MALICIOUS

Classifications: Spyware

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**10101010.exe**
ID	#3869281
MD5	2b99e5c85cd8b0e6decf30d6daee094e
SHA1	c3e7652e16a2e03d96b0274b5520d19b96196a03
SHA256	e4defd8a187a513212cb19c9f2a800505395e66d9cd9eb3a96c291060224e7dd
File Size	308.00 KB
Report Created	2022-03-22 13:03 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 18 matches)

Score	Category	Operation	Count	Classification
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Total Commander, AbleFTP, git.			
2/5	Data Collection	Reads sensitive ftp data	2	-
	• (Process #1) 10101010.exe tries to read sensitive data of ftp application "AbleFTP" by file. • (Process #1) 10101010.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) 10101010.exe tries to read sensitive data of application "git" by file.			
2/5	System Modification	Changes the desktop wallpaper	1	-
	• (Process #1) 10101010.exe sets the desktop wallpaper to the file "c:\users\rdhj0cnfevzx\1.bmp".			
2/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #15) cmd.exe creates a new explorer.exe process.			
1/5	Anti Analysis	Tries to detect analyzer sandbox	1	-
	• (Process #1) 10101010.exe is possibly trying to detect analyzer sandbox by checking for patched sleep.			
1/5	Hide Tracks	Creates process with hidden window	9	-
	• (Process #1) 10101010.exe starts (process #2) taskkill.exe with a hidden window. • (Process #1) 10101010.exe starts (process #3) taskkill.exe with a hidden window. • (Process #1) 10101010.exe starts (process #4) taskkill.exe with a hidden window. • (Process #1) 10101010.exe starts (process #5) taskkill.exe with a hidden window. • (Process #1) 10101010.exe starts (process #6) taskkill.exe with a hidden window. • (Process #1) 10101010.exe starts (process #7) taskkill.exe with a hidden window. • (Process #1) 10101010.exe starts (process #14) cmd.exe with a hidden window. • (Process #1) 10101010.exe starts (process #15) cmd.exe with a hidden window. • (Process #1) 10101010.exe starts (process #16) cmd.exe with a hidden window.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) 10101010.exe resolves 76 API functions by name.			
1/5	Crash	An unmonitored process crashed	1	-
	• Unmonitored process microsoftedge.exe crashed.			
-	Trusted	Known clean file	1	-
	• File "C:\Users\RDhJ0CNFevzX\cpt.txt" is a known clean file.			

Mitre ATT&CK Matrix

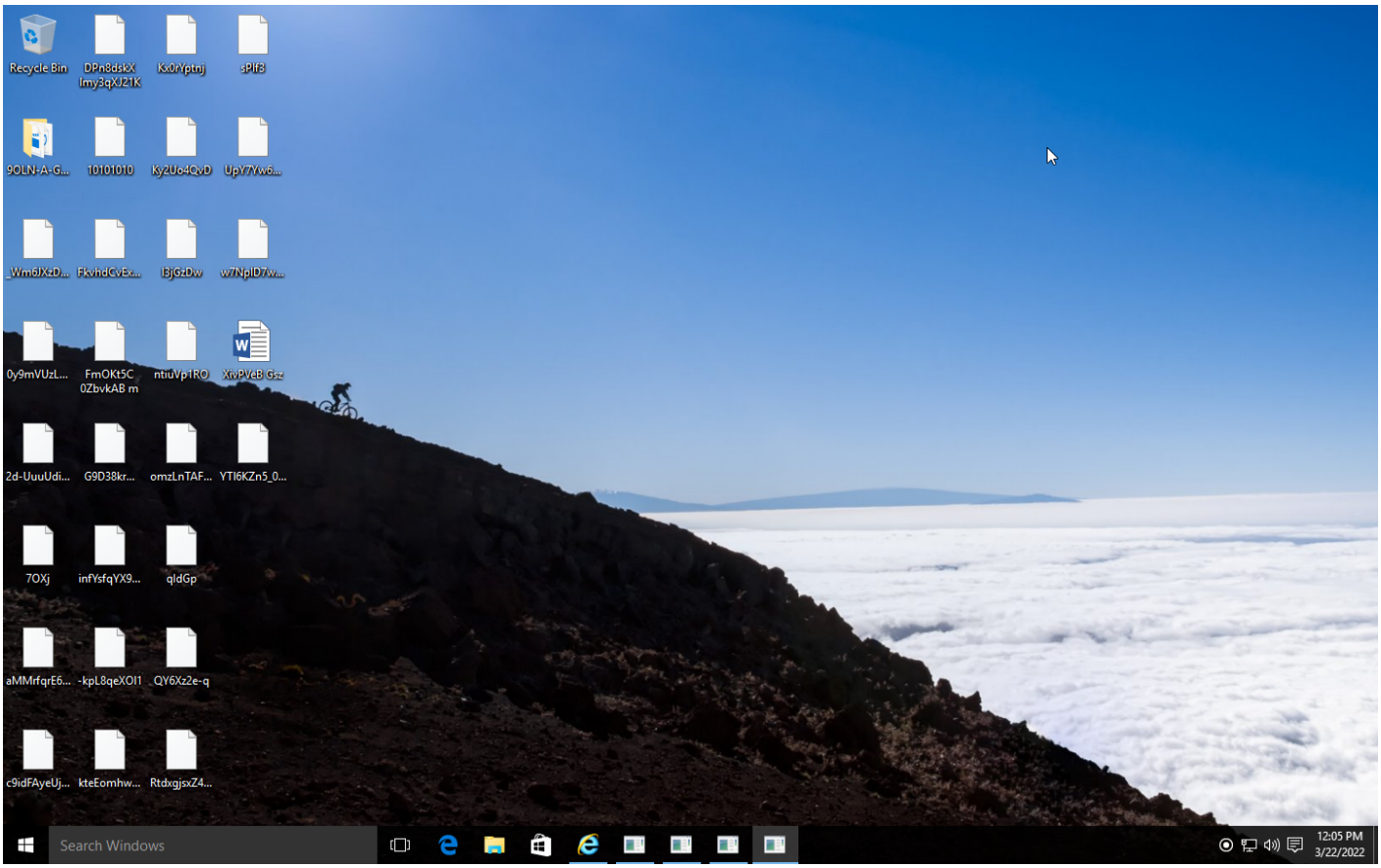
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1491 Defacement
				#T1143 Hidden Window		#T1497 Virtualization/ Sandbox Evasion		#T1005 Data from Local System			
				#T1045 Software Packing		#T1124 System Time Discovery					

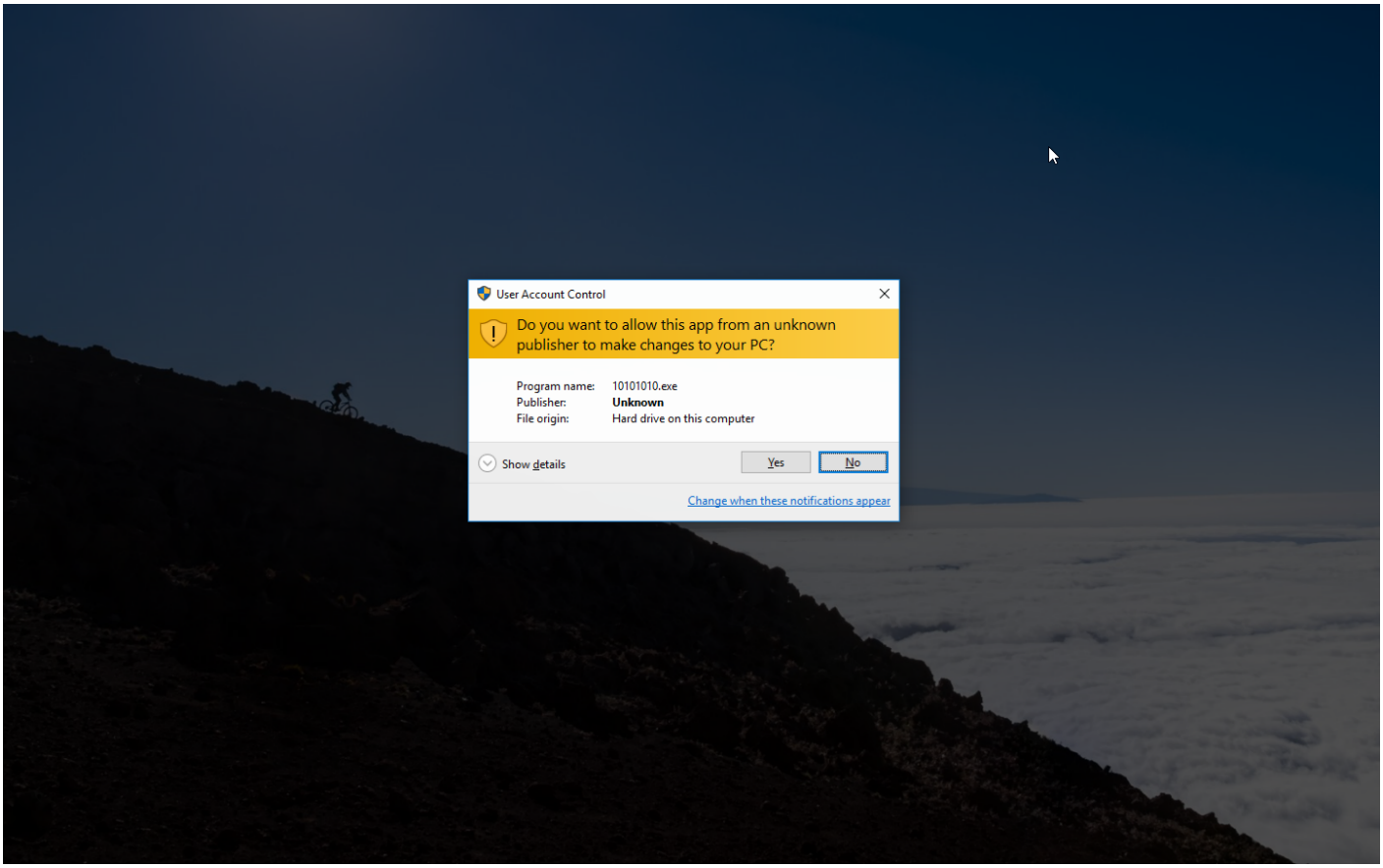
Sample Information

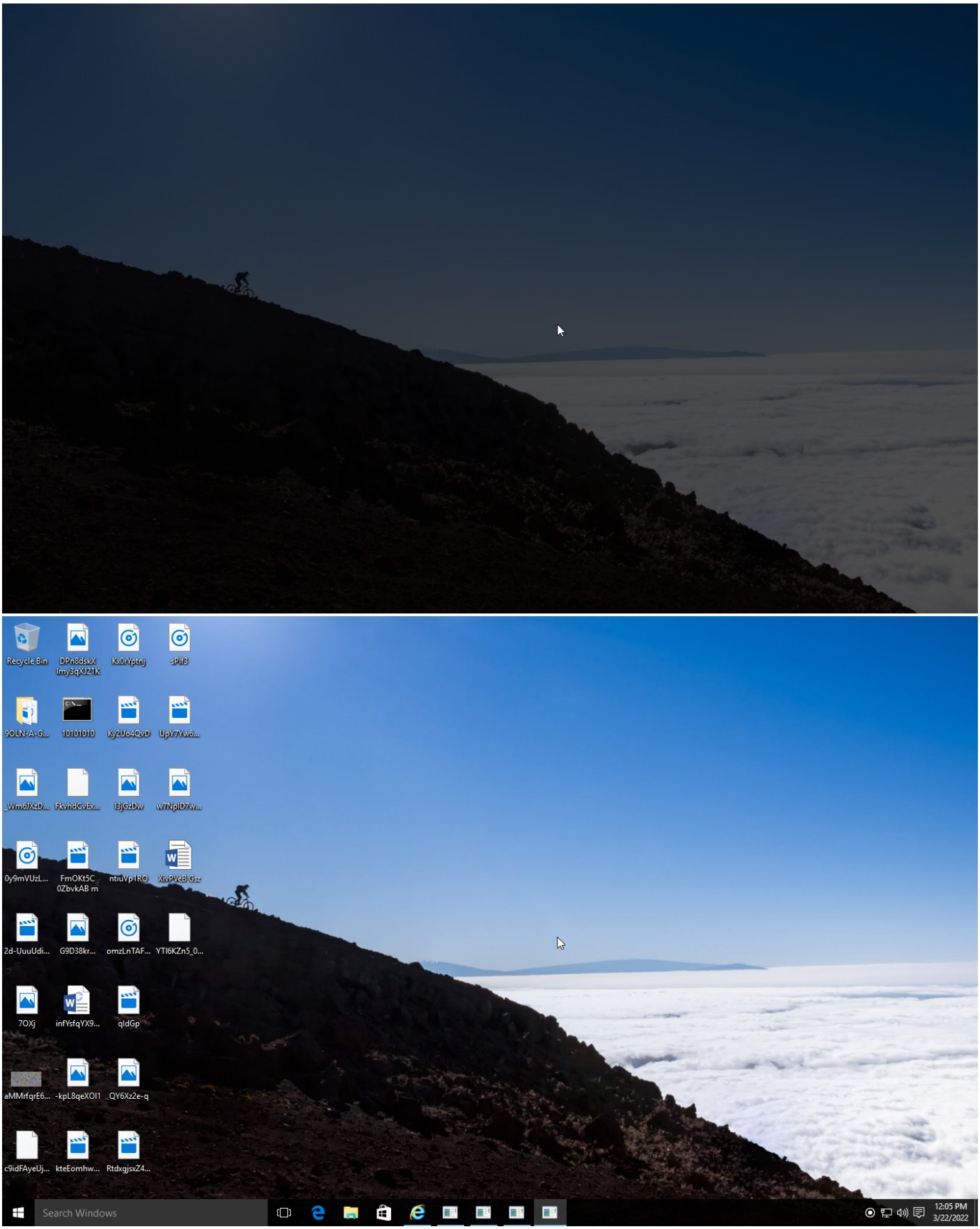
ID	#3869281
MD5	2b99e5c85cd8b0e6decf30d6daee094e
SHA1	c3e7652e16a2e03d96b0274b5520d19b96196a03
SHA256	e4defd8a187a513212cb19c9f2a800505395e66d9cd9eb3a96c291060224e7dd
SSDeep	6144:9mEdSunAqHdroKcykhPBbiMV5xzr2fXGzN:94ujKyUp+gOg
ImpHash	818c0e000ca7da0505349e2306c68948
File Name	10101010.exe
File Size	308.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-03-22 13:03 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	13
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
DPn8dskX
lmy3qXJ21K
Ks0rYptnj
sPlf3
9OLN-A-G...
10101010
Ky2Uo4QvD
UpY7Yw6...
_Wm6JX-D...
FkvhdCvEx...
I3jGzDw
w7NplD7w...
0y9mVUzL...
FmOKt5C
0ZbvkAB m
ntiuVp1RO
XivPVeB Gsz
2d-UuuUdi...
G9D38kr...
omzLnTAF...
YTI6KZn5_0...
7OXj
infYsfqYX9...
qldGp
aMMrfqrE6...
-kpL8qeXOI1
QY6Xz2e-q
c9idFAyeUj...
kteEomhw...
RtdxgjsxZ4...
Search Windows
12:05 PM
3/22/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 10101010.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

