← Blog

Anastasia Tikhonova

Global Threat Research Lead

Nice Try Tonto Team

How a nation-state APT attempted to attack Group-IB

February 13, 2023 · min to read · Advanced Persistent Threats

APT China Hacker group Threat Intelligence

In 2023, IT and cybersecurity companies remain one of the most attractive targets for cybercriminals, according to the latest threat report "**Hi-Tech Crime Trends 2022/2023**". The compromise of a vendor's infrastructure opens up ample opportunities to penetrate the network further and gain access to a huge pool of data about the victim's customers and partners. Remember how the SolarWinds attack put Microsoft, Cisco, FireEye, Mimecast, and 18,000 other companies at risk?

In light of the military conflict, **nation-state threat actors from around the world,** including from countries that are not directly involved in the crisis, **are actively carrying out cyber espionage operations.**

In the summer of 2022, the Group-IB **Managed Extended Detection and Response** (MXDR) solution successfully detected and blocked an email carrying a malicious attachment. This email was intended for Group-IB's employees. While analyzing this attack, **Anastasia Tikhonova**, Head of APT Research, and **Dmitry Kupin**, Senior Malware Analyst, at the Group-IB Threat Intelligence team found patterns in the actions of the attackers and attributed the observed TTPs to Tonto Team. The results of their research are worthy of a separate blog. These findings were presented at GovWare 2022 in Singapore by Anastasia Tikhonova.

As always, we provide indicators of compromise associated with **the Tonto Team campaign** and detailed analysis of the tools, techniques, and procedures (TTPs) of the threat actor in the MITRE ATT&CK® format (Adversarial Tactics, Techniques & Common Knowledge). This information is useful for organizations fighting cybercrime and information security professionals — chief information officers, SOC analysts, and incident responders — in other sectors targeted by **Tonto Team**. Our goal is to assist in the adoption of preventive measures against **the Tonto Team attacks**.

Key findings

In June 2022, the Group-IB **Managed XDR solution detected and blocked an attempt to deliver a malicious email to Group-IB's employees**.

The attackers used phishing emails to deliver malicious Microsoft Office documents created with **the Royal Road Weaponizer**, a tool widely used by Chinese nation-state threat actors.

During the attack, Group-IB researchers noticed the use of the Bisonal.DoubleT backdoor. Bisonal.DoubleT is a unique tool developed by the Tonto Team APT.

The attackers used a new downloader that Group-IB analysts named **TontoTeam.Downloader** (aka **QuickMute**).

Who is Tonto Team?

Tonto Team (aka **HeartBeat, Karma Panda, CactusPete, Bronze Huntley, Earth Akhlut**) is a cyber espionage threat actor that is believed to originate from China. The threat actor has been targeting government, military, energy, financial, educational, healthcare, and technology sector companies since 2009. **Initially focusing on Asia Pacific** (South Korea, Japan, Taiwan), and **the United States**, by 2020, the group had expanded its operations to **Eastern Europe**.

Nation state apt it all started with an email...

On the evening of June 20, 2022, Group-IB Managed XDR triggered an alert and blocked malicious emails that were sent to two Group-IB employees:

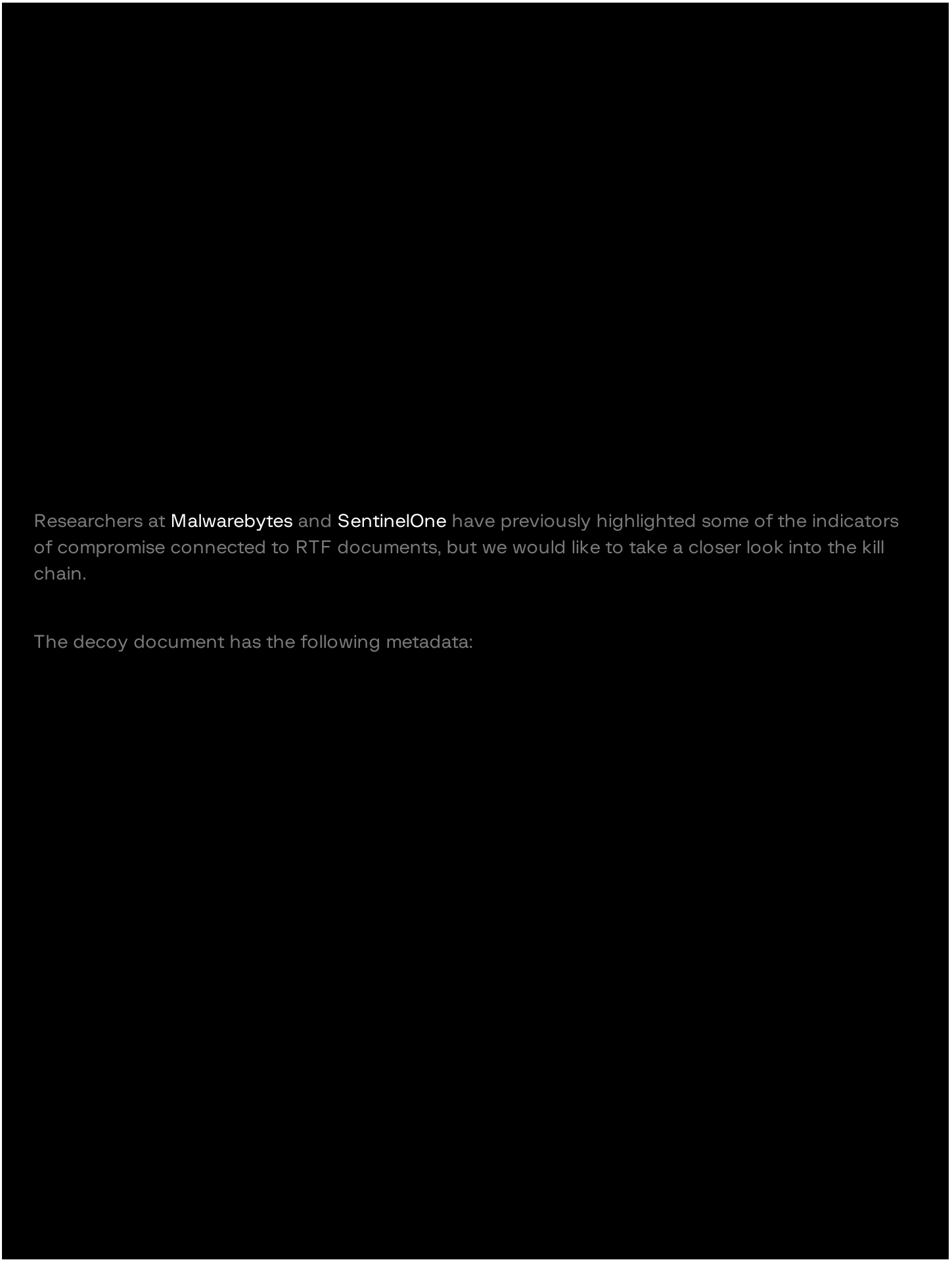
Screenshots of alerts in Group-IB Managed XDR (Subject of the letter: State cloud issues in terms of information security. Meeting protocol)

The threat actors posed as an employee of a legitimate company and used a fake mail created with **GMX Mail (Global Message eXchange)**, a free email service. The targeted phishing emails were supposed to be the first stage of an attack.

