Executive Summary

- On May 27th 2022, @nao_sec identified a malicious Microsoft Word document using a "ms-msdt" protocol scheme for arbitrary code execution.
- As the industry continues to identify novel ways to abuse this ability over the weekend, Microsoft assigned it as CVE-2022-30190.
- Similar to what we observed with Log4j, the methods of execution and outcomes of this vulnerability continue to expand as it gains more researcher and attacker attention.
- Specific attackers have been observed exploiting the vulnerability. Chinese APTs have potentially made use of it around May 20th, 2022, but first samples identified as easily as mid-April 2022.
- Defenders should consider it a critical vulnerability and seek mitigation steps immediately. Additional effort should then be made to hunt for execution prior to public knowledge as attackers could have already abused it.

Background

Concerns are rising after Microsoft confirmed that its Microsoft Windows Support Diagnostic Tool (ms-msdt) contains a zero-click remote code execution vulnerability. The zero day appears to have been exploited in the wild since at least early April 2022, based on current reports.

The vulnerability, dubbed "Follina", makes use of how the ms-msdt handles URLs. In its simplest form, calling ms-msdt can allow attackers to execute code on a machine. The vulnerability impacts all Windows versions currently supported by Microsoft.

The call to ms-msdt with code execution is most commonly being reported on through the abuse of Microsoft , `.doc` and `.rtf` files. However, as we continue to gain new insight into the vulnerability, newer methods are coming to light. For example as Will Dormann observed, a WGET to an attacker domain can return HTML content with the call to ms-msdt to run code on the machine running the WGET.

Observed Threat Activity

Since we are in the very early stages of this vulnerability being publicly known, we expect to update this section as we continue our analysis and research. However, at the time of writing our colleagues from Malwarebytes identified the first public sample (f531a7c270d43656e34d578c8e71bc39) of a matching Word document on April 12th 2022. This sample is themed around the Russian invasion of Ukraine.

On May 27th 2022, @nao_sec tweeted about a file uploaded to VirusTotal from Belarus (52945af1def85b171870b31fa4782e52) that uses Word's external link to load HTML and then uses the "ms-msdt" scheme to execute PowerShell code. In this sample, the file beacons out to `xmlformats[.]com`, which at the time of discovery resolved to `141[.]105.65.149`. Note that the actor behind this particular sample began their infrastructure build around May 20th.

Subsequently, on May 30th 2022, a Chinese APT was observed by Proofpoint abusing the vulnerability through the C2 domain `tibet-gov.web[.]app`.

Mitigation Guidance

You can disable “Troubleshooting wizards” in one of two ways. Either through GPO:

HKLM\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnostics - EnableDiagnostics - 0

or in the user interface:

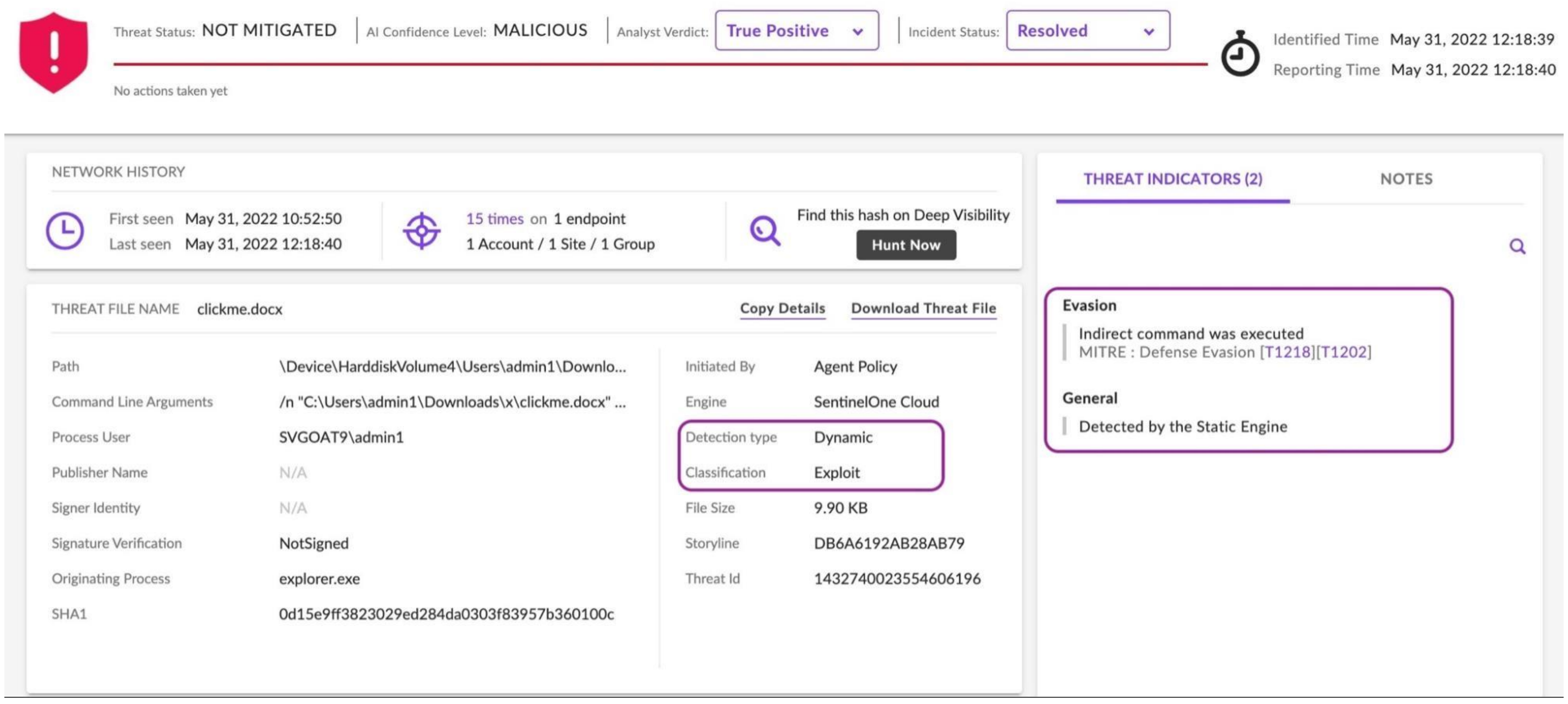
Group Policy Editor -> Computer Configuration -> Administrative Templates -> System -> Troubleshooting and Diagnostics -> Scripted Diagnostics. Set "Troubleshooting: Allow users to access and run Troubleshooting Wizards" to "disabled".

Microsoft has also recommended disabling the MSDT URL Protocol by executing the following command:

reg delete HKEY_CLASSES_ROOT\ms-msdt /f

SentinelOne vs CVE-2022-30190 (Follina)

The SentinelOne agent detects the execution of known “Fallina” samples exploiting CVE-2022-30190.



Threat Status: NOT MITIGATED | AI Confidence Level: MALICIOUS | Analyst Verdict: True Positive | Incident Status: Resolved

No actions taken yet

Identified Time May 31, 2022 12:18:39
Reporting Time May 31, 2022 12:18:40

NETWORK HISTORY

First seen May 31, 2022 10:52:50
Last seen May 31, 2022 12:18:40

15 times on 1 endpoint
1 Account / 1 Site / 1 Group

Find this hash on Deep Visibility

THREAT FILE NAME clickme.docx

Path	\Device\HarddiskVolume4\Users\admin1\Downlo...
Command Line Arguments	/n "C:\Users\admin1\Downloads\x\clickme.docx" ...
Process User	SVGOAT9\admin1
Publisher Name	N/A
Signer Identity	N/A
Signature Verification	NotSigned
Originating Process	explorer.exe
SHA1	0d15e9ff3823029ed284da0303f83957b360100c

Initiated By	Agent Policy
Engine	SentinelOne Cloud
Detection type	Dynamic
Classification	Exploit
File Size	9.90 KB
Storyline	DB6A6192AB28AB79
Threat Id	1432740023554606196

Evasion
Indirect command was executed
MITRE : Defense Evasion [T1218][T1202]

General
Detected by the Static Engine

SentinelOne customers can use the following STAR rule for real-time behavioral detection or as a hunting rule in Deep Visibility:

EndpointOS = "windows" AND EventType = "Process Creation" AND SrcProcName In Contains Anycase ("winword.exe","excel.exe","powerpnt.exe","outlook.exe") AND TgtProcName Contains Anycase "msdt.exe"

Additional Resources

- Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability
- SANS Internet Storm Center Analysis and Summary
- Summary and Analysis by researcher Kevin Beaumont
- Additional Research by Will Dormann