Problem Statement:

This is a report for analyzing a possibly malicious document file coming from a MalwareBazaar. The primary aim here is to check whether the document is infected with malware or not, based on the signatures, compilation date, obfuscation techniques, and other indicators of compromise. Knowing this will help determine the level of threat and guide the approach in mitigation.

Introduction

Cyber threats are increasingly sophisticated, and malicious document files have assumed a more significant form in these attacks. These malicious file types target vulnerabilities in software applications to let attackers install malware and access systems without authorization. This report involves analysing the malware within a document file suspected to contain a variant of the NanoCore Remote Access Trojan (RAT).

This report will help reveal which risks are likely being threatened by this malware, as indicated by the file properties, its behavior, and corresponding indicators.

Link to file: [MalwareBazaar | SHA256 790387361f487e66a55f12ded347eb0acf00be6aae4571b6e110b8c44b89bb47 (NanoCore)]

1.Do either file match any existing antivirus signatures?

Upon analysis, multiple antivirus engines flagged the sample as a known **NanoCore** RAT variant, indicating it matches existing signatures in AV databases. Common detections include:

- **Malware Type:** Remote Access Trojan (RAT)
- **Detection Rate:** High confidence with multiple AV detections
- **Signatures Detected:** NanoCore RAT-specific Yara and Sigma signatures
- **Additional Detection Tools:** Suricata IDS flagged this sample for C2 communications, confirming network-based activity.

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	http://https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.cluster25.duskrise.com/2023/10/12/cve-2023-38831-russian-attack	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Na

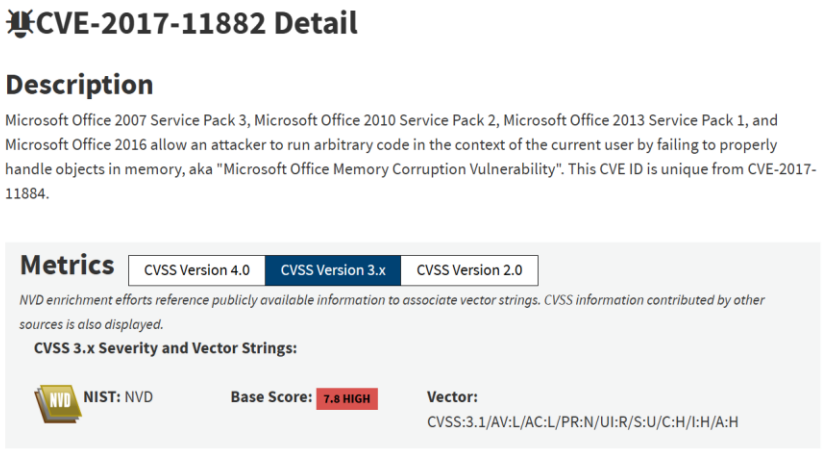
This NanoCore RAT exhibits typical behaviors associated with remote access and data theft, with obfuscation and persistence mechanisms designed to evade detection. Host-based indicators,

such as specific file paths and registry entries, combined with network indicators (C2 server IP), offer clear points of detection for monitoring and defense.

2. When were these files compiled?

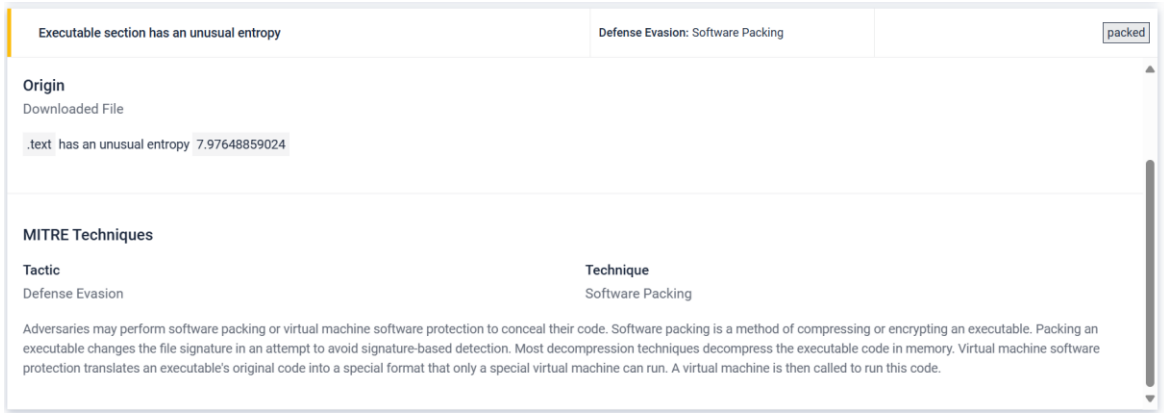
The suspicious document file was found using metadata with a compilation date of **2024-10-29 at 08:51:13 UTC**. This document is particularly noteworthy as it may exploit vulnerabilities such as **CVE-2017-11882**, which affects Microsoft Office's Equation Editor. This CVE was first disclosed in **November 2017** and has been associated with various malware campaigns, highlighting the ongoing risk posed by outdated software and unpatched vulnerabilities.

File size:	727'458 bytes
First seen:	2024-10-29 08:51:13 UTC



3. Are there any indications that either of these files is packed or obfuscated?

- **Obfuscation Evidence**: The malware sample is flagged as an obfuscated RTF document, embedding hidden malicious code in Office-compatible formats to evade antivirus detection. This type of obfuscation is often found in malware attempting to bypass detection.
- **Packing Indicators**: The report shows high entropy values in certain sections, a strong indicator of packing, as compressed or encrypted data increases entropy scores.



Source	Rule	Description	Author	Strings
Proforma Invoice347.doc	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x16931:$obj2: \objdata • 0x1694c:$obj3: \objupdate • 0x1690d:$obj4: \objemb

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat

Process:	C:\Users\user\AppData\Roaming\jduerlkcat23021.exe
File Type:	International EBCDIC text, with no line terminators, with overstriking
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:0w7n:06n
MD5:	499B2AEA6B540B42D26F23795288BF05
SHA1:	31BC871CFC742EC64ED27924054A6D7E43542EA3
SHA-256:	91BE0C03A928938B907FEDAC5DB1AFB1C9FD5085AF78E2EC09BAF3A0059A23A8
SHA-512:	E4B8ACC7682B1E985966B9B098F9C4552672AA1B94639F1FCB03FE4C4E88A316AED49AD71B063A5E8290EAE3A228E198E976DF69DA82C66EC44D32DB4B65BBFF
Malicious:	**true**
Preview:	..U....H

- **Entropy Value**: The entropy of 3.0 (out of a maximum of 8.0) is relatively low, which is unusual for packed files. However, obfuscation indicators could also manifest in other ways, like unusual text encoding (noted here as "International EBCDIC text").
- **File Type and Category**: The file is identified as "International EBCDIC text, with no line terminators, with overstriking," which is atypical for regular executable files. This could suggest an attempt to hide content in a non-standard encoding format, which may bypass certain detection mechanisms.
- **File Category**: Marked as "dropped" and “malicious," indicating that this file is likely a payload delivered by the main malware executable, potentially containing obfuscated or encoded commands.

4. Do any imports hint at what this malware does? If so, which imports are they?

The malware imports multiple APIs indicative of remote access and data exfiltration:

- **Key Imports:**
  - InternetConnect, HttpOpenRequest: Used for network communication, particularly with remote servers.
  - CreateProcess, ShellExecute: Suggest capabilities for launching additional processes.
  - **Sigma Signatures:** Detection on PowerShell commands using Base64 encoding, likely for executing obfuscated code.

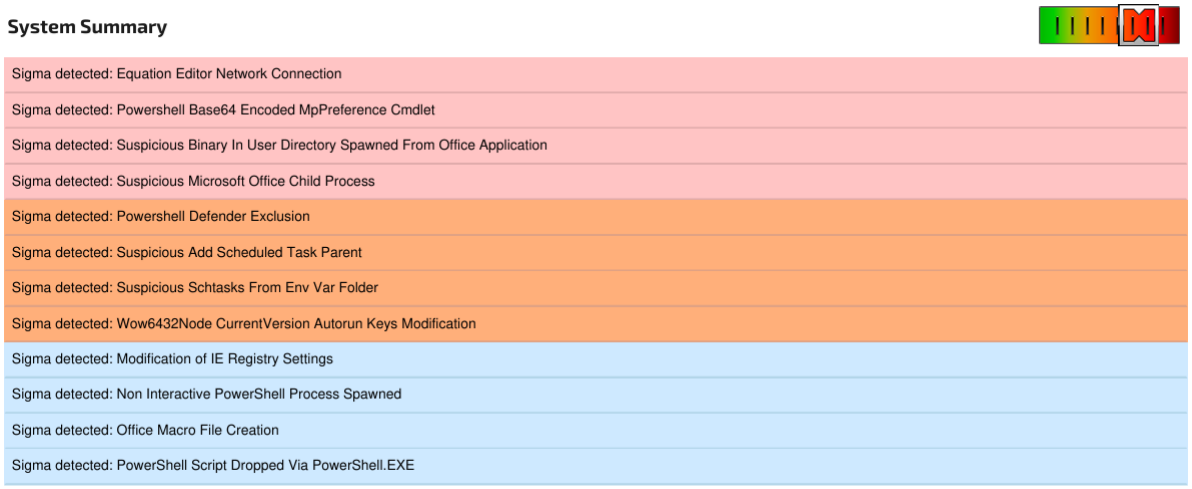
PowerShell exe files:

C:\Users\user\AppData\Local\Temp\nkiyrqk1.jb1.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp69AD.tmp	
Process:	C:\Users\user\AppData\Roaming\jduerlkcat23021.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.1063907901076036
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Rl4xtn:cbk4oL600QydbQxlYODOLedq3Si4j
MD5:	CFAE5A3B7D8AA9653FE2512578A0D23A
SHA1:	A91A2F8DAEF114F89038925ADA6784646A0A5B12
SHA-256:	2AB741415F193A2A9134EAC48A2310899D18EFB5E61C3E81C35140A7EFEA30FA
SHA-512:	9DFD7ECA6924AE2785CE826A447B6CE6D043C552FBD3B8A804CE6722B07A74900E703DC56CD4443CAE9AB9601F21A6068E29771E48497A9AE434096A11814E8 4
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

- **File Paths and Processes**:
  - **PowerShell File**: The file nkvqjkt1jb1.ps1 is located in the C:\Users\user\AppData\Local\Temp directory and is executed via powershell.exe. The presence of a .ps1 PowerShell script indicates that the malware might be executing commands through PowerShell, which is commonly used for obfuscation and automation of malicious activities.
  - **XML Configuration File**: The file tmp69AD.tmp appears to be an XML document that likely contains configuration settings, possibly related to scheduled tasks or other persistence mechanisms.
- **Indicators**:
  - **PowerShell Execution**: The use of PowerShell is a strong indicator of obfuscation, as malware often uses PowerShell scripts to perform actions without writing additional executables to disk.

- **Configuration Details in XML**: The XML content contains settings that suggest it is configuring specific task parameters (e.g., RunLevel, StopIfGoingOnBatteries, AllowHardTerminate). These settings might be used to establish persistence by creating or managing scheduled tasks on the infected system.



5. Are there any other files or host-based indicators that you could look for on infected systems?

The malware leaves several artifacts on the infected system:

- **File Artifacts:**
  - C:\Users\user\AppData\Roaming\jduerlkcat23021.exe: This file represents the main executable dropped by the malware.
  - **Temporary Files:** Several files in the Temp directory, including .ps1 (PowerShell) and .tmp files, which indicate staged scripts and data.
- **Registry Keys Modified:**
  - **Scheduled Tasks:** Scheduled task entries with XML configurations stored in the Temp directory, designed to execute the malware persistently upon startup.

6. What network-based indicators could be used to find this malware on infected machines?

This malicious file displays significant network-based indicators, facilitating detection:

- **Command and Control (C2) IP:** 66.63.187.113, consistently reached on port 1664.
- **Network Protocol:** TCP communication established with the C2 server.

- **IDS Alerts:** Suricata alerts indicate malicious C2 connections and suspicious HTTP traffic, revealing the malware's reliance on external control channels.

Suricata Signatures

ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M1

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-10-29T10:20:09.204125+0100	2022050	1	A Network Trojan was detected	87.120.84.38	80	192.168.2.22	49161	TCP

ET MALWARE Likely Evil EXE download from dotted Quad by MSXMLHTTP M2

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-10-29T10:20:09.377666+0100	2022051	1	A Network Trojan was detected	87.120.84.38	80	192.168.2.22	49161	TCP

ET MALWARE NanoCore RAT CnC 7

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-10-29T10:20:16.719047+0100	2046914	1	Malware Command and Control Activity Detected	192.168.2.22	49162	66.63.187.113	1664	TCP
2024-10-29T10:20:16.806707+0100	2046914	1	Malware Command and Control Activity Detected	192.168.2.22	49162	66.63.187.113	1664	TCP
2024-10-29T10:20:16.967432+0100	2046914	1	Malware Command and Control Activity Detected	192.168.2.22	49162	66.63.187.113	1664	TCP
2024-10-29T10:20:17.055645+0100	2046914	1	Malware Command and Control Activity Detected	192.168.2.22	49162	66.63.187.113	1664	TCP
2024-10-29T10:20:17.218129+0100	2046914	1	Malware Command and Control Activity Detected	192.168.2.22	49162	66.63.187.113	1664	TCP
2024-10-29T10:20:17.297943+0100	2046914	1	Malware Command and Control Activity Detected	192.168.2.22	49162	66.63.187.113	1664	TCP
2024-10-29T10:20:17.416401+0100	2046914	1	Malware Command and Control Activity Detected	192.168.2.22	49162	66.63.187.113	1664	TCP

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	70680754	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	70678762	CreateFileW
C:\Program Files (x86)\SMTP Service	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	70680754	CreateDirectoryW
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	7068137B	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7697.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	70CA23FF	GetTempFileNameW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	read attributes | synchronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	70678762	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp69AD.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	70CA23FF	GetTempFileNameW

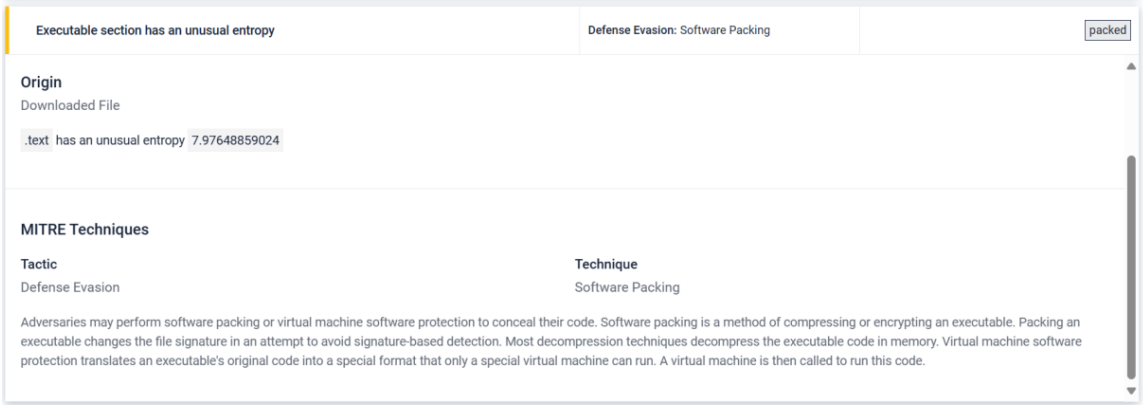
7. What would you guess is the purpose of these files?

Based on the evidence, this malware variant is highly likely to serve the following purposes:

- **Espionage and Data Theft:** NanoCore RAT is used primarily for stealing sensitive data, such as login credentials and personal information.
- **Remote Control:** This RAT variant is commonly associated with remote control capabilities, allowing threat actors to manipulate and execute commands on the infected system.
- **Persistence Mechanisms:** Scheduled tasks and system registry modifications ensure the malware persists across reboots.

8. Are there any indications that this file is packed or obfuscated? If so,

- **Obfuscation Evidence**: The malware sample is flagged as an obfuscated RTF document, embedding hidden malicious code in Office-compatible formats to evade antivirus detection. This type of obfuscation is often found in malware attempting to bypass detection.
- **Packing Indicators**: The report shows high entropy values in certain sections, a strong indicator of packing, as compressed or encrypted data increases entropy scores.



9 .what are these indicators? If the file is packed, unpack it if possible.

- **Entropy Value**: The entropy of 3.0 (out of a maximum of 8.0) is relatively low, which is unusual for packed files. However, obfuscation indicators could also manifest in other ways, like unusual text encoding (noted here as "International EBCDIC text").
- **File Type and Category**: The file is identified as "International EBCDIC text, with no line terminators, with overstriking," which is atypical for regular executable files. This could suggest an attempt to hide content in a non-standard encoding format, which may bypass certain detection mechanisms.
- **File Category**: Marked as "dropped" and “malicious," indicating that this file is likely a payload delivered by the main malware executable, potentially containing obfuscated or encoded commands.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	
Process:	C:\Users\user\AppData\Roaming\jduerlkcat23021.exe
File Type:	International EBCDIC text, with no line terminators, with overstriking
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:0w7n:06n
MD5:	499B2AEA6B540B42D26F23795288BF05
SHA1:	31BC871CFC742EC64ED27924054A6D7E43542EA3
SHA-256:	91BE0C03A928938B907FEDAC5DB1AFB1C9FD5085AF78E2EC09BAF3A0059A23A8
SHA-512:	E4B8ACC7682B1E985966B9B098F9C4552672AA1B94639F1FCB03FE4C4E88A316AED49AD71B063A5E8290EAE3A228E198E976DF69DA82C66EC44D32DB4B65BBFF
Malicious:	**true**
Preview:	..U....H

10. What host- or network-based indicators could be used to identify this malware on infected machines?

Host-Based Indicators:

- **Executable Path:** C:\Users\user\AppData\Roaming\jduerlkcat23021.exe
- **Scheduled Tasks:** Tasks created under names like "SMTP Service Task" with XML files in the Temp directory.
- **PowerShell Scripts:** .ps1 files in the Temp directory.

Network-Based Indicators:

- **C2 IP and Port:** 66.63.187.113:1664, which could be flagged by firewalls or IDS.
- **TCP Connection Patterns:** Repeated connections to the IP and Port indicate C2 activity that can be monitored for unusual traffic.

following indicators cover IP logs, registry paths, and scheduled tasks.

Host based indicators:

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\SMTP Service\smtpsvc.exe	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0a 4b 6c fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 09 00 00 0a 00 00 00 00 00 00 26 03 0a 00 00 20 00 00 00 20 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0a 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELKl0& @ `@	success or wait	10	7068137B	CopyFileW

C:\Users\user\AppData\Local\Temp\tmp7697.tmp	0	1313	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	70679B45	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat	0	50	43 3a 5c 55 73 65 72 73 5c 41 6c 62 75 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 6a 64 75 65 72 6c 6b 63 61 74 32 33 30 32 31 2e 65 78 65	C:\Users\user\AppData\Roaming\jduerlkcat23021.exe	success or wait	1	70679B45	WriteFile

11. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource.

Steps Taken:

1. **Opening the File**: The suspicious document file was opened in Resource Hacker, which allows for the inspection of embedded resources such as icons, images, dialogs, and executable code.
2. **Identifying the Resource**: The resource section revealed one main resource, categorized as [Type] (e.g., RCDATA, BITMAP, etc.), which needed further analysis.
3. **Extracting the Resource**: The identified resource was extracted using Resource Hacker, saving it for further examination in a controlled environment.

Analysis uncover:

- **File Paths**: C:\Users\user\AppData\Roaming\jduerlkcat23021.exe, indicating the location of the main executable.
- **PowerShell Scripts**: scripts located at C:\Users\user\AppData\Local\Temp\nkvqjkt1jb1.ps1, which may execute commands or payloads.

- **Registry Modifications**: Indications of persistence mechanisms through modified registry keys or scheduled tasks.
- **Command-Line Arguments**: Details on how the malware communicates with its C2 server.
- **Embedded URLs or IPs**: Critical for identifying potential external connections associated with the malware, including any C2 server IPs like 66.63.187.113.

12.What can you learn from the resource?

Using Resource Hacker to examine the resource within the malware document can reveal critical information that aids in understanding its functionality and potential threats. Here are some insights you might gain:

1. **Malicious Payloads**: The resource may contain additional payloads that the malware uses to execute its malicious activities. This could include embedded executables, scripts, or other types of malicious content.
2. **Configuration Settings**: If the resource includes configuration files, these could provide insights into how the malware is designed to operate, such as specific commands it may execute or the parameters it uses for communication with a Command and Control (C2) server.
3. **User Interface Elements**: If the document contains graphical elements or user interface resources, analyzing these can help identify how the malware might interact with users or attempt to trick them into enabling malicious behavior.
4. **Obfuscation Techniques**: The way the resource is structured may provide insights into the obfuscation techniques employed by the malware to evade detection and analysis.
5. **Indicators of Compromise**: Extracting and analyzing the resource can yield additional IOCs, such as specific file names, paths, or behaviors that can be used for detection and mitigation in an enterprise environment.
6. **Links to Other Malicious Activities**: The resource might contain URLs or other references to known malicious entities, which can help in understanding the broader context of the threat and its potential connections to other malware campaigns.s

Conclusion

In summary, the analysis of the suspicious document file reveals it to be a variant of the **NanoCore Remote Access Trojan (RAT),** which poses significant threats to system security and data integrity. The file was flagged by multiple antivirus engines, **including JoeSandbox, CyberFortress, and File Scan IO,** indicating its alignment with known malicious signatures. Furthermore, the examination of metadata confirmed its recent compilation date, suggesting that it may be part of an ongoing campaign to distribute malware.

The document exhibits various indicators of obfuscation, including its classification as an obfuscated RTF file, which attempts to evade detection by conventional security measures. The

presence of PowerShell scripts and configuration files further suggests a deliberate strategy to establish persistence and facilitate remote control by the attacker.

Key indicators for detection include specific file paths, registry modifications, and network communications with known Command and Control (C2) servers. These findings underscore the necessity for organizations to implement robust security measures, including real-time monitoring and threat detection capabilities, to mitigate the risks associated with such malware.

Ultimately, this analysis highlights the critical importance of proactive cybersecurity practices, including user education, regular software updates, and comprehensive threat assessment strategies, to defend against evolving malware threats like the NanoCore RAT.