Analysis of the malicious document

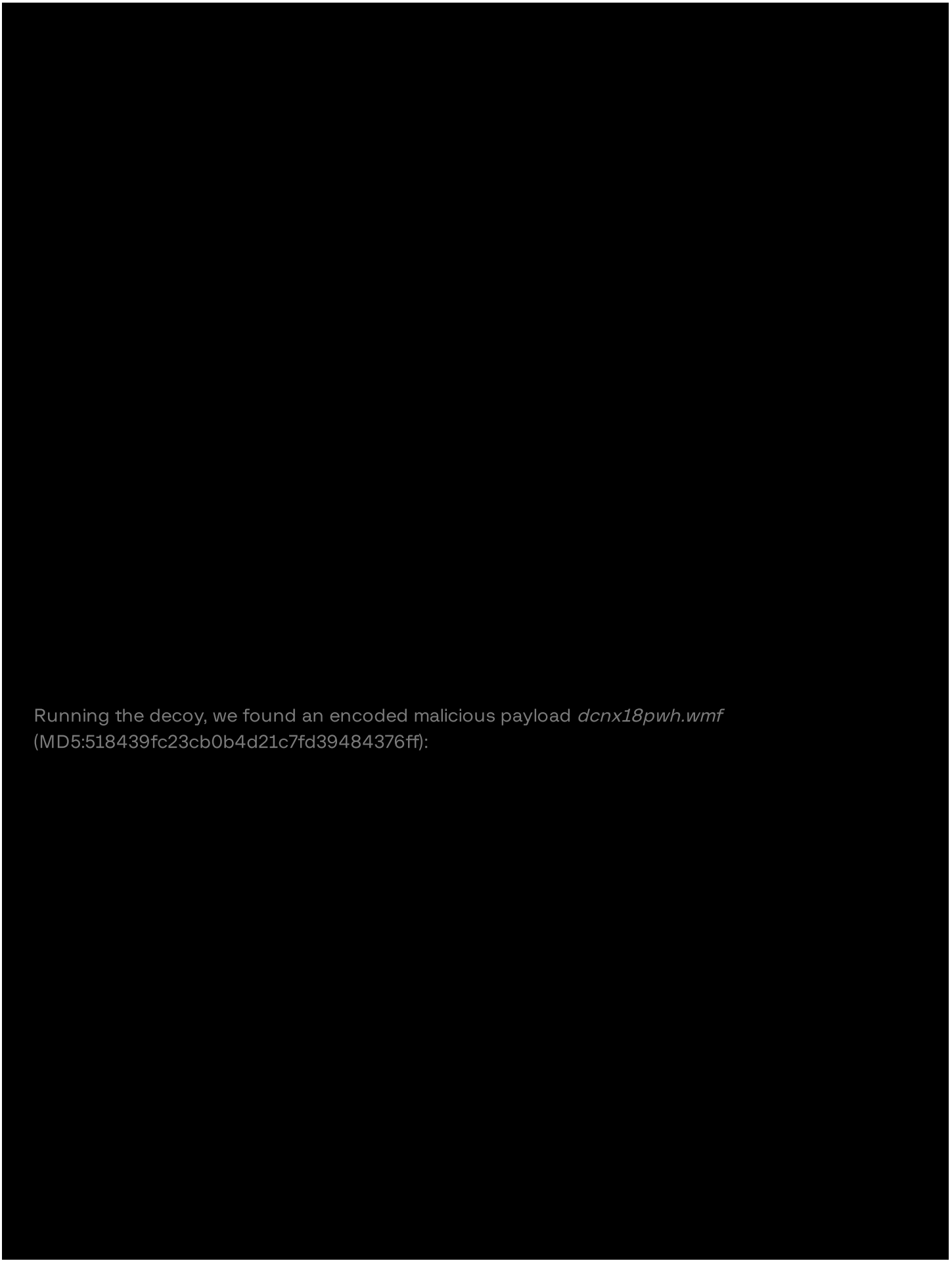
The file "*17.06.2022_Протокол_МРГ_Подгруппа_ИБ.doc*" was attached to the email:

The analyzed file is a malicious document in a Rich Text Format (RTF) that was created via the **Royal Road RTF Weaponizer**. **The weaponizer is mainly used by Chinese APT groups**. The tool allows the threat actor to create malicious RTF exploits with plausible decoy content for *CVE-2017-11882, CVE-2018-0802, and CVE-2018-0798*, which are the vulnerabilities in the **Microsoft Equation Editor.**



Researchers at Malwarebytes and SentinelOne have previously highlighted some of the indicators of compromise connected to RTF documents, but we would like to take a closer look into the kill chain.

The decoy document has the following metadata:



Running the decoy, we found an encoded malicious payload *dcnx18pwh.wmf* (MD5:518439fc23cb0b4d21c7fd39484376ff):

Analysis of the decrypted payload

The decrypted payload was a malicious EXE file in PE32 format (MD5:e40c514739768ba04ab17ff0126c1533) that can be classified as a **Bisonal.DoubleT** backdoor. This malware provides remote access to an infected computer and allows an attacker to execute various commands on it.

We conducted a static analysis of the Bisonal.DoubleT sample to compare it with an old version detected in 2020 (MD5:c3d25232add0238d04864fc992e7a330) and found similar strings:

In addition, we conducted a dynamic comparison analysis of the sample obtained in 2022 with other samples in the Bisonal.DoubleT malware family:

MD5	**e40c514739768ba04ab17ff0126c1533 (sample 2022)**	**c3c (sa**
URL	hXXp://137.220.176[.]165/ru/order/index.php?strPageID=234989760	hX upc strF
User-Agent	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7\r\nCookie: JSESSIONID=AHAKQAIOMIBQAAA3HEKQAAIAAAAAMAAAAAAQAAAAAEFAASSFKJJE6TCEFVIEGBQAJVUWO5LFNQFAASSFKJJE6TCEFVIEGAAAAIADEMQ=	Mo App Chr

The identical patterns of network requests are highlighted in red, and the generated ID is in blue.

Sample 2022 with MD5: e40c514739768ba04ab17ff0126c1533

Sample 2020 with MD5: c3d25232add0238d04864fc992e7a330

In the sample obtained in 2020, we have found traces of communication with the C2 server *offices-update[.]com*, which was also mentioned by IZ:SOC in connection with another Bisonal malware sample.

Connection to the C2 of the Bisonal sample from the IZ:SOC public report

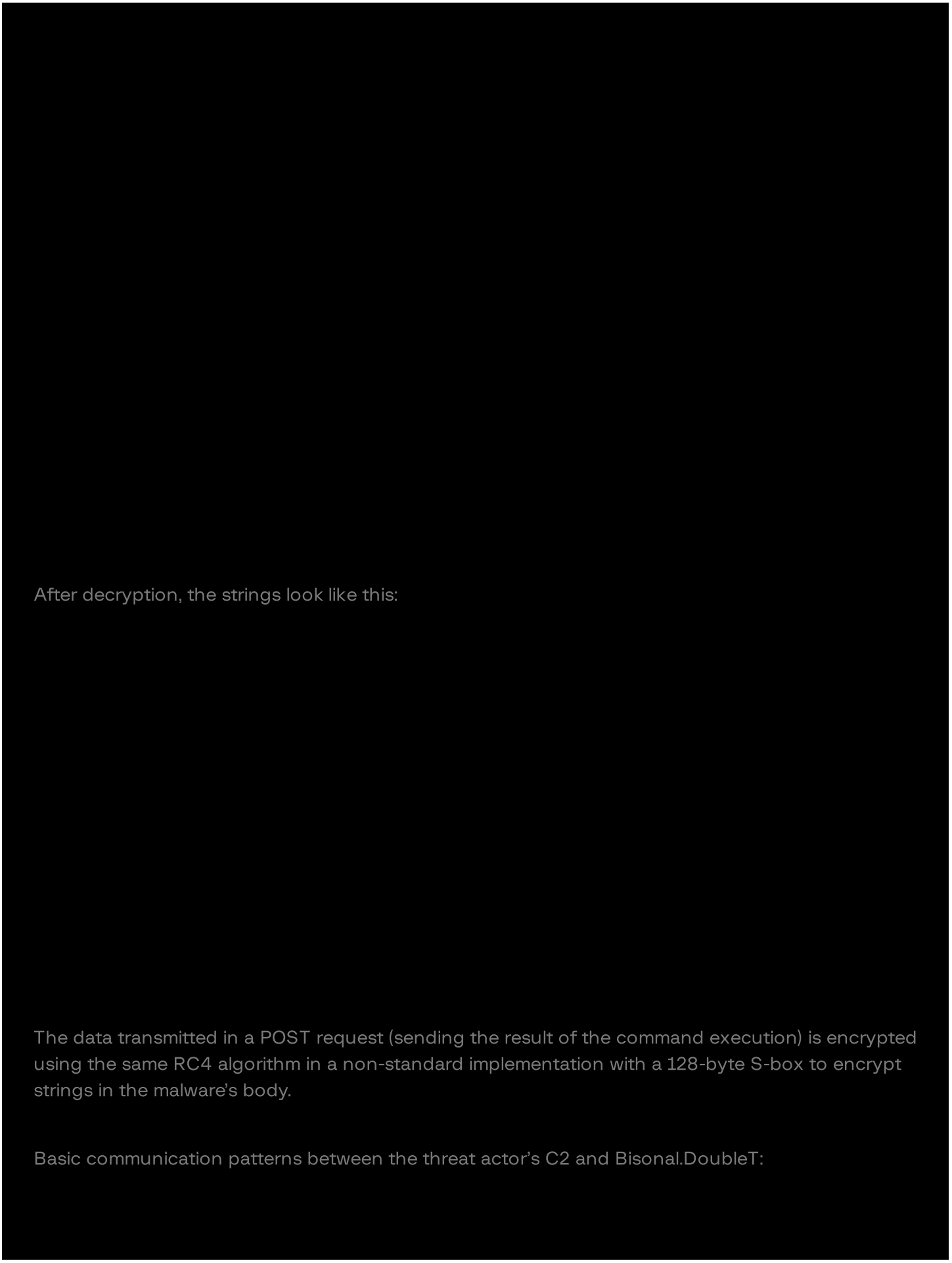
As you can see from the table and the screenshot above, the network requests are very similar.

The main functionality of Bisonal.DoubleT:

- collecting information about the compromised host: system language encoding, proxy server address, time since system boot, hostname, account name under which the file is running, and local IP address;
- getting a list of processes;
- stopping a specified process;
- getting remote access to cmd.exe;
- downloading a file from the control server and running it;
- creating a file on a disk using the local language encoding.

The collected information about the compromised host is encoded using the Base32 algorithm.

All of the important strings are encoded using the following RC4 algorithm in a non-standard implementation with a 128-byte S-box:



After decryption, the strings look like this:

The data transmitted in a POST request (sending the result of the command execution) is encrypted using the same RC4 algorithm in a non-standard implementation with a 128-byte S-box to encrypt strings in the malware's body.

Basic communication patterns between the threat actor's C2 and Bisonal.DoubleT:

Request	Template	Example
Hello – GET request	hXXps://137[.]220[.]176[.]165/ru/order/index.php?strPageID=[ID], where ID is a decimal number	hXXps://137[.]220 strPageID=16788
Command – GET request	hXXps://137[.]220[.]176[.]165/ru/news/index.php?strPageID=[ID]&newsID=[YYYY-MM-DD-mmss]	hXXps://137[.]220 strPageID=16788
Response – POST request	hXXps://137[.]220[.]176[.]165/xhome[.]native[.]page/datareader.php?sid=[ID]	hXXps://137[.]220 sid=167880896
Download & Execute – GET request	hXXps://137[.]220[.]176[.]165/siteFiles/index.php?strPageID=[ID]	hXXps://137[.]220 strPageID=16788

Attribution

The set of files described above can be considered related to the cyberespionage group Tonto Team. The Bisonal.DoubleT malware was previously attributed to this threat actor and has

been used by the group since at least 2019.

Analysis of the network infrastructure showed the usage of the IP address (*137[.]220[.]176[.]165*), which had previously been seen **in the Tonto Team attacks**. The document was also created in the Royal Road RTF Weaponizer.

Thus, there are several connections between the attempted attack against Group-IB and the Tonto Team APT:

- Metadata in the decoy documents indicates that the operating system language of the document's author was Simplified Chinese.

Documents are created in Royal Road, the well-known malicious document builder widely used by Chinese APT groups.

Malicious documents are commonly used to deliver custom malware. **Bisonal** and its **DoubleT** version are both existing for over 10 years with continuous development and are attributed to the Tonto Team.

It was not the first time the Tonto Team has shown interest in the IT sector. In March 2021, the group hacked into the email servers of a purchasing company and a software development and cybersecurity consulting company based in Eastern Europe.

Therefore, Group-IB specialists assess with high confidence that this activity was carried out by the Tonto Team.

We've seen them before

During the research, we wondered **if it was not the first attempt of the Tonto Team to attack Group-IB**. To answer this question, we have studied the entire Group-IB Managed XDR database of neutralized malicious mailings and discovered that **in the summer of 2021 the threat actor tried to attack Group-IB employees**. The attempt was unsuccessful.

The screenshot below shows that on June 28, 2021, the Group-IB Managed XDR blocked an email sent to our employees. This email contained a file that we identified as malicious:

The **Group-IB malware detonation platform analyzed the malicious attachment**, so we were able to see the following picture:

Is it really the same scheme?

In 2021, **the threat actor used spearphishing** as the initial attack vector and once again employed fake mail registered with the GMX Mail service.

The analyzed file "*30 июня В 17.30 – очередное заседание Исполкома АДЭ.doc*" (MD5:7c138c6b6f88643d7c16e741f98e0503) is a malicious RTF document that was created in the Royal Road RTF Weaponizer, similar to the email attachment used in the 2022 attack on Group-IB.

The decoy has the following metadata:

Malicious encoded payload (8.t MD5: d5d0a1a034dcefdb08d9ca51c7694a22):

Analysis of the decrypted payload

The decrypted payload is a malicious PE32 format DLL file that can be classified as **Bisonal.Dropper**. This malware is used to deploy the Bisonal backdoor on the victim's system.

Compiled Date: 06/28/2021 01:44:01 UTC (which is 9:44 Beijing time – the beginning of a workday in China)

Bisonal.Dropper creates a file "*%AppData%|Roaming|conhost.exe*" (Bisonal.DoubleT backdoor). It records random overlay data to "conhost.exe" to change the backdoor hash.

The dropper also adds “conhost.exe” to the system startup by creating a registry key setting:

```
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] userInit = "%AppData%\Roaming\conhos
```

The backdoor will run only after a system reboot. Bisonal.DoubleT may write the following error messages to the log file “*%windows%|temp|log.txt*“:

“[!] get pRegSetValueEx error\n”

“[!] get pGetProcAddress error\n”

“[!] get LoadLibraryA error\n”

“conhost.exe” (MD5: f53965ab81f746f5a2bf183d2a704c72) is a malicious EXE file in PE32 format that can be classified as a Bisonal.DoubleT backdoor. Comparing this sample from 2021 with the sample from 2022, we haven’t found any difference in functionality and encryption algorithms.

In the 2021 sample, all important strings are also encoded using the RC4 algorithm in a non-standard implementation with a 128-byte S-box:

After decryption, the strings look like this:

In addition, we compared the decrypted strings of the 2022 and 2021 samples. The different strings of the 2022 sample are marked in red, and the strings of the 2021 sample are highlighted in yellow. Below is the result of comparing the strings of the indicated Bisonal.DoubleT samples:

Basic communication patterns between C2 and Bisonal.DoubleT:

Request	Template	Example
Hello – GET request	hXXps://103[.]85[.]20[.]194/ru/order/index.php?strPageID=[ID], where ID is a decimal number	hXXps://103[.]85[.]2 strPageID=167880
Command – GET request	hXXps://103[.]85[.]20[.]194/ru/news/index.php?strPageID=[ID]&newsID=[YYYY-MM-DD-mmss]	hXXps://103[.]85[.]2 strPageID=167880
Response – POST request	hXXps://103[.]85[.]20[.]194/xhome[.]native[.]page/datareader.php?sid=[ID]	hXXps://103[.]85[.]2 sid=167880896
Download & Execute – GET request	hXXps://103[.]85[.]20[.]194/siteFiles/index.php?strPageID=[ID]	hXXps://103[.]85[.]2 strPageID=167880

So, there's nothing new at all?

In the 2022 attack, Tonto Team used a new downloader that Group-IB named **TontoTeam.Downloader**. It has also been called **QuickMute** in another public source.

As usual, the group used a malicious RTF document that was created in Royal Road — *Вниманию.doc* (MD5: 8cdd56b2b4e1e901f7e728a984221d10).

Malicious encoded payload:

Analysis of TontoTeam.Downloader

The decrypted payload is a malicious EXE file in PE32 format (MD5: 66c46b76bb1a1e7ecdb091619a8f5089), which can be classified as a downloader. **This file is used to download malware for the next stage of the attack**, which is a DLL with the specified export function “HttpsVictimMain”.

The configuration data of the analyzed file is encrypted using RC4. The key is contained in the malware body and is 256 bytes long.

Decrypted configuration data:

```
https!upportteam[.]lingrevelat[.]com$443$1111111111111111111111111111111111111111111111111
```

Parameter	Value	Description

param_1	https	Network protocol type
param_2	upportteam[.]lingrevelat[.]com	Domain name
param_3	443	Network port
param_4	111111111111111111111111111111111 111111111111111111111111111111111111111 111111111111111111111111111111111 111111111111111111111111111111111111111111111111111111	Setting the operating time (malware works at a certain time on certain days of the week)
param_5	{A931568B-94AF-449D-B7F6-6585EF9E9839}	Mutex name
param_6	https-note-86	Unknown, possibly malware ID

The functionality of the TontoTeam.Downloader:

- Multithreading.
- Passing important strings (the name of the exported function, User-Agent, URL path, etc.) through the stack.
- Using encryption algorithms: RC4, XOR.
- Creating a “Notepad” window with the “Wrap” class.
- Creating a mutex “{A931568B-94AF-449D-B7F6-6585EF9E9839}”.
- Creating a mutex “QuitMutex%d”, where %d is the PID of the currently running process (downloader). It is used to prevent the payload file from re-downloading and running.
- Checking the local time and comparing it with the value in param_4. If the value of the array of param_4 by the index of the product of the hour and the day of the week (which are taken from the local time on the victim’s computer) is not equal to 1, then the main functionality is not executed.
- Downloading a payload from hXXtps://upportteam[.]lingrevelat[.]com/update/v32/default, which is a malicious dynamic-link library (DLL) with the “HttpsVictimMain” exported function. DLL is encrypted with RC4 and XOR algorithms. The XOR algorithm decrypts data at offset 0x104 (260) bytes, which are pre-decrypted by RC4.

Network request example:

```
GET /update/v32/default HTTP/1.1
Cache-Control: no-cache
```

```
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Host: upportteam[.]lingrevelat[.]com
```

Possibly using system proxy settings or settings specified in configuration data.

Decrypting downloaded data from a URL and checking if it is a PE32 file.

Loading the next stage payload (the downloaded malicious DLL) to memory and calling the “HttpsVictimMain” exported function. The function is also used to transfer the following parameters: domain name, network port, RC4 key (is contained in the downloaded DLL), number of hours of days of the week, unknown parameter with the value “https-note-86” (maybe its BotID or CampaignID), proxy server, proxy network port, proxy user, proxy password.

Advanced Persistent Threats – Conclusion

Group-IB experts have previously warned about **threats from TaskMasters and TA428**, **other Chinese nation-state cyber threat actors.** Based on the conducted analysis, the company’s Threat Intelligence team concluded that Tonto Team is behind the 2021-2022 attempted attacks on Group-IB.

The main goal of Chinese APTs are espionage and intellectual property theft. Undoubtedly, **Tonto Team will keep probing IT and cybersecurity companies** by leveraging spear phishing to deliver

malicious documents using vulnerabilities with decoys specially prepared for this purpose.

Successful supply chain attacks against IT and cybersecurity companies give attackers access to a large number of victims' customers and partners. Therefore, organizations in these sectors need to stay up to date with ever-evolving tools, tactics, and methods of threat actors and employ Group-IB Managed XDR for advanced threat detection and response. **This solution proved its efficiency in preventing the alleged Tonto Team attack on the Group-IB's employees.**

Group-IB **Managed XDR** contains a whole range of advanced cybersecurity solutions to stop complex targeted attacks:

- Endpoint Detection & Response (EDR)
- Network Traffic Analysis (NTA)
- Malware Detonation Platform (MDP)
- Business Email Protection (BEP)
- Threat Intelligence (TI)
- Managed Services (MS)

Learn more about the solution in our blog post.

Group-IB will continue to research **the methods, tools and tactics of Tonto Team** and inform the organizations targeted by this pro-state group. We aspire to promptly inform the attacked organizations about the discovered malicious activity against them – it helps minimize the damage from threat actor's actions. Additionally, **we consider informing the cybersecurity community about the discovered threats as a part of our mission** and encourage other researchers to study complex threats together, share data and use our technologies to combat intruders.

IoCs

Hash

Network indicators

User-Agent

Mutexes

MITRE ATT&CK®

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

YARA rules

```
import "pe"

rule apt_tontoteam__bisonal_doublet
{
    meta:
```

```
        author = "Dmitry Kupin"
        company = "Group-IB"
        description = "Detects Bisonal.DoubleT samples"
        date = "2022-06-20"
        hash = "58c1cab2a56ae9713b057626953f8967c3bacbf2cda68ce104bbb4ece4e35650"

    strings:
        $s0 = "ABCDEFGHIJKLMNOPQRSTUVWXYZ234567=" fullword ascii
        $s1 = "{\"status\":\"success\"}" fullword ascii
        $s2 = "GetNativeSystemInfo" fullword ascii
        $s3 = "::Off" fullword ascii
        $s4 = "::On" fullword ascii

    condition:
        all of ( $s* ) or pe.imphash ( ) == "2edcf20dae8aede04f118ccf201f5bd2" or pe.imph
}

rule apt_tontoteam__downloader
{
    meta:
        author = "Dmitry Kupin"
        company = "Group-IB"
        description = "Detects TontoTeam.Downloader samples"
        date = "2022-06-17"
        hash = "c357faf78d6fb1460bfcd2741d1e99a9f19cf6dffd6c09bda84a2f0928015398"

    strings:
        $config_parse_str = "%[^!]!%[^$]$%[^$]$%[^$]$%[^$]$%[^$]$%[^$]$%[^$]$%[^$]$%[^$]$%[^$]$
        $s_file_description = "Wrap Module" fullword wide
        $s_mutex = "QuitMutex%d" fullword wide
        $s_window_name = "Notepad" fullword wide
        $s_window_class_name = "Wrap" fullword wide
        $rc4_key = { 38 05 87 0F 0C 6B 9F 2A 2B 1F F8 DA D2 6E 1E 42
                 8D 3D 07 5F 36 F9 91 21 FC 7D EB 8A 06 C7 66 3F
                 29 2F EF FB 78 B6 1B 7B 04 14 B2 30 98 D0 7F 8B
                 BF EC 47 FE 94 5D A6 CF 15 44 FF AB C9 57 46 81
                 93 69 82 58 08 03 B5 68 25 83 1D 0A 1A 9E D6 48
                 2E 09 EA C1 02 0D 51 F2 6C 0B 4D E8 A9 32 5B AE
                 B7 A7 C5 01 3A 8F 72 00 4E 76 DB 65 4A 23 70 BA
                 97 52 D7 D4 E2 8E 89 3B AC 9B 90 63 28 1C 39 A0
                 77 27 A5 0E EE D5 4C E7 41 B8 9A 17 B4 37 A4 F1
                 A3 55 C4 B9 CD CC 88 D1 CB 18 22 4F 2D 8C E5 9D
                 BB F5 35 60 FA 84 E0 73 13 C6 C2 79 B3 5E 71 26
                 D9 F7 3C 2C F3 45 7A 43 10 4B CE E6 86 16 ED AD
                 12 BC DE 85 AF 19 A8 C8 E3 E9 31 F0 61 5A 99 75
                 A2 E1 56 B0 D8 53 7C DD DF BE E4 80 C0 54 C3 74
                 7E 6D 20 49 64 67 B1 40 A1 95 D3 DC BD 24 9C FD
```

```
                    3E 6F 5C 62 34 F4 6A 50 CA 92 AA 96 33 11 F6 59 }
        $protocols = { 00 74 00 63 00 70 00 00 00 75 00 64 00 70 00 00
                       00 68 00 74 00 74 00 70 00 00 00 00 00 68 00 74
                       00 74 00 70 00 73 00 00 00 25 00 73 00 3A 00 25
                       00 64 00 }

    condition:
        $config_parse_str or $rc4_key or $protocols or all of ( $s_* ) or pe.imphash ( ) :
}
```