaskMasters (aka BlueTraveller). Based on the information about attacks on various federal executive authorities in 2020, presented in the SOLAR JSOC and NCIRC report, it is possible that in some cases the Chinese APT TA428 was behind the attacks, while others could have been performed by TaskMasters.

Researchers from SentinelLabs have linked Mail-O to Smanager and Tmanger (tools used by TA428). Group-IB specialists found common code parts in the malware's exported functions "Entery" and "ServiceMain". We can say with moderate confidence that Mail-O was developed by TA428.

Based on research done by NTT Security, it can be said that TA428 has already used the malware Albaniiutas. Group-IB experts have shown that the Trojan is a new version of BlueTraveller (RemShell). As such, it can be assumed that Webdav-O is also linked to TA428.

It is noteworthy that Chinese hacker groups actively exchange tools and infrastructure, but perhaps it is just the case here.

There is also strong evidence that points to one large hacker group consisting of several intelligence units of the People's Liberation Army of China. For example, unit 61398 from Shanghai is responsible for the actions of a well-known group called APT1 (aka Comment Crew), and unit 61419 from Qingdao has been linked to Tick. Each unit attacks to the fullest, according to a strict timeline and order. This means that one Trojan can be configured and modified by hackers from different departments with different levels of training and with various objectives.

IoCs

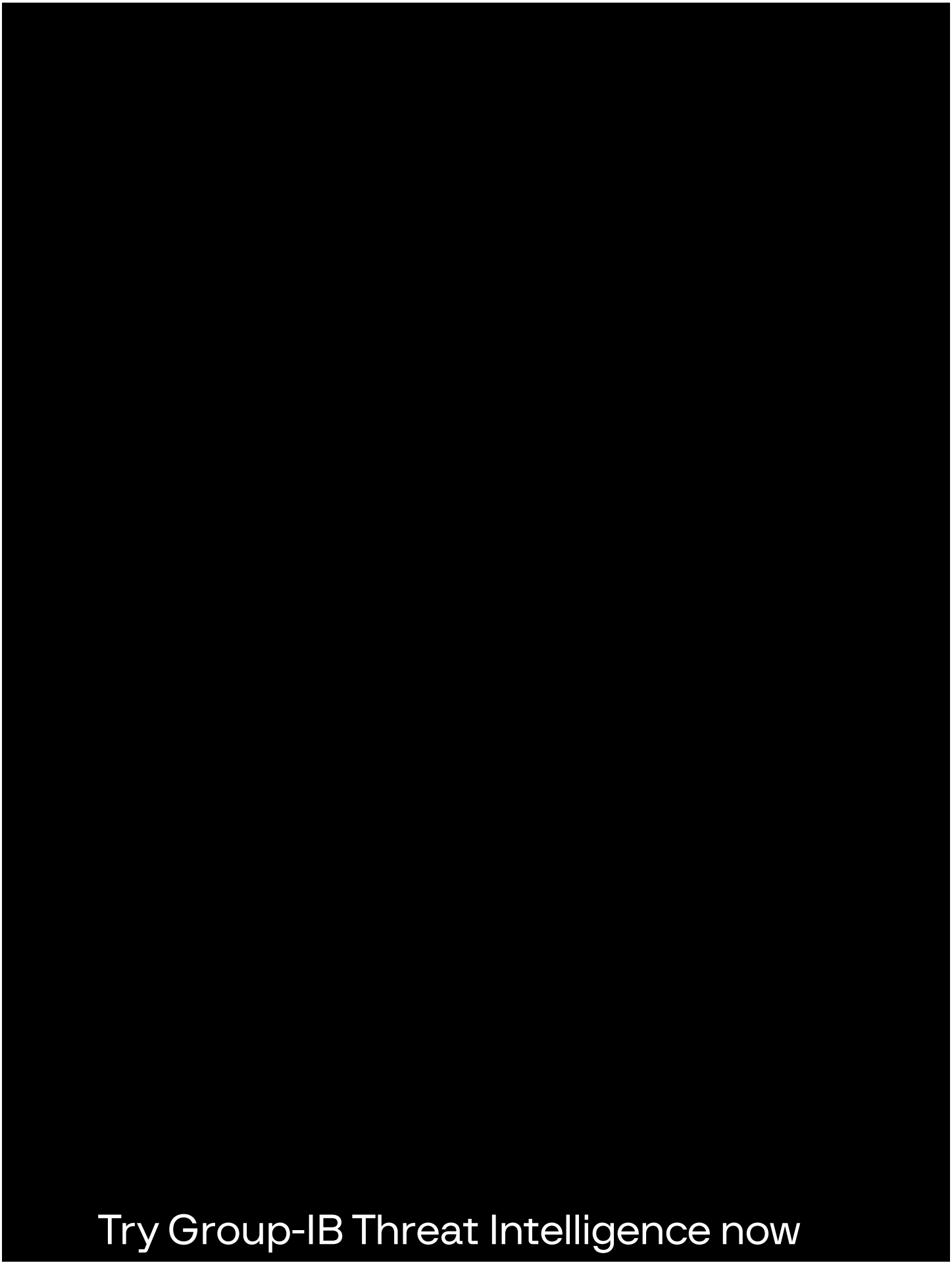
In Yandex.Disk cloud storage

On the host

Email

Network indicators

Hash


Try Group-IB Threat Intelligence now

YARA rule

```
import "pe"

rule webdavo_rat
{
  meta:
    author = "Dmitry Kupin"
    company = "Group-IB"
    family = "webdavo.rat"
    description = "Suspected Webdav-O RAT (YaDisk)"
    sample = "7874c9ab2828bc3bf920e8cdee027e745ff059237c61b7276bbba5311147ebb6" // x86
    sample = "849e6ed87188de6dc9f2ef37e7c446806057677c6e05a367abbd649784abdf77" // x64
    severity = 9
    date = "2021-06-10"

  strings:
    $rc4_key_0 = { 8A 4F 01 47 34 C9 75 F8 2B C8 C1 E9 D2 F3 A5 8B }
    $rc4_key_1 = { C3 02 03 04 05 DD EE 08 09 10 11 12 1F D2 15 16 }
    $s0 = "y_dll.dll" fullword ascii
    $s1 = "test3.txt" fullword ascii
    $s2 = "DELETE" fullword wide
    $s3 = "PROPFIND" fullword wide

  condition:
    (any of ($rc4_key*) or 3 of ($s*)) or
    (
     pe.imphash() == "43021febc8494d66a8bc60d0fa953473" or
     pe.imphash() == "68320a454321f215a3b6fcd7d585626b"
    )
}
```

```
rule albaniiutas_dropper_exe
{
  meta:
    author = "Dmitry Kupin"
    company = "Group-IB"
    family = "albaniiutas.dropper"
    description = "Suspected Albaniiutas dropper"
    sample = "2a3c8dabdee7393094d72ce26ccbce34bff924a1be801f745d184a33119eeda4" // csrss.
    sample = "71750c58eee35107db1a8e4d583f3b1a918dbffbd42a6c870b100a98fd0342e0" // csrss.
    sample = "83b619f65d49afbb76c849c3f5315dbcb4d2c7f4ddf89ac93c26977e85105f32" // droppe
    sample = "690bf6b83cecbf0ac5c5f4939a9283f194b1a8815a62531a000f3020fee2ec42" // droppe
    severity = 9
    date = "2021-07-06"

  strings:
    $eventname = /[0-9A-F]{8}-[0-9A-F]{4}-4551-8F84-08E738AEC[0-9A-F]{3}/ fullword ascii w
    $rc4_key = { 00 4C 21 51 40 57 23 45 24 52 25 54 5E 59 26 55 2A 41 7C 7D 74 7E 6B 00
    $aes256_str_seed = { 00 65 34 65 35 32 37 36 63 30 30 30 30 31 66 66 35 00 } // e4e52
    $s0 = "Release Entery Error" fullword ascii
    $s1 = "FileVJCr error" fullword ascii
    $s2 = "wchWSMhostr error" fullword ascii
    $s3 = "zlib err0r" fullword ascii
    $s4 = "De err0r" fullword ascii
    $s5 = "CreateFileW_CH error!" fullword ascii
    $s6 = "GetConfigOffset error!" fullword ascii

  condition:
    5 of them or
    (
     pe.imphash() == "222e118fa8c0eafeef102e49953507b9" or
     pe.imphash() == "7210d5941678578c0a31adb5c361254d" or
     pe.imphash() == "41e9907a6c468b4118e968a01461a45b"
    )
}

rule albaniiutas_rat_dll
{
  meta:
    author = "Dmitry Kupin"
    company = "Group-IB"
    family = "albaniiutas.rat"
    description = "Suspected Albaniiutas RAT (fileless)"
    sample = "fd43fa2e70bcc3b60236366756049422928 7bf4716638477889ae3f816efc705" // dumped
    severity = 9
    date = "2021-07-06"
```

```
    strings:
      $rc4_key = { 00 4C 21 51 40 57 23 45 24 52 25 54 5E 59 26 55 2A 41 7C 7D 74 7E 6B 00 }
      $aes256_str_seed = { 00 30 33 30 34 32 37 36 63 66 34 66 33 31 33 34 35 00 } // 03042
      $s0 = "http://%s/%s/%s/" fullword ascii
      $s1 = "%s%04d/%s" fullword ascii
      $s2 = "GetRemoteFileData error!" fullword ascii
      $s3 = "ReadInjectFile error!" fullword ascii
      $s4 = "%02d%02d" fullword ascii
      $s5 = "ReadInject succeed!" fullword ascii
      $s6 = "/index.htm" fullword ascii
      $s7 = "commandstr" fullword ascii
      $s8 = "ClientX.dll" fullword ascii
      $s9 = "GetPluginObject" fullword ascii
      $s10 = "D4444 0k!" fullword ascii
      $s11 = "D5555 E00r!" fullword ascii
      $s12 = "U4444 0k!" fullword ascii
      $s13 = "U5555 E00r!" fullword ascii

    condition:
      5 of them
  }
```

References

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends