Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

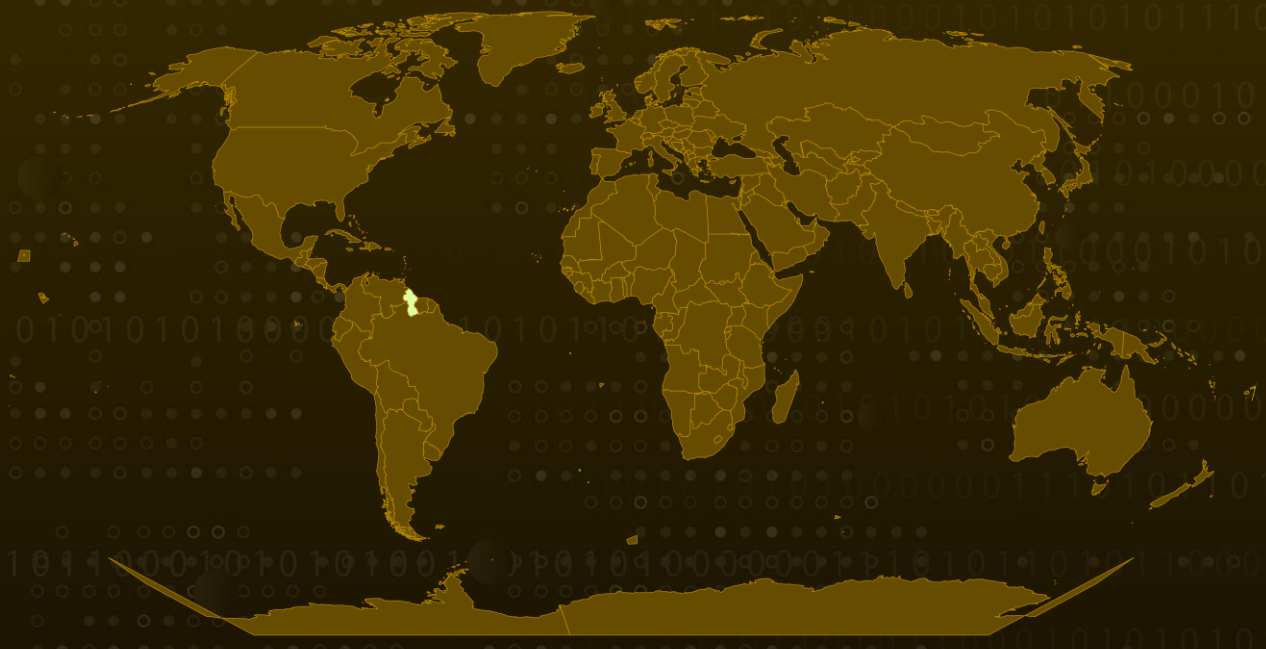
Unveiling Operation Jacana: Targeting the Guyana Government with DinodasRAT

Date of Publication	Admiralty Code	TA Number
October 6, 2023	A1	TA2023400

Summary

First appeared: February 2023
Malware: DinodasRAT
Attack Region: Guyana
Targeted Industry: Government
Affected Platform: Windows
Attack: A cyber espionage campaign named Operation Jacana was identified in February 2023, targeting a government entity in Guyana. This campaign began with a spear-phishing attack and resulted in the deployment of a C++-based implant called DinodasRAT.

Attack Regions



Attack Details

#1 A new malware threat known as "DinodasRAT" has emerged, following its use in a targeted cyber-espionage operation named Operation Jacana against a governmental organization in Guyana.

#2 The Operation Jacana campaign initiated with highly targeted spear-phishing emails that alluded to recent developments in Guyanese public and political matters. Following the initial compromise achieved through these spear-phishing emails, the attackers then proceeded to conduct lateral movement within the victim's internal network.

#3 To extract sensitive data, the threat actors leveraged a previously unreported backdoor known as DinodasRAT. In these spear-phishing emails, recipients were directed to click on a link, which, when accessed, triggered the download of a ZIP file from a compromised Vietnamese government website. This ZIP file contained malware samples. When the victim opened the ZIP file, their system became infected with the DinodasRAT malware.

#4 DinodasRAT employs the Tiny Encryption Algorithm (TEA) to encrypt the data it transmits to the command-and-control (C2) server. Additionally, DinodasRAT possesses a range of functionalities, including the ability to exfiltrate system metadata, files, manipulate Windows registry keys, and execute commands.

#5 In addition to DinodasRAT, the attackers employed other tools during the intrusion, including Korplug and the SoftEther VPN client. These additional tools have raised suspicions that the operation may be connected to China-aligned threat operators.

Recommendations

Email Security: Implement robust email filtering to counteract spam, phishing, and malicious attachments, and exercise caution with unverified links and email attachments by validating their authenticity before opening.

Endpoint Security: Implement robust endpoint security solutions that encompass antivirus and anti-malware software. Keep these security tools up-to-date to ensure comprehensive defense against emerging threats.

Network Segmentation: Implement proper network segmentation to limit the lateral movement of malware within the network. By dividing the network into smaller, isolated segments, organizations and can prevent it from accessing critical systems and sensitive data.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0003 Persistence	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1583 Acquire Infrastructure	T1583.003 Virtual Private Server
T1587 Develop Capabilities	T1587.001 Malware	T1608 Stage Capabilities	T1608.001 Upload Malware
T1584 Compromise Infrastructure	T1584.004 Server	T1588 Obtain Capabilities	T1588.001 Malware
T1588.002 Tool	T1566 Phishing	T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter

T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059.005 Visual Basic	T1106 Native API
T1204 User Execution	T1204.001 Malicious Link	T1204.002 Malicious File	T1140 Deobfuscate/Decode Files or Information
T1036 Masquerading	T1036.007 Double File Extension	T1070 Indicator Removal	T1070.004 File Deletion
T1564 Hide Artifacts	T1564.001 Hidden Files and Directories	T1078 Valid Accounts	T1078.002 Domain Accounts
T1053 Scheduled Task/Job	T1003 OS Credential Dumping	T1003.003 NTDS	T1083 File and Directory Discovery
T1012 Query Registry	T1057 Process Discovery	T1007 System Service Discovery	T1082 System Information Discovery
T1115 Clipboard Data	T1113 Screen Capture	T1573 Encrypted Channel	T1573.001 Symmetric Cryptography
T1095 Non-Application Layer Protocol	T1132 Data Encoding	T1041 Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	599EA9B26581EBC7B4BDFC02E6C792B6588B751E, 8BDC8FA3E398733F50F8572D04172CD4B9765BBC, 9C660AC9E32AD853CAAA995F5FC112E281D8520A, 6022383243927CAFC74D8DC937423DBED2A170B8, B2B86DDA48A109EDD932B460649F60F505D5D71C, EFD1387BB272FFE75EC9BF5C1DD614356B6D40B5, 9343E9716933382DA172124803F5463A8454E347,

TYPE	VALUE
SHA1	C92DAC928D70EDED7D52CB1347850AA422CEA817, FFBA119D86688AFC098109E08811F67A6E5DECDA, 9A6E803A28D27462D2DF47B52E34120FB2CF814B, 33065850B30A7C797A9F1E5B219388C6991674DB, 6129E37412AFEAFEE47ECEB4C52094EE185E6768, 010451191D8556DCF65C7187BE9579E99323F74D
IPv4	23.106.122[.]5, 23.106.122[.]46, 23.106.123[.]166, 42.119.111[.]97, 115.126.98[.]204, 118.99.6[.]202, 199.231.211[.]19
Filenames	President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.doc.exe, client.exe, tools.exe, Client.exe, windowsupdate.exe, people.zip, lass.exe, 2.dll, 1.dll, President Mohamed Irfaan Ali's Official Visit to Nassau, The Bahamas.exe, 114.exe, hh.hsnx, COTED_Att. I to Sav. 230 (Draft Agenda).docx.exe
Domains	`fta.moit.gov[.]vn, update.microsoft-settings[.]com

References

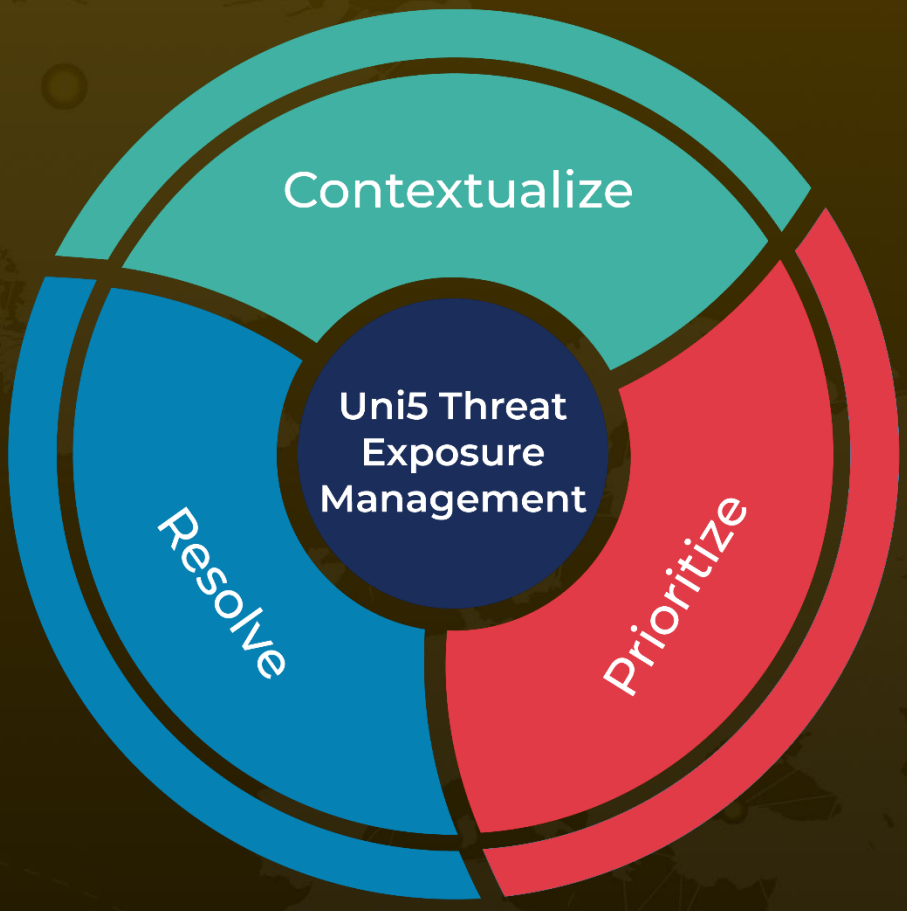
https://www.welivesecurity.com/en/eset-research/operation-jacana-spying-guyana-entity/

https://github.com/eset/malware-ioc/tree/master/operation_jacana

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 6, 2023 • 3:30 AM

More at www.hivepro.com