2 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

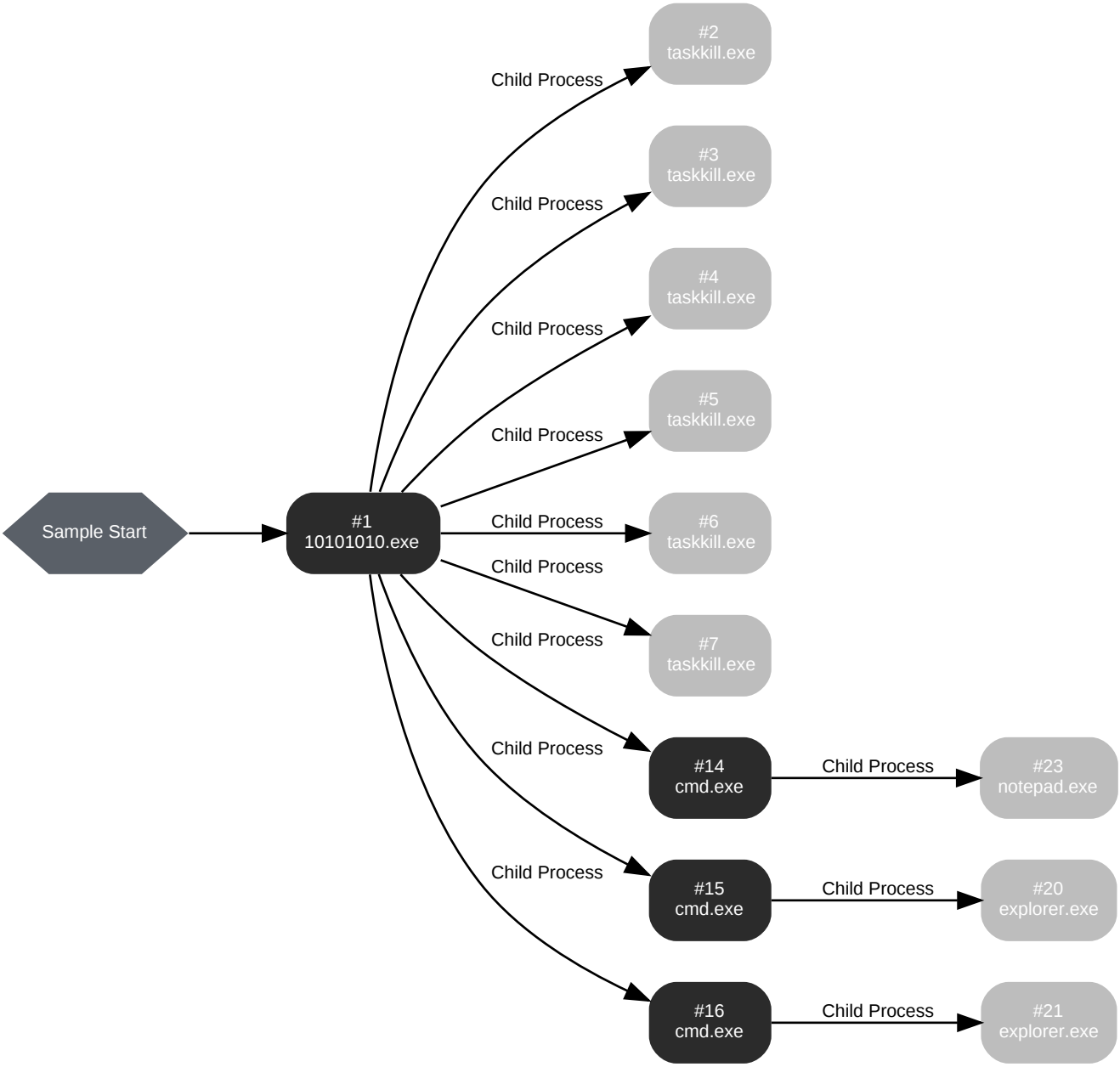
0 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
	http://mypage1.eu5.org/1.php	-	-		0 bytes	NA
	http://mypage1.unaux.com/index.htm	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: 10101010.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\10101010.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\10101010.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 69349, Reason: Analysis Target
Unmonitor End Time	End Time: 153305, Reason: Terminated
Monitor duration	83.96s
Return Code	0
PID	3864
Parent PID	1184
Bitness	32 Bit

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
-	31.79 KB	0562f9704a4c320bd0b4d3b93f691645063de71f0ec9d384aecdb0c5b3510dbf	✗
C:\Users\RDhJ0CNFevzX\Desktop\key1.txt	34 bytes	fa50a993ff179c990aea12383a3e9e7e6e996d882f6fe712819be644f1f912a5	✗
C:\Users\RDhJ0CNFevzX\Desktop\INSTRUCTIONS.txt	607 bytes	59a1f296a4c94d7c676fb8e97400de56172a3bf854812aa36e15f78c4ffe527f	✗
C:\Users\RDhJ0CNFevzX\1.bmp	3075.05 KB	0fb2a16bb74da3c20e99a585e28f138ee4862987230916607bab4729d2f49888	✗
C:\Users\RDhJ0CNFevzX\cpt.txt	3 bytes	f1b2f662800122bed0ff255693df89c4487fbdcf453d3524a42d4ec20c3d9c04	✗

Host Behavior

Type	Count
System	2422
Module	99
Environment	1
File	680
-	2
Mutex	1
Window	25
Registry	7
Keyboard	1
Process	9
-	2

Process #2: taskkill.exe

ID	2
File Name	c:\windows\syswow64\taskkill.exe
Command Line	TASKKILL /IM 1cv8.exe /F
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 118773, Reason: Child Process
Unmonitor End Time	End Time: 204963, Reason: Terminated
Monitor duration	86.19s
Return Code	128
PID	744
Parent PID	3864
Bitness	32 Bit

Process #3: taskkill.exe

ID	3
File Name	c:\windows\syswow64\taskkill.exe
Command Line	TASKKILL /IM winword.exe /F
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 119116, Reason: Child Process
Unmonitor End Time	End Time: 205162, Reason: Terminated
Monitor duration	86.05s
Return Code	128
PID	836
Parent PID	3864
Bitness	32 Bit

Process #4: taskkill.exe

ID	4
File Name	c:\windows\syswow64\taskkill.exe
Command Line	TASKKILL /IM excel.exe /F
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 119136, Reason: Child Process
Unmonitor End Time	End Time: 204957, Reason: Terminated
Monitor duration	85.82s
Return Code	128
PID	1452
Parent PID	3864
Bitness	32 Bit

Process #5: taskkill.exe

ID	5
File Name	c:\windows\syswow64\taskkill.exe
Command Line	TASKKILL /IM powerpnt.exe /F
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 119153, Reason: Child Process
Unmonitor End Time	End Time: 205000, Reason: Terminated
Monitor duration	85.85s
Return Code	128
PID	884
Parent PID	3864
Bitness	32 Bit

Process #6: taskkill.exe

ID	6
File Name	c:\windows\syswow64\taskkill.exe
Command Line	TASKKILL /IM vmware.exe /F
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 119172, Reason: Child Process
Unmonitor End Time	End Time: 205004, Reason: Terminated
Monitor duration	85.83s
Return Code	128
PID	612
Parent PID	3864
Bitness	32 Bit

Process #7: taskkill.exe

ID	7
File Name	c:\windows\syswow64\taskkill.exe
Command Line	TASKKILL /IM VirtualBox.exe /F
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 119191, Reason: Child Process
Unmonitor End Time	End Time: 204961, Reason: Terminated
Monitor duration	85.77s
Return Code	128
PID	3384
Parent PID	3864
Bitness	32 Bit

Process #14: cmd.exe

ID	14
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c C:\Users\RDhJ0CNFevzX\Desktop\INSTRUCTIONS.txt
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 131238, Reason: Child Process
Unmonitor End Time	End Time: 309363, Reason: Terminated by Timeout
Monitor duration	178.12s
Return Code	Unknown
PID	3176
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	11
Environment	14
System	1
Process	1

Process #15: cmd.exe

ID	15
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c explorer.exe http://mypage1.eu5.org/1.php
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 133981, Reason: Child Process
Unmonitor End Time	End Time: 222671, Reason: Terminated
Monitor duration	88.69s
Return Code	1
PID	3820
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	19
System	1
Process	1

Process #16: cmd.exe

ID	16
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c explorer.exe http://mypage1.unaux.com/index.htm
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 134006, Reason: Child Process
Unmonitor End Time	End Time: 219746, Reason: Terminated
Monitor duration	85.74s
Return Code	1
PID	1620
Parent PID	3864
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	17
Environment	19
System	1
Process	1

Process #20: explorer.exe

ID	20
File Name	c:\windows\syswow64\explorer.exe
Command Line	explorer.exe http://mypage1.eu5.org/1.php
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 154069, Reason: Child Process
Unmonitor End Time	End Time: 222175, Reason: Terminated
Monitor duration	68.11s
Return Code	1
PID	3784
Parent PID	3820
Bitness	32 Bit

Process #21: explorer.exe

ID	21
File Name	c:\windows\syswow64\explorer.exe
Command Line	explorer.exe http://mypage1.unaux.com/index.htm
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 156983, Reason: Child Process
Unmonitor End Time	End Time: 219302, Reason: Terminated
Monitor duration	62.32s
Return Code	1
PID	3772
Parent PID	1620
Bitness	32 Bit

Process #23: notepad.exe

ID	23
File Name	c:\windows\syswow64\notepad.exe
Command Line	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\RDhJ0CNFevzX\Desktop\INSTRUCTIONS.txt
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 177626, Reason: Child Process
Unmonitor End Time	End Time: 309363, Reason: Terminated by Timeout
Monitor duration	131.74s
Return Code	Unknown
PID	4348
Parent PID	3176
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e4defd8a187a513212cb19c9f2a800505395e66d9cd9eb3a96c291060224e7dd	C:\Users\RDhJ0CNFevzX\Desktop\10101010.exe	Sample File	308.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
0fb2a16bb74da3c20e99a585e28f138ee486298723091660 7bab4729d2f49888	C:\Users\RDhJ0CNFevzX\1.bmp	Dropped File	3075.05 KB	image/bmp	Create, Write, Access	SUSPICIOUS
0562f9704a4c320bd0b4d3b9 3f691645063de71f0ec9d384 aecdb0c5b3510dbf	c:\users\rdhj0cnfevzx\appdata\local\temp\~dfa07b71dbcc340f2c.tmp	Dropped File	31.79 KB	application/CDFV2	-	CLEAN
fa50a993ff179c990aea12383 a3e9e7e6e996d882f6fe7128 19be644f1f912a5	C:\Users\RDhJ0CNFevzX\Desktop\key1.txt	Dropped File	34 bytes	text/plain	Create, Write, Access	CLEAN
59a1f296a4c94d7c676fb8e9 7400de56172a3bf854812aa3 6e15f78c4ffe527f	C:\Users\RDhJ0CNFevzX\Desktop\INSTRUCTIONS.txt	Dropped File	607 bytes	text/plain	Create, Write, Access	CLEAN
f1b2f662800122bed0ff25569 3df89c4487fbdcf453d3524a4 2d4ec20c3d9c04	C:\Users\RDhJ0CNFevzX\cpt.txt	Dropped File	3 bytes	text/plain	Read, Create, Write, Access	CLEAN
ece7dff309c7fea3c65c5b98a faae0b3d0b5cde56ad70f25b e40ff50764f8868	-	Embedded File	5.66 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\10101010.exe	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSVBVM60.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\cpt.txt	Dropped File	Read, Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\key1.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\INSTRUCTIONS.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\1.bmp	Dropped File	Create, Write, Access	CLEAN
WINHELP.INI	Accessed File	Read, Access	CLEAN
C:\Windows\SYSTEM32\.HLP	Accessed File	Access	CLEAN
C:\Windows\Help\.HLP	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
explorer.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://mypage1.eu5.org/1.php	-	-	-	-	CLEAN
http://mypage1.unaux.com/index.htm	-	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
mypage1.eu5.org	-	-	HTTP	CLEAN
mypage1.unaux.com	-	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
162.253.155.226	mypage1.eu5.org	United States	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors	access	10101010.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows	access	10101010.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\HTML Help	access	10101010.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\HTML Help\.HLP	read, access	10101010.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Help	access	10101010.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
10101010.exe	"C:\Users\RDhJ0CNFevzX\Desktop\10101010.exe"	SUSPICIOUS
cmd.exe	cmd /c explorer.exe http://mypage1.eu5.org/1.php	SUSPICIOUS
explorer.exe	explorer.exe http://mypage1.eu5.org/1.php	SUSPICIOUS
taskkill.exe	TASKKILL /IM 1cv8.exe /F	CLEAN

Process Name	Commandline	Verdict
taskkill.exe	TASKKILL /IM winword.exe /F	CLEAN
taskkill.exe	TASKKILL /IM excel.exe /F	CLEAN
taskkill.exe	TASKKILL /IM powerpnt.exe /F	CLEAN
taskkill.exe	TASKKILL /IM vmware.exe /F	CLEAN
taskkill.exe	TASKKILL /IM VirtualBox.exe /F	CLEAN
cmd.exe	cmd /c C:\Users\RDhJ0CNFevzX\Desktop\INSTRUCTIONS.txt	CLEAN
cmd.exe	cmd /c explorer.exe http://mypage1.unaux.com/index.htm	CLEAN
explorer.exe	explorer.exe http://mypage1.unaux.com/index.htm	CLEAN
notepad.exe	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\RDhJ0CNFevzX\Desktop\INSTRUCTIONS.txt	CLEAN

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	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.16 / 2022-03-11 16:16:43
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.16 / 2022-03-11 16:16:43
YARA Built-in Ruleset Version	4.4.1.16

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