



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ

СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №6

Аналіз шкідливого програмного забезпечення

Перевірив:

Козленко О. В.

Виконав:

студент IV курсу

групи ФБ-01

Сахній Н. Р.

Київ 2024

Мета: Проведення детального аналізу шкідливого програмного забезпечення (ШПЗ), порівняння результатів загальнодоступного та спеціального аналізу.

Завдання: Проаналізувати приклад шкідливого програмного забезпечення у онлайн утилітах Cuckoo (<https://cuckoo.cert.ee/>) та зробити звіт.

- Дослідження зразків ШПЗ із репозиторію theZoo в Cuckoo Sandbox:

➤ Ransomware.WannaCry

The screenshot shows the Cuckoo Sandbox web interface. The top navigation bar includes 'Dashboard', 'Recent', 'Pending', and 'Search'. The left sidebar lists various analysis tools like 'Summary', 'Static Analysis', 'Extracted Artifacts', etc. The main content area is titled 'Summary' and displays details for an archive named 'Ransomware.WannaCry.zip'. It includes a 'Score' section indicating the sample is 'very suspicious' with a score of 10 out of 10. A 'Feedback' section is also present. Below the summary, a 'Yara' rule is shown, listing several rules that detect WannaCry ransomware, such as 'WannaDecryptor', 'WannaCry_Ransomware_Generic', and 'WannaCry_Ransomware_Dropper'.

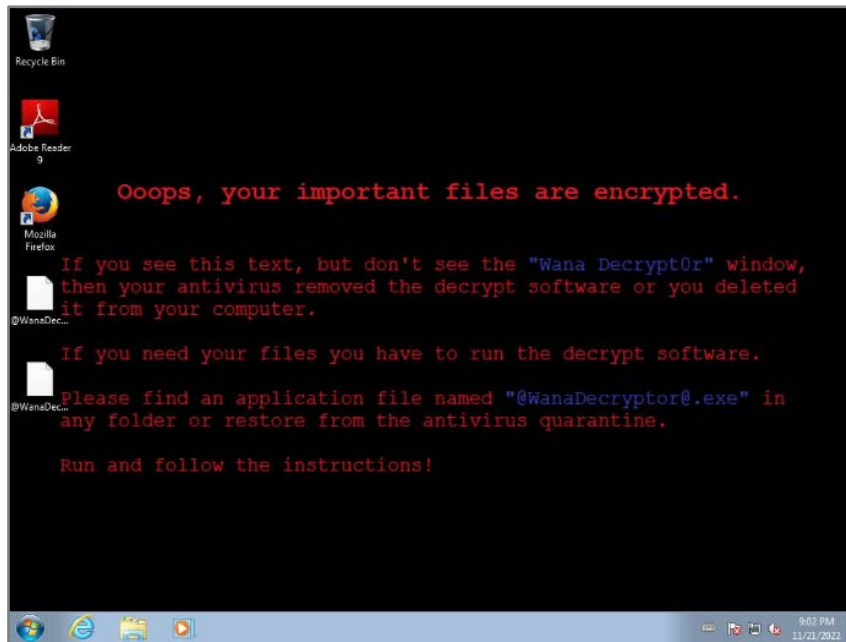
Field	Value
Size	3.4MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512	(Link to show SHA512)
CRC32	4022FCAA
ssdeep	None

Yara

- WannaDecryptor - Detection for common strings of WannaDecryptor
- Wanna_Sample_84c82835a5d21bbcf75a61706d8ab549 - Specific sample match for WannaCryptor
- ransom_telefonica - Ransomware Telefonica
- WannaCry_Ransomware_Generic - Detects WannaCry Ransomware on Disk and in Virtual Page
- WannaCry_Ransomware - Detects WannaCry Ransomware
- WannaCry_Ransomware_Dropper - WannaCry Ransomware Dropper
- wannacry_static_ransom - Detects WannaCryptor spreaded during 2017-May-12th campaign and variants
- WannaCry_Ransomware - Detects WannaCry Ransomware
- CrowdStrike_CSIT_17102_03 - WannaCry ransomware, encrypted file header
- Win32_Ransomware_WannaCry - Yara rule that detects WannaCry ransomware.

The screenshot shows the 'Analysis' page in the Cuckoo Sandbox interface. It displays a list of system events. The top section shows a summary of events, including 'Deletes a large number of files from the system indicative of ransomware, wiper malware or system destruction (50 out of 1250 events)' and 'Writes a potential ransom message to disk (1 event)'. Below this, a table lists individual events with columns for 'Time & API', 'Arguments', 'Status', 'Return', and 'Repeated'. One event is highlighted, showing a 'NtWriteFile' operation on March 2, 2024, at 3:24 p.m. The arguments for this event include a buffer containing a ransom message in English and a file path 'C:\Users\Administrator\AppData\Local\Temp\@Please_Read_Me.txt'. The status is '1', the return value is '0', and it was repeated '0' times.

Time & API	Arguments	Status	Return	Repeated
March 2, 2024, 3:24 p.m.	buffer: Q: What's wrong with my files? A: Oops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted. If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely! Let's start decrypting! Q: What do I do? A: First, you need to pay service fees for the decryption. Please send \$300 worth of bitcoin to this bitcoin address: 115p7UWngoj1phvKpHjcrdfJHXj6LrtN Next, please find an application file named "WannaDecryptor.exe". It is the decrypt software. Run and follow the instructions! (You may need to disable your antivirus for a while.) Q: How can I trust? A: Don't worry about decryption. We will decrypt your files surely because nobody will trust us if we cheat users. * If you need our assistance, send a message by clicking <Contact us> on the decryptor window. offset: 0 file_handle: 0x00000128 file_path: C:\Users\Administrator\AppData\Local\Temp\@Please_Read_Me.txt	1	0	0



➤ Ransomware.Rex

cuckoo

Dashboard Recent Pending Search

Submit Import

Summary

File WTEpZSFwgb[1]

Summary

Download Resubmit sample

Size	7.3MB
Type	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, Go BuildID=fc5a3d09dbaf04f6ec0587eae8c207fe211c5530, stripped
MD5	5bd44a35094fe6f7794d895122ddfa62
SHA1	98172e49c3d5d70ffdcfd071f9762c58430a393
SHA256	762a4f2bf5ea4ff72fce674da1adf29f0b9357be18de4cd992d79198c56bb514
SHA512	Show SHA512
CRC32	F0DD41CB
ssdeep	None

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Yara

- CrowdStrike_CSIT_18006_06 - Detects possible PHP-based webshells. The strings below are frequently used to obfuscate malicious webshell code.
- shellcode - Matched shellcode byte patterns
- network_smtp_raw - Communications smtp

Information on Execution

Category	Started	Completed	Duration	Routing	Logs
FILE	Nov. 21, 2022, 8:30 p.m.	Nov. 21, 2022, 8:32 p.m.	97 seconds	internet	Show Analyzer Log Show Cuckoo Log

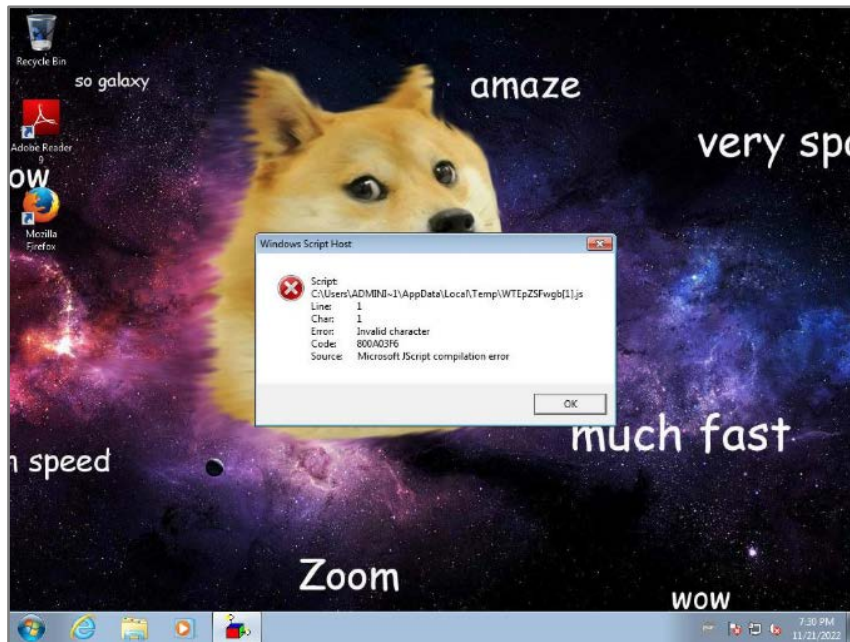
Signatures

Yara rules detected for file (3 events)

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)

File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)

File has been identified by 40 AntiVirus engines on VirusTotal as malicious (40 events)



➤ Win32.Triton

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import

Summary

Archive Win32.Triton @ Win32.Triton.zip

Summary		Download	Resubmit sample
Size	84.0KB		
Type	PE32 executable (GUI) Intel 80386, for MS Windows		
MD5	1904cad4927541e47d453becbd934bf0		
SHA1	aafa932eda97859e2b72772a3a8581760e860a46		
SHA256	70efbd074326e7bbd4e851ded5c362fe5fe06282ed4bbb4b9f761f1b12ee32f7		
SHA512	Show SHA512		
CRC32	135E4C7D		
ssdeep	None		
Yara	<ul style="list-style-type: none"> DebuggerCheck_QueryInfo - (no description) DebuggerHiding_Thread - (no description) anti_dbg - Checks if being debugged win_files_operation - Affect private profile 		

Score

This archive is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an *alpha* feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
ARCHIVE	Nov. 21, 2022, 9:18 p.m.	Nov. 21, 2022, 9:19 p.m.	25 seconds	internet	Show Analyzer Log Show Cuckoo Log

Signatures

- Yara rules detected for file (4 events) >
- File has been identified by 13 AntiVirus engine on IRMA as malicious (13 events) >
- File has been identified by 59 AntiVirus engines on VirusTotal as malicious (50 out of 59 events) >

Shamoon

cuckoo Dashboard Recent Pending Search Submit Import

Archive D214C717A357FE3A455610B197C390AA @ Shamoon.zip

Summary

Download Resubmit sample

Size	966.0KB
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	d214c717a357fe3a455610b197c390aa
SHA1	502920a97e01c2d022ac401601a311818f336542
SHA256	f9d94c5de86aa170384f1e2e71d95ec373536899cb7985633d3ecfdb67af0f72
SHA512	Show SHA512
CRC32	2468B2CC
ssdeep	None

Score

This archive is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Yara

- CrowdStrike_Shamoon_DroppedFile - Rule to detect Shamoon malware <http://goo.gl/QTxohN>
- CrowdStrike_Shamoon_DroppedFile - Rule to detect Shamoon malware <http://goo.gl/QTxohN>
- StoneDrill_ntssrvr32 - Detects malware from StoneDrill threat report
- anti_dbg - Checks if being debugged
- win_registry - Affect system registries
- win_files_operation - Affect private profile

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
ARCHIVE	Nov. 21, 2022, 9:41 p.m.	Nov. 21, 2022, 9:42 p.m.	83 seconds	internet	Show Analyzer Log Show Cuckoo Log

Signatures

Yara rules detected for file (6 events)



The file contains an unknown PE resource name possibly indicative of a packer (3 events)

The binary likely contains encrypted or compressed data indicative of a packer (2 events)

File has been identified by 15 AntiVirus engine on IRMA as malicious (15 events)

File has been identified by 59 AntiVirus engines on VirusTotal as malicious (50 out of 59 events)

Screenshots



➤ Ransomware.Thanos

Summary

File *Ransomware.Thanos.zip*

Summary

Download

Resubmit sample

Size	145.3KB
Type	Zip archive data, at least v7[0x314] to extract
MD5	00184463f3b071369d60353c692be6f0
SHA1	d3c1e90f39da2997ef4888b54d706b1a1fde642a
SHA256	cd0f55dd00111251cd580c7e7cc1d17448faf27e4ef39818d75ce330628c7787
SHA512	Show SHA512
CRC32	618FB6A8
ssdeep	None
Yara	None matched

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution					
Analysis					
Category	Started	Completed	Duration	Routing	Logs
FILE	Nov. 21, 2022, 10:07 p.m.	Nov. 21, 2022, 10:08 p.m.	20 seconds	internet	Show Analyzer Log Show Cuckoo Log

File has been identified by 8 AntiVirus engines on VirusTotal as malicious (8 events)	
Elastic	Windows.Ransomware.Thanos
Avast	Other:Malware-gen [Trj]
NANO-Antivirus	Trojan.Win32.DelShad.hnjzoa
Comodo	Malware@#y0vczrq8prlx
McAfee-GW-Edition	Artemis
Microsoft	Ransom:Win32/DelShad

Fortinet	W32/DelShad.THY!tr.ransom
AVG	Other.Malware-gen [Trj]