Tracking the Progression of Earth Hundun's Cyberespionage Campaign in 2024

By By: Pierre Lee, Cyris Tseng May 16, 2024 Read time: 10 min (2665 words)

Published: 2024-05-16 · Archived: 2026-04-05 13:13:55 UTC

Summary

- Earth Hundun is known for targeting the Asia-Pacific and now employs updated tactics for infection spread and communication.
- This report details how Waterbear and Deuterbear operate, including the stages of infection, command and control (C&C) interaction, and malware component behavior.
- Deuterbear, while similar to Waterbear in many ways, shows advancements in capabilities such as including support for shellcode plugins, avoiding handshakes for RAT operation, and using HTTPS for C&C communication.
- Comparing the two malware variants, Deuterbear uses a shellcode format, possesses anti-memory scanning, and shares a traffic key with its downloader unlike Waterbear.
- The evolution of Waterbear into Deuterbear indicates the development of tools for anti-analysis and detection evasion in Earth Hundun's toolbox.

Introduction

In our previous report, we introduced the sophisticated cyberespionage campaign orchestrated by Earth Hundun, a threat actor known for targeting the Asia-Pacific region using the Waterbear malware and its latest iteration, Deuterbear. We first observed Deuterbear being used by Earth Hundun in October 2022, and it has since been part of the group’s subsequent campaigns.

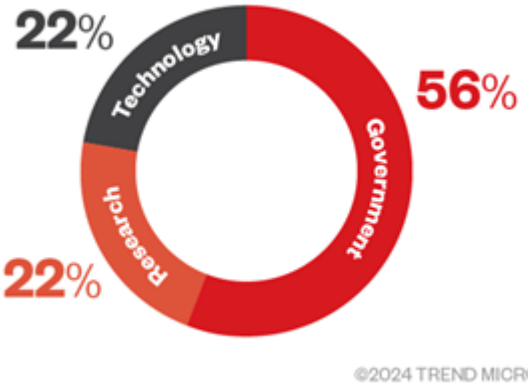

Figure 1. The industry distribution of endpoints infected by Waterbear and Deuterbear since 2022.

Our analysis provided insights into the intricate workings of the downloader, detailing its infection flow, traffic behavior, anti-analysis techniques, and evolutionary trajectory.

In this entry, we examine the behavior of the final Remote Access Trojan (RAT) that we recently managed to download from a C&C server, based on an Earth Hundun campaign from 2024.

In our first entry, we focused on the Waterbear downloader (the first stage) and examined its network behavior. This report uses a case study to describe how the threat actor uses the Waterbear RAT and plugin during the second stage and how Waterbear downloaders are spread to other machines, making it more difficult to detect and track.

Furthermore, we examine the major updates to Deuterbear, including the ability to accept plugins with shellcode formats and the ability to function even without handshakes during RAT operation.

Finally, we will share our findings about the interaction between Earth Hundun and its victims through the Waterbear and Deuterbear malware, showcasing the sophisticated tactics employed by this threat actor.

Waterbear case study

The following flow chart from a previous campaign illustrates how Waterbear operates in the victim's environment and then spreads more Waterbear downloaders across the internal network.

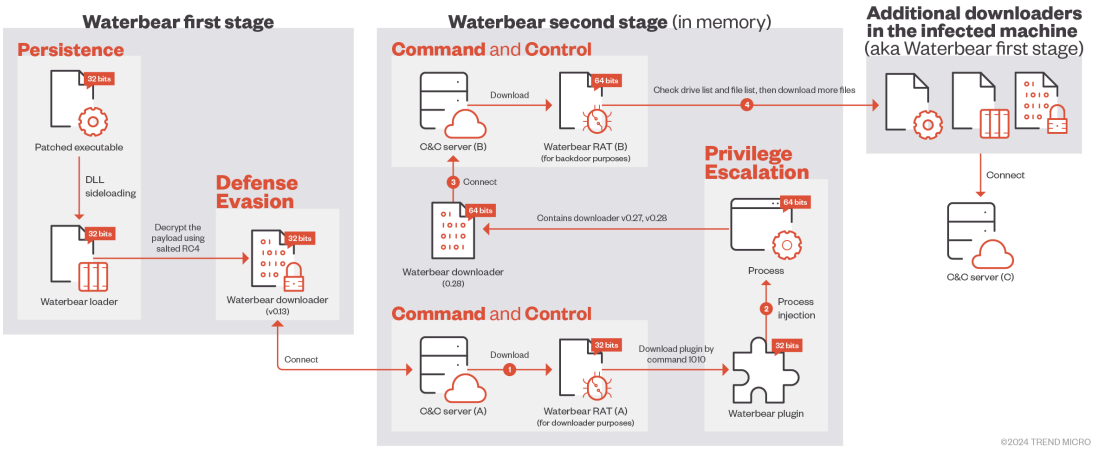

Figure 2. One of the Waterbear campaign attack chains

First stage

Waterbear usually employs a group of three files for downloading purposes during the first stage of an attack (as mentioned in the previous report). These include the patched legitimate executable, the loader, and the encrypted downloader.

Second stage

1. After connecting to the C&C server, we downloaded the Waterbear RAT (A) in memory, which contains several command codes inside (see Table 1 for the list of RAT commands). In this case, the Waterbear RAT

(A) was only used to download the Waterbear plugin via RAT command 1010 and activate the first export function, “Start”, in the plugin to inject the chosen process.

2. The Waterbear plugin contains Waterbear downloader versions 0.27 and 0.28, both unencrypted, varying based on the process's bit version. If the process is 32-bit, version 0.27 of the Waterbear downloader will run. On the other hand, version 0.28 will execute to facilitate further downloads on the 64-bit process.

   Waterbear downloader versions 0.27 and 0.28 are the latest that we know of. Their behaviors are the same as the versions before 2020.

3. In this case, the Waterbear plugin injects into a 64-bit process, which results in version 0.28 of the Waterbear downloader trying to connect to the new C&C IP address — which is assigned by Waterbear RAT (A) — and download Waterbear RAT (B), which is almost the same as the previous one, just with a different RSA key inside.
4. Waterbear RAT (B) will be used to collect the information from the infected machine, including the list of drives and files, and then further spread the Waterbear downloader to other machines. Interestingly, Earth Hundun will replace the C&C string with an internal IP address after downloading the new stage of the RAT or downloader. This is to erase activity traces or connect to other C&C servers in the victim's environment, showing that the threat actor can arbitrarily choose its connection targets.

Waterbear RAT command

Since discussing Waterbear’s functions in our previous blog entry, there have been more that have been implemented, with the latest version shown in the following table:

Command group	Command code (Hex)	Command code (Dec)	Capability
File management	2	2	Enumerate disk drives
	3	3	List files
	4	4	Upload file to C&C server
	5	5	Download file from C&C server
	6	6	Rename file
	7	7	Create folder
	8	8	Delete file
	A	10	Execute file
	B	11	Move file
	C	12	Disguise file metadata
	D	13	File operation

Other	326	806	Get system language, system time, and Windows installation date
Window management	327	807	Enumerate windows
	329	809	Hide window
	32A	810	Show window
	32B	811	Close window
	32C	812	Minimize window
	32D	813	Maximize window
	32F	815	Take a screenshot
	330	816	Set screenshot event signaled
	331	817	Remote desktop
Process management	332	818	Enumerate process
	333	819	Terminate process
	335	821	Suspend process with pID
	336	822	Resume process with pID
	337	823	Retrieve process module information
	338	824	Retrieve process module information (for files or objects using the authenticode policy provider)
Network management	339	825	Get extended TCP table
	33A	826	SetTcpEntry Set state of the TCP connection with MIB_TCP_STATE_DELETE_TCB
Service management	33B	827	Enumerate services
	33C	828	Manipulate service
	33D	829	
	33E	830	
	33F	831	
	340	832	

Configuration management	341	833	Get C&C in downloader configuration
	342	834	Set C&C in downloader configuration
Remote shell	3EE	1006	Start remote shell
management	3EF	1007	Exit remote shell
	3F0	1008	Get remote shell PID
	3F2	1010	Download plugin and execute the export function “Start”
Unknown	514	1300	Unknown
Registry management	7DB	2011	Enumerate registry
	7DC	2012	Enumerate registry value
	7DD	2013	Create registry key
	7DE	2014	Set registry value
	7DF	2015	Delete registry key
	7E0	2016	Delete registry value
Basic control	1F41	8001	Get current window
	1F44	8004	Set the infection mark in registry HKCU\Console\Quick\Edit
	1F45	8005	Terminate connection and RAT process
Proxy	2332	9010	Update C&C IP address
	2333	9011	Proxy data to the connected server
	2334	9012	Shutdown all connections
	2335	9013	Shutdown the given connection
	2336	9014	Listen port
	2337	9015	Proxy data via the specified socket handle
	2338	9016	Close the specified socket handle
	2339	9017	Shutdown both sending and receiving of a specific socket handle

	233A	9018	Proxy the data from the socket back to the C&C server

Table 1. List of Waterbear RAT commands

Before receiving the backdoor command, the RAT sends the victim's information to the C&C server via command code 8002:

Data offset	Data size	Data content
0x00	0x01	IsUserAnAdmin
0x01	0x9C	GetVersionExA
0x9D	0x10	gethostbyname
0xAD	0x44	gethostname
0xF1	0x18	GetUserNameA
0x109	0x04	GetLastInputInfo
0x10D	0x50	GetWindowTextA
0x15D	0x12	GetAdaptersInfo
0x16F	0x10	Downloader version
0x17F	0x30	Drive of information in current process
0x1AF	0x04	Infection mark in HKCU\Control Panel\Colors
0x1B3	0x04	GetCurrentProcessId
0x1B7	0x01	RAT version

Table 2. The structure of victim information that Waterbear sends to the C&C server

This section will explain Earth Hundun's use of Deuterbear and provide a comprehensive analysis of the Deuterbear RAT.

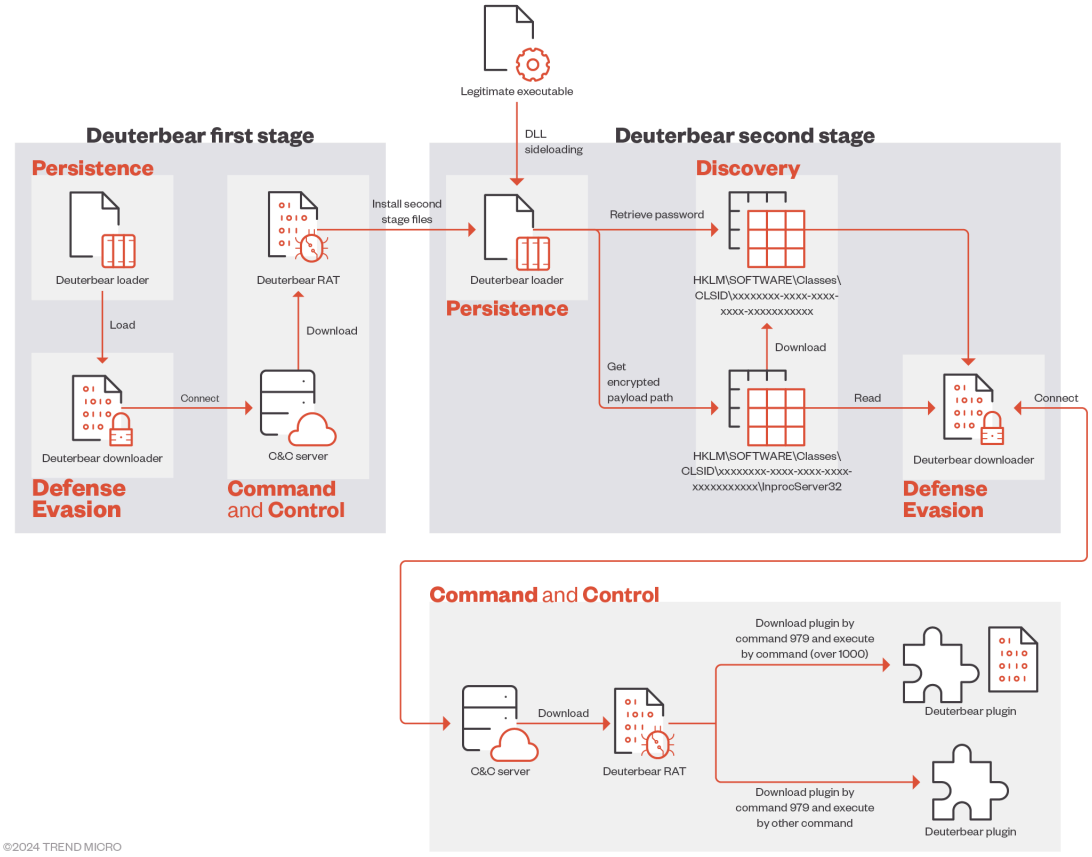

Figure 3. Installation pathway of Deuterbear

The installation pathway of Deuterbear is depicted in Figure 3. Note that it is similar to Waterbear, which implements two stages to install the backdoor.

In the first stage, the loader employs a basic XOR calculation to decrypt the downloader, facilitating the retrieval of the first stage RAT from the C&C server. Subsequently, the threat actor applies the first stage RAT to survey the victim's system and identify an appropriate folder for persistence. This is where the second-stage Deuterbear components will be installed, including the loader with CryptUnprotectData decryption, the encrypted downloader, and associated registries (the decryption flow was discussed in the previous blog entry).

In most of the infected systems, only the second stage Deuterbear is available. Our monitoring indicates that all components of the first stage Deuterbear are totally removed after the "persistence installation" is completed. It seems that Earth Hundun prefers to keep the loaders using CryptUnprotectData decryption, even in cases where the successful installation of Deuterbear is achieved during the first stage. This strategy effectively protects their tracks and prevents the malware from easily being analyzed by threat researchers, particularly in simulated environments rather than real victim systems.

Deuterbear RAT

The Deuterbear RAT directly inherits several components from the downloader, including:

- All anti-analysis techniques (please refer to our previous report for more details).
- HTTPS tunnel.

- Routine to receive and send traffic.
- RC4 key to decrypt and encrypt traffic.
- Routine to decrypt and encrypt the desired function.
- Key to decrypt and encrypt the desired function.

Due to having the same HTTPS channel and RC4 traffic key, Deuterbear RAT doesn't require a handshake with the C&C server to update communication protocols. This enables the threat actor to seamlessly control the client, regardless of whether the process is in the downloader or RAT status. Prior to executing backdoor commands, the Deuterbear RAT transmits victim information to the C&C server via RAT command 975 with the structure (Table 3) highly reminiscent of the Waterbear RAT (Table 2).

Data offset	Data size	Data content
0x00	0x04	Signature in configuration of downloader (00 00 01 00)
0x04	0x01	IsUserAnAdmin
0x05	0x20	GetUserNameA
0x25	0x80	OS version
0xA5	0x04	gethostbyname
0xA9	0x46	gethostname
0xEF	0x50	GetWindowTextA
0x13F	0x04	GetLastInputInfo
0x143	0x26	GetAdaptersInfo
0x169	0x04	GetCurrentProcessId
0x16D	0x01	RAT Version
0x16E	0x04	Infection mark in HKCU\Control Panel\Colors
0x172	0x08	Last write time of temp folder in system folder

Table 3. The structure of victim information that Deuterbear sends to the C&C server

Deuterbear RAT command

Comparing Deuterbear with Waterbear reveals several functionalities directly replicated from the Waterbear RAT, such as process management, file management, and remote shell capabilities.

Although Deuterbear streamlines its capabilities, retaining only 20 RAT commands (Table 4) compared to over 60 for Waterbear (Table 1), the Deuterbear RAT accepts more plugins to enhance flexibility and accommodate additional functionalities, including two shellcodes and a portable executable (PE) DLL via RAT command 979.

After installing the plugins, the threat actor sends the next traffic to determine which plugin is launched. There are three kinds of protocols:

- Execute the first shellcode and the first export function of PE(DLL)
- Execute the second shellcode and the first export function of PE(DLL)
- Only execute the first export function of PE(DLL)

Command group	**Command code (Hex)**	**Command code (Dec)**	**Capability**
File management	0x27	39	List files (date, size, name)
	0x28	40	Upload file to C&C server
	0x29	41	Download file from C&C server
	0x2A	42	Rename file
	0x2C	44	SHFileOperationA
	0x2E	46	Execute File
Process management	0xE7	231	Enumerate process
	0xE8	232	Terminate targeted process
Configuration management	0x1FF	511	Collect data in the downloader configuration >C&C string >Execution time
	0x200	512	Update data in the downloader configuration >C&C string >Execution time
Remote shell management	0x2FC	764	Start remote shell
	0x2FD	765	Exit remote shell
	0x2FE	766	Get PID of remote shell
Basic control	0x3CE	974	Get current window
	0x3D1	977	Set infection mark in HKCU\Control Panel\Colors
	0x3D2	978	Terminate connection and RAT process

Plugins management	0x3D3	979	Download plugins from C&C server: >PE (DLL) >First Shellcode (Encrypted by key fromconfig of downloader) >Second shellcode(Encrypted by key from config of downloader)
	0x3D4	980	Uninstall plugins
	0x3E8~0x578	1000~1400	Execute plugins >First shellcode >First export function of PE (DLL)
	> 0x578	> 1400	Execute plugins >Second shellcode >First export function of PE (DLL)
	Other	Other	Execute plugins >First export function of PE (DLL)

Table 4. List of Deuterbear RAT commands

Examples of similarities in backdoor commands between Waterbear and Deuterbear are shown in the images from Figure 4 to Figure 6.

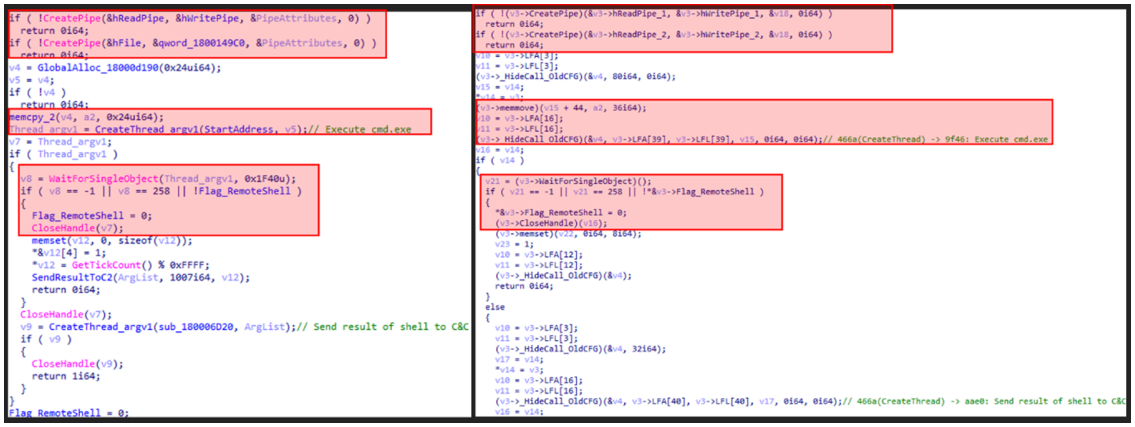

Figure 4. The function that starts remote shell in Waterbear RAT (left) and Deuterbear RAT (right)

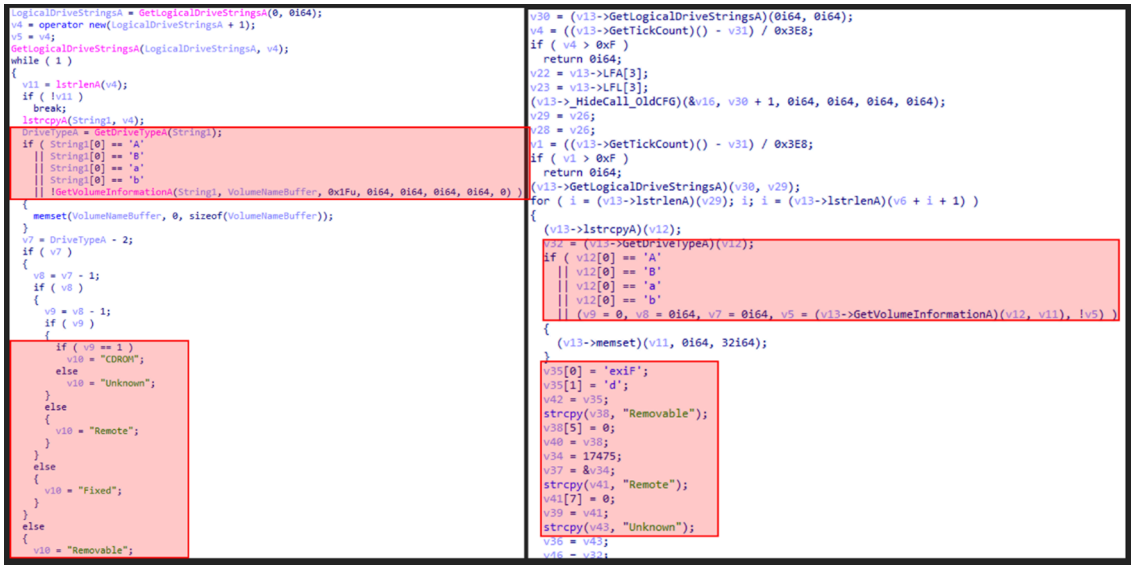

Figure 5. The function that enumerates disk drives in Waterbear RAT (left) and Deuterbear RAT (right)

Figure 6. The function that lists files in Waterbear RAT (left) and Deuterbear RAT (right)

Comparison

Comparing the Waterbear and Deuterbear downloaders, Table 5 shows the differences in the RAT part:

Properties	**Waterbear RAT**	**Deuterbear RAT**
Format	PE file	Shellcode
Anti-Memory scanning	No	Yes
C&C communication	HTTP	HTTPS
Size of packet header	10	5
Share the same traffic key with downloader	No	Yes

Format of Plugin	PE file	PE file and shellcode
Registry of infection mark	HKCU\Console\Quick\Edit	HKCU\Control Panel\Colors
Counts of backdoor command	60+	20
Functionality of backdoor command	File management Process management Configuration management Remote Shell management Windows management Registry management Service management Network management Proxy	File management Process management Configuration management Remote Shell management Plugins management

Table 5. Differences between the Waterbear RAT and Deuterbear RAT

Conclusion and recommendations

Waterbear has gone through continuous evolution, eventually giving rise to the emergence of a new malware, Deuterbear. Interestingly, both Waterbear and Deuterbear continue to evolve independently, rather than one simply replacing the other.

Based on the downloader analysis presented in April 2024. We made a comprehensive examination of the RAT, which is a component seldom downloaded from the C&C server due to temporary port openings. Through a systematic comparison of Deuterbear and Waterbear in the loader, downloader, RAT and behavioral aspects, we gained insights into the evolution of the techniques employed by Earth Hundun. While the Waterbear and Deuterbear family represent just one facet of the group's arsenal, we believe that continuous refinement of tools will be implemented in other malware for anti-analysis, and detection evasion, particularly in traffic and file handling.

Organizations can defend themselves from Earth Hundun attacks by performing a memory scan for downloads and the Waterbear and Deuterbear RATs. Furthermore, detecting the registry used to **decrypt** the Deuterbear downloader can help scan for its presence within the system.

MITRE ATT&CK

Tactic	**Technique**	**ID**	**Description**
Execution	Shared Modules	T1129	Dynamically loads the DLLs through the shellcode
	Native API	T1106	Dynamically loads the APIs through the shellcode

Persistence	Hijack Execution Flow: DLL Side-Loading	T1574.002	Uses modified legitimate executable to load the malicious DLL
	Boot or Logon Autostart Execution: Print Processors	T1547.012	Deuterbear abuses print processors to run malicious DLLs during system
Privilege Escalation	Process Injection	T1055	Waterbear and Deuterbear inject the targeted process
Defense Evasion	Deobfuscate/Decode Files or Information	T1140	Uses RC4 or CryptUnprotectData to decrypt encrypted downloader
	Execution Guardrails	T1480	Targets specific path/registry in the victim's environment
	Virtualization/Sandbox Evasion: Time Based Evasion	T1497.003	Deuterbear checks sandbox by API, Sleep, whether normal operation.
	Debugger Evasion	T1622	Deuterbear checks debugger mode by process time.
Discovery	File and Directory Discovery	T1083	Waterbear and Deuterbear RAT searches files and directories or in specific locations.
	System Network Configuration Discovery: Internet Connection Discovery	T1016.001	Downloaders check for internet connectivity on compromised systems.
	System Network Connections Discovery	T1049	Waterbear and Deuterbear RAT lists network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.
	Process Discovery	T1057	Waterbear and Deuterbear RAT searches specific process.
	System Information Discovery	T1082	Waterbear and Deuterbear RAT get detailed information about the operating system and hardware, including version, username, and architecture.
	Query Registry	T1012	Queries data from registry to decrypt downloader

Lateral Movement	Remote Services: Windows Remote Management	T1021.006	Waterbear and Deuterbear RAT control remote shell
Collection	Data from Local System	T1005	Collects basic information of victim
Exfiltration	Exfiltration Over Command-and-Control Channel	T1041	Sends collected data to C&C
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	Downloaders communicate with C&C by HTTP/HTTPS
	Encrypted Channel	T1573	Employs a RC4/RSA to conceal command and control traffic
	Data Encoding: Non-Standard Encoding	T1132.002	Encodes traffic with a non-standard RC4 to make the content of traffic more difficult to detect

Indicators of Compromise

The indicators of compromise for this entry can be found on this link.

Tags
