MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Tbopbh.exe**
ID	#3290212
MD5	14c8482f302b5e81e3fa1b18a509289d
SHA1	16525cb2fd86dce842107eb1ba6174b23f188537
SHA256	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
File Size	209.91 KB
Report Created	2022-01-17 00:02 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (4 rules, 4 matches)

Score	Category	Operation	Count	Classification
4/5	Execution	Executes encoded PowerShell command	1	-
	• (Process #1) tbopbh.exe executes base64-encoded Powershell command.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
2/5	Heuristics	Signed executable failed signature validation	1	-
	• C:\Users\RDhJ0CNFevzX\Desktop\Tbopbh.exe is signed, but signature validation failed.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) tbopbh.exe starts (process #2) powershell.exe with a hidden window.			

Mitre ATT&CK Matrix

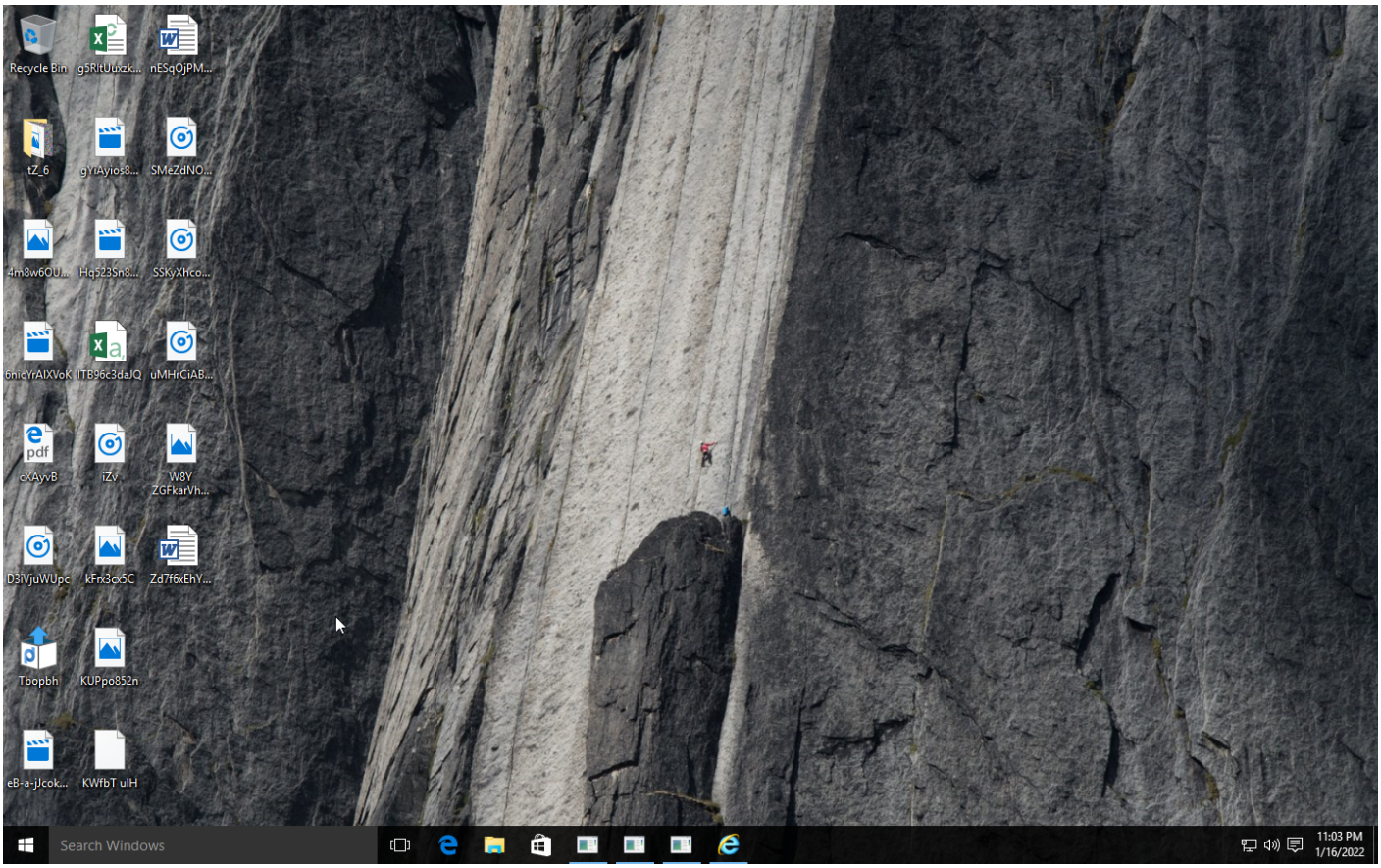
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1086 PowerShell			#T1143 Hidden Window							
				#T1140 Deobfuscate/ Decode Files or Information							
				#T1027 Obfuscated Files or Information							

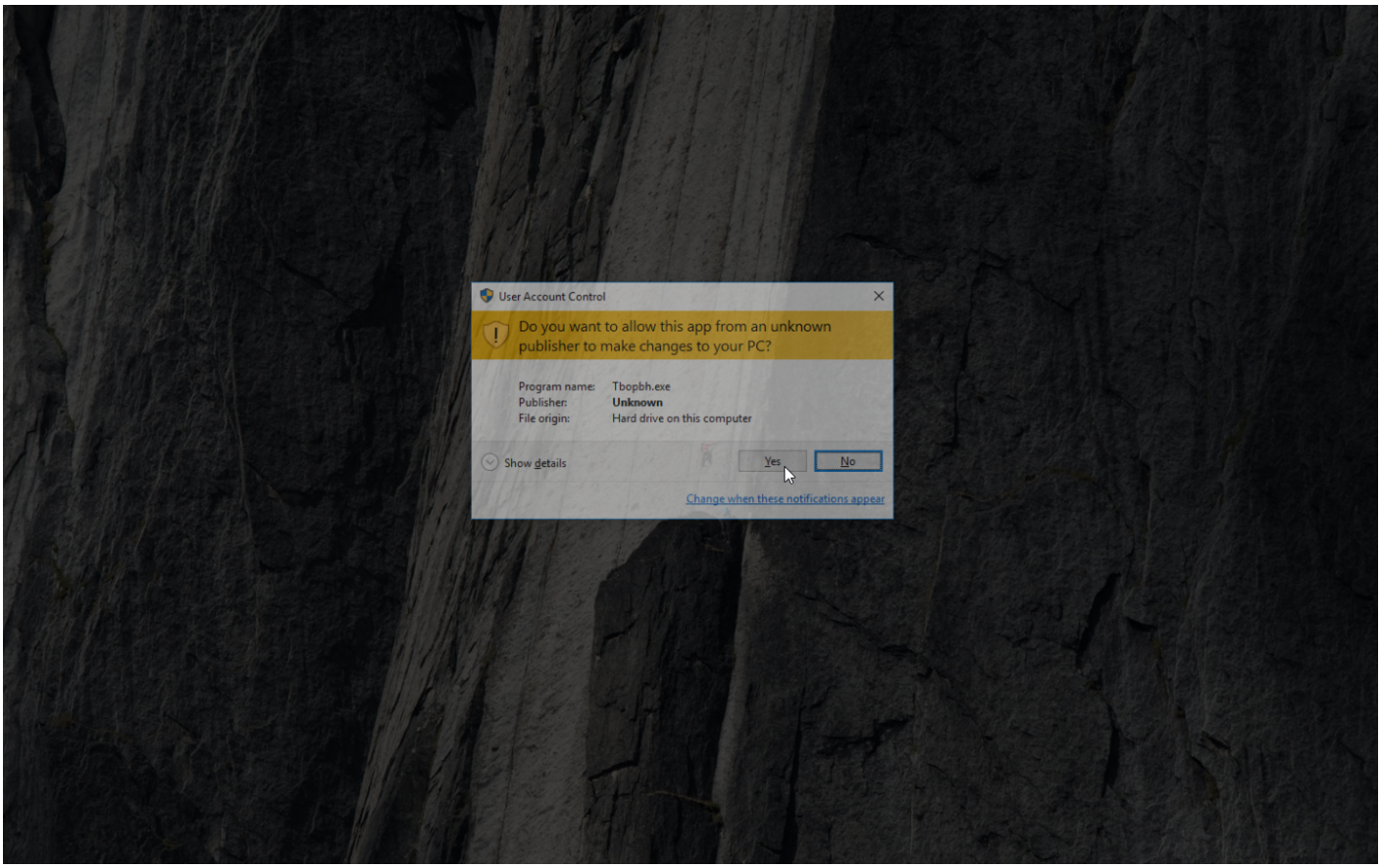
Sample Information

ID	#3290212
MD5	14c8482f302b5e81e3fa1b18a509289d
SHA1	16525cb2fd86dce842107eb1ba6174b23f188537
SHA256	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
SSDeep	3072:vf1GlJZUnjNbGgNQfYySlHiP1WLz4PcSOvG2jxZ:FbGoJ8iP19PjmGyf
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	Tbopbh.exe
File Size	209.91 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-01-17 00:02 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
g5RtUuxzk...
nESqOjPM...
tZ_6
gYtAyios8...
SMeZdNO...
4m8w6OU...
Hq523Sn8...
SSKyXHco...
6nicYrAIXVoK
ITB96c3daJQ
uMHrCiAB...
cXAyvB
iZv
W8Y ZGFkarVh...
D3iVjuWUpc
kFrx3cx5C
Zd7f6xEhY...
Tbopbh
KUPpo852n
eB-a-jJcok...
KWfbT ulH
Search Windows
11:03 PM
1/16/2022



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph

Process #1: tbopbh.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\tbopbh.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\Tbopbh.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 81490, Reason: Analysis Target
Unmonitor End Time	End Time: 321538, Reason: Terminated by Timeout
Monitor duration	240.05s
Return Code	Unknown
PID	796
Parent PID	1560
Bitness	32 Bit

Host Behavior

Type	Count
File	1
Process	1

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 127165, Reason: Child Process
Unmonitor End Time	End Time: 321538, Reason: Terminated by Timeout
Monitor duration	194.37s
Return Code	Unknown
PID	2356
Parent PID	796
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
File	1
Environment	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	C:\Users\RDhJ0CNFevzX\Desktop\Tbopbh.exe	Sample File	209.91 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
2282d72c7ebe715e339b0717c7708861fb4959f1dc948423ccd1ff9bd783e902	-	Embedded File	7.33 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN

Process

Process Name	Commandline	Verdict
tbopbh.exe	"C:\Users\RDhJ0CNFevzX\Desktop\Tbopbh.exe"	MALICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==	SUSPICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows