MALICIOUS

Classifications: Spyware | Keylogger

Threat Names: Mal/Generic-S | SnakeKeylogger

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe**
ID	#7164612
MD5	cc17147aa1a1f904d8b9aef3516b804e
SHA1	6cc7070b205acdd8b136889cc7d8042201a09ef0
SHA256	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171
File Size	766.00 KB
Report Created	2023-03-17 01:52 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 19 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	SnakeKeylogger configuration was extracted	1	Keylogger
	• A configuration for SnakeKeylogger was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "SnakeKeylogger" from ruleset "Malware" has matched on a memory dump for (process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe modifies memory of (process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe alters context of (process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\IFNGRZH.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\IFNGRZH.exe", to be triggered by REGISTRATION.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe creates mutex with name "lgYctlHZz".			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe enables process privilege "SeDebugPrivilege". • (Process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe starts (process #3) schtasks.exe with a hidden window. • (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe starts (process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe reads from (process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			

Score	Category	Operation	Count	Classification
1/5	Network Connection	Performs DNS request	1	-
	• (Process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe resolves hostname "checkip.dyndns.org" to IP "193.122.6.168".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe opens an outgoing TCP connection to host "132.226.247.73:80".			
1/5	Discovery	Checks external IP address	1	-
	• (Process #7) 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe checks external IP by asking IP info service at "http://checkip.dyndns.org".			

Malware Configuration: SnakeKeylogger

Mitre ATT&CK Matrix

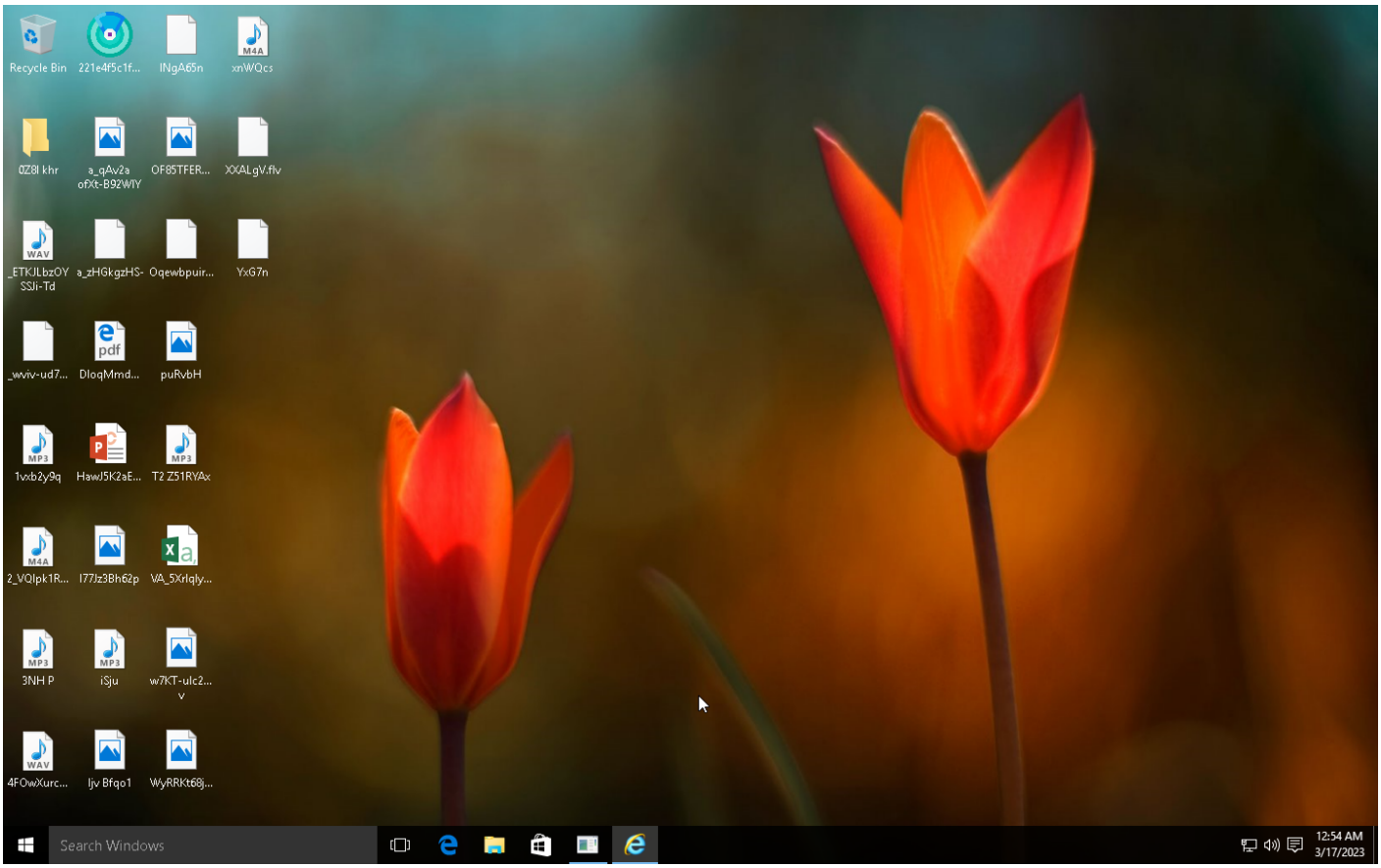
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window	#T1214 Credentials in Registry	#T1012 Query Registry		#T1119 Automated Collection			
				#T1045 Software Packing		#T1016 System Network Configuration Discovery		#T1005 Data from Local System			

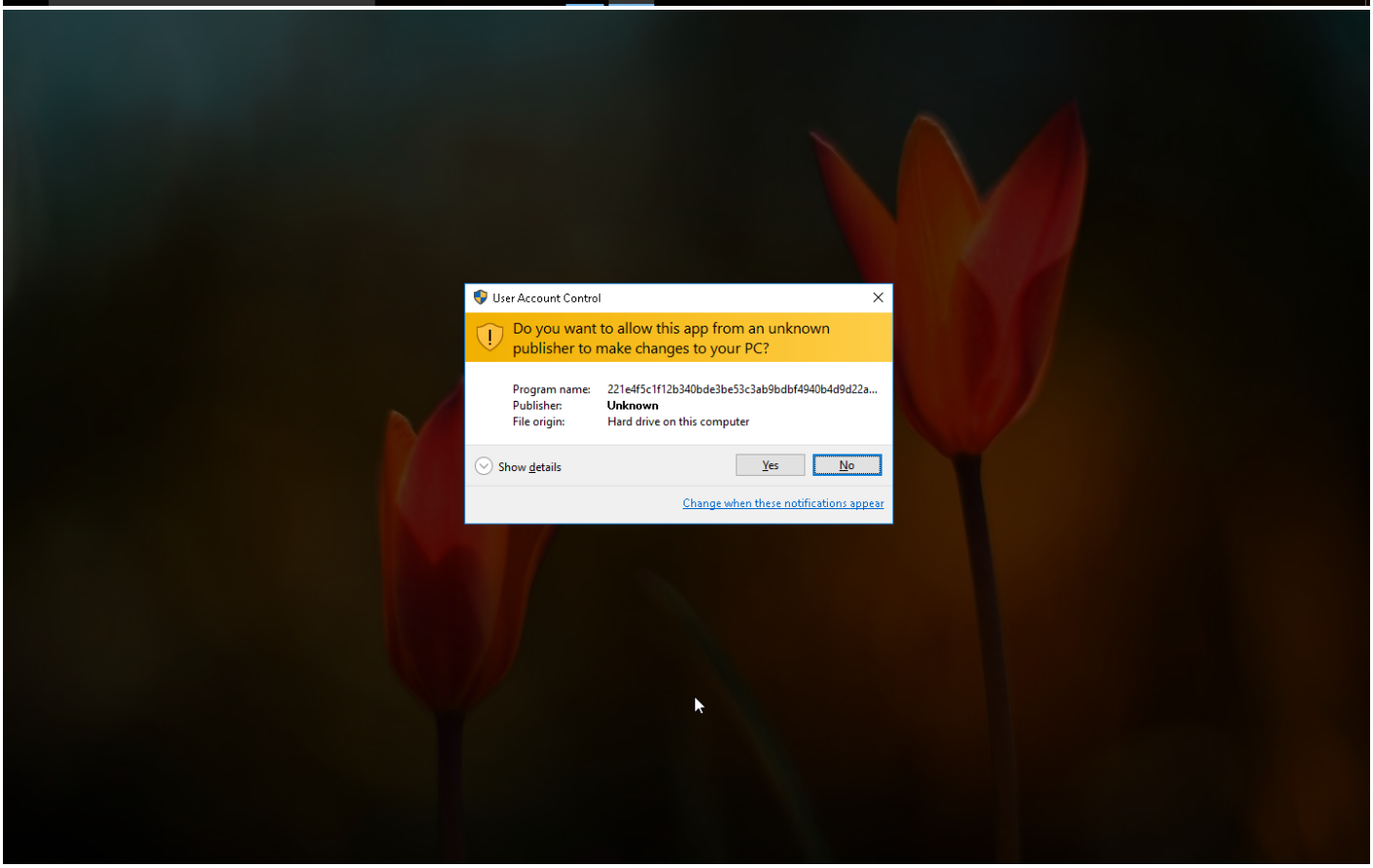
Sample Information

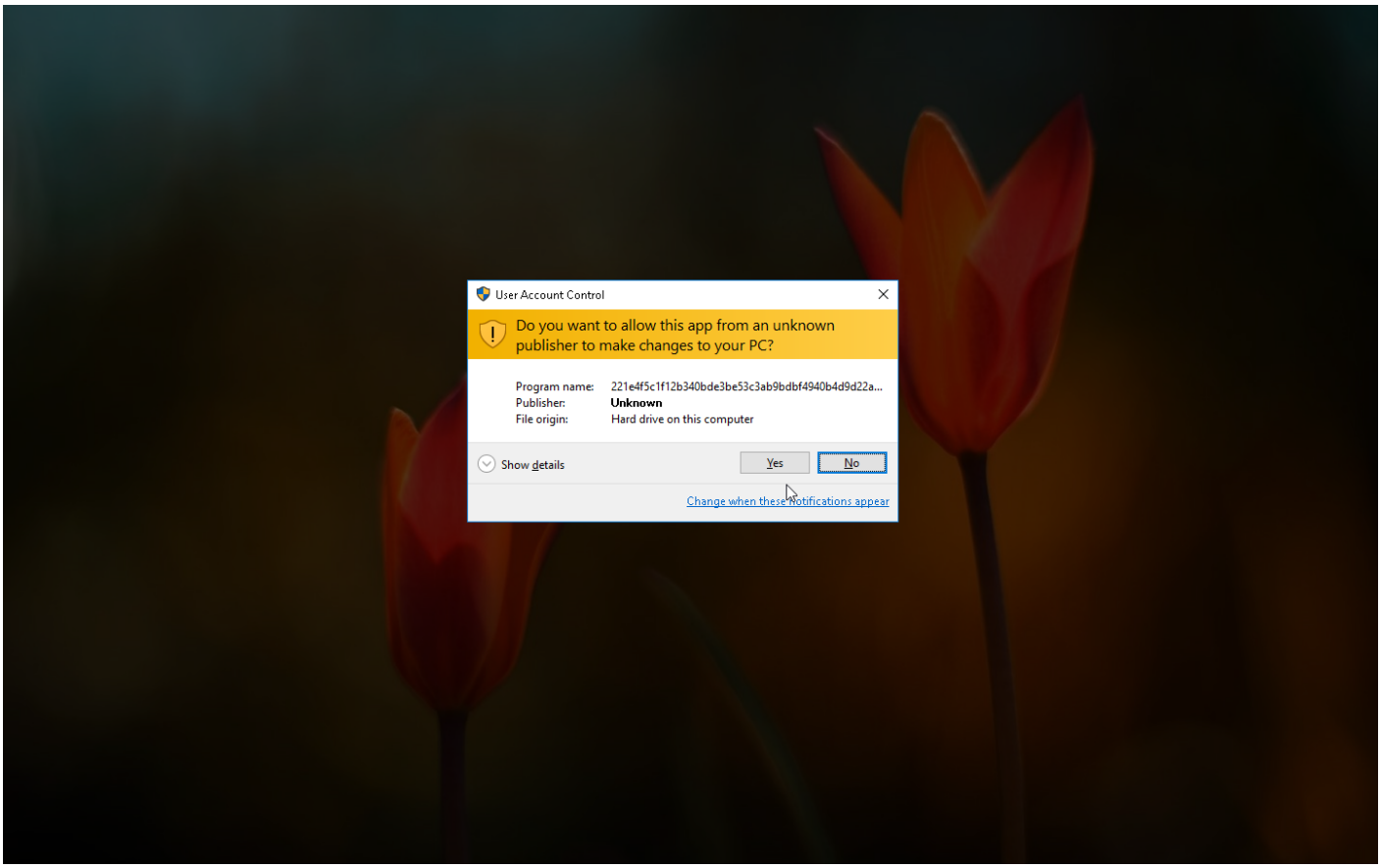
ID	#7164612
MD5	cc17147aa1a1f904d8b9aef3516b804e
SHA1	6cc7070b205acdd8b136889cc7d8042201a09ef0
SHA256	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171
SSDeep	12288:jzAuF5iJGRTwdx8SQ7ZIuhjvOmODV17VfGuVr4UG4mHd/wunj/N/VI04:LFEJTUdshjvUD/7d1r1unx/VI0
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe
File Size	766.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

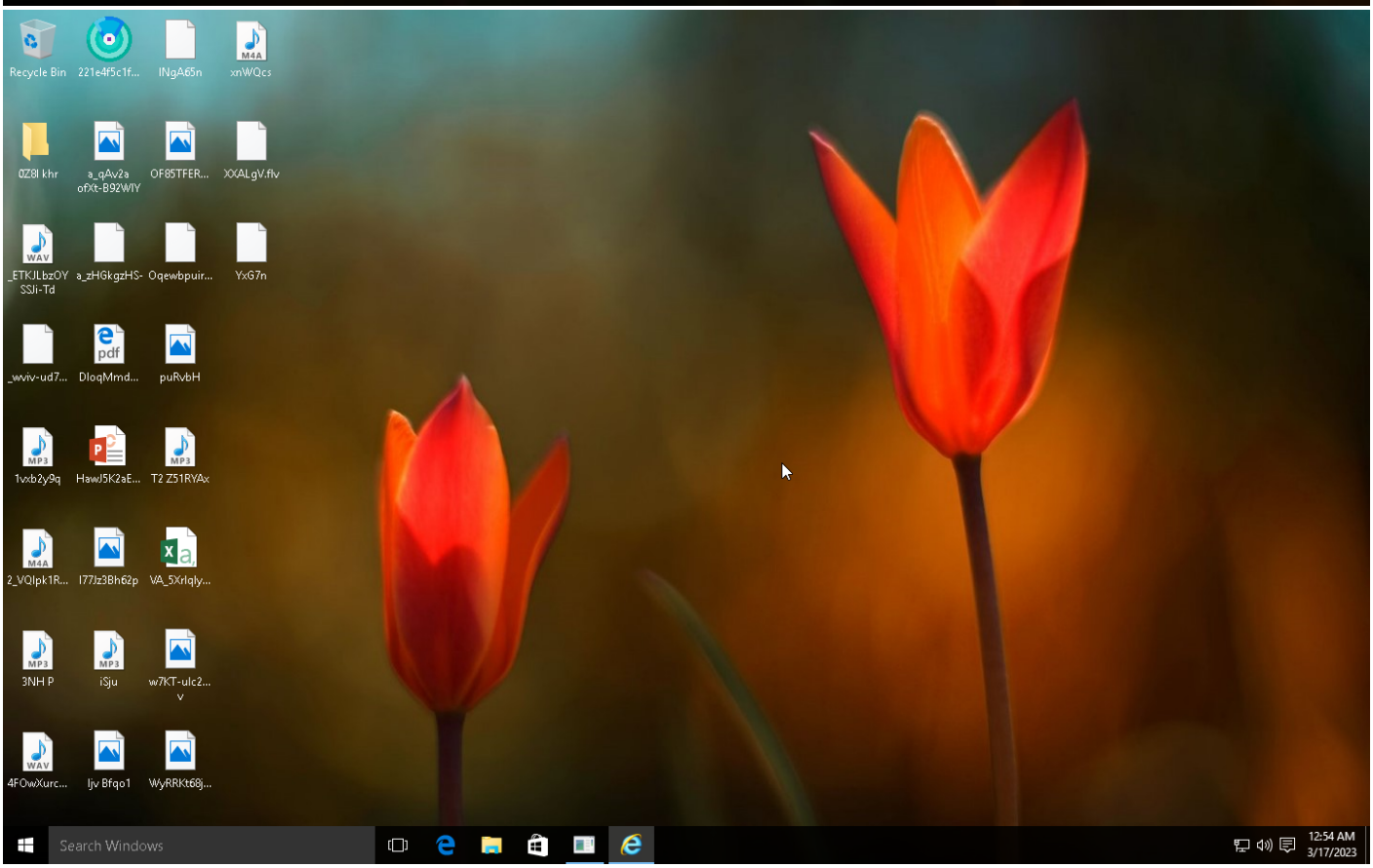
Analysis Information

Creation Time	2023-03-17 01:52 (UTC+1)
Analysis Duration	00:03:25
Termination Reason	Timeout
Number of Monitored Processes	8
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	1


Recycle Bin
221e4f5c1f...
INgA65n
xnWQcs
0Z8l khr
a_qAv2a ofXt-B92WIY
OF85TFER...
XXALgV.flv
_ETKJLbzOY SSli-Td
a_zHGkgzHS-
Oqewbpuir...
YxG7n
_wviv-ud7...
DloqMmd...
puRvbH
1vxb2y9q
HawJ5K2aE...
T2 Z51RYAx
2_VQlpk1R...
I77Jz3Bh62p
VA_5Xrlqly...
3NH P
iSju
w7KT-ulc2... v
4FOwXurc...
ljv Bfqo1
WyRRKt68j...
Search Windows
12:54 AM
3/17/2023


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22a...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

1.85 KB total sent

1.74 KB total received

3 ports 80, 53, 445

2 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 363 bytes sent, 405 bytes received

HTTP Requests

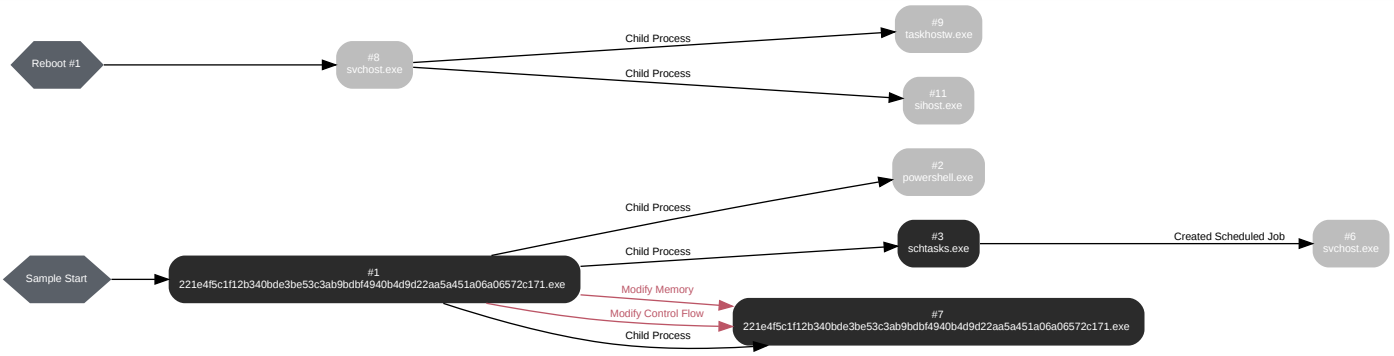
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://checkip[.]dyndns[.]org	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	checkip[.]dyndns[.]org, checkip[.]dyndns[.]com	NO_ERROR	193.122.6.168, 193.122.130.0, 132.226.247.73, 158.101.44.242, 132.226.8.169	checkip[.]dyndns[.]com	CLEAN

BEHAVIOR

Process Graph



Process #1: 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 116621, Reason: Analysis Target
Unmonitor End Time	End Time: 193149, Reason: Terminated
Monitor duration	76.53s
Return Code	0
PID	3372
Parent PID	1900
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\IFNGRZH.exe	766.00 KB	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp16B3.tmp	1.56 KB	493f65e79af5a168fcf79b4557b85b5598f853f39bbffe7e9cfa3c63548160cd	✖

Host Behavior

Type	Count
Registry	4
Module	105
Window	4
File	10
Mutex	2
User	2
System	8
Process	4
-	3
-	7

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" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\IFNGRZH.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 176790, Reason: Child Process
Unmonitor End Time	End Time: 208148, Reason: Terminated
Monitor duration	31.36s
Return Code	1073807364
PID	4716
Parent PID	3372
Bitness	32 Bit

Process #3: schtasks.exe

ID	3
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\IFNGRZH" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp16B3.tmp"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 176918, Reason: Child Process
Unmonitor End Time	End Time: 183212, Reason: Terminated
Monitor duration	6.29s
Return Code	0
PID	4692
Parent PID	3372
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
COM	1
File	10

Process #6: svchost.exe

ID	6
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 180499, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 317217, Reason: Terminated by timeout
Monitor duration	136.72s
Return Code	Unknown
PID	864
Parent PID	4692
Bitness	64 Bit

Process #7: 221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 183474, Reason: Child Process
Unmonitor End Time	End Time: 213051, Reason: Terminated
Monitor duration	29.58s
Return Code	1073807364
PID	4556
Parent PID	3372
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	0xd28	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	0xd28	0x402000(4202496)	0x1ea00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	0xd28	0x422000(4333568)	0x1200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	0xd28	0x424000(4341760)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	0xd28	0x3c3008(3944456)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	0xd28 / 0x11ac	0x4207fe(4327422)	-	✔	1

Host Behavior

Type	Count
User	1
System	6
Registry	66
Module	3
File	24
-	13
Environment	4
-	2

Network Behavior

Type	Count
HTTP	1
DNS	1
TCP	1

Process #8: svchost.exe

ID	8
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 234209, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 317217, Reason: Terminated by timeout
Monitor duration	83.01s
Return Code	Unknown
PID	856
Parent PID	4692
Bitness	64 Bit

Process #9: taskhostw.exe

ID	9
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 271172, Reason: Child Process
Unmonitor End Time	End Time: 317217, Reason: Terminated by timeout
Monitor duration	46.05s
Return Code	Unknown
PID	1232
Parent PID	856
Bitness	64 Bit

Process #11: sihost.exe

ID	11
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 283078, Reason: Child Process
Unmonitor End Time	End Time: 317217, Reason: Terminated by timeout
Monitor duration	34.14s
Return Code	Unknown
PID	1512
Parent PID	856
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171	C:\Users\RDhJ0CNFevzX\AppData\Roaming\IFNGRZH.exe, C:\Users\RDhJ0CNFevzX\Desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	Dropped File	766.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
6422009ebb2d117a18193a60242ae969355fe091e2a47c8ee54b2bfb3204514a	-	Extracted File	13.91 KB	image/png	-	CLEAN
493f65e79af5a168fcf79b4557b85b5598f853f39bbffe7e9cfa3c63548160cd	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp16B3.tmp	Dropped File	1.56 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN
1cd5527f780c5023ee64244b5d3cd9ed1adc55b06bc3bd2bf0d30a58e43e5969	-	Downloaded File	104 bytes	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\IFNGRZH.exe	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	Accessed File, Sample File	Access	MALICIOUS
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp16B3.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Default\Ya Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Xpom\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://checkip[.]dyndns[.]org	Contacted, Extracted	132.226.247.73, 158.101.44.242, 193.122.6.168, 193.122.130.0, 132.226.8.169	Germany, Brazil, Japan, United States	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
checkip[.]dyndns[.]org	132.226.247.73, 158.101.44.242, 193.122.6.168, 193.122.130.0, 132.226.8.169	Germany, Brazil, Japan, United States	DNS, HTTP, TCP	CLEAN
checkip[.]dyndns[.]com	132.226.247.73, 158.101.44.242, 193.122.6.168, 193.122.130.0, 132.226.8.169	Germany, Brazil, Japan, United States	DNS, HTTP, TCP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
132.226.8.169	checkip[.]dyndns[.]org, checkip[.]dyndns[.]com	Japan	DNS	CLEAN
193.122.6.168	checkip[.]dyndns[.]org, checkip[.]dyndns[.]com	Germany	DNS	CLEAN
132.226.247.73	checkip[.]dyndns[.]org, checkip[.]dyndns[.]com	Brazil	DNS, HTTP, TCP	CLEAN
193.122.130.0	checkip[.]dyndns[.]org, checkip[.]dyndns[.]com	United States	DNS	CLEAN
158.101.44.242	checkip[.]dyndns[.]org, checkip[.]dyndns[.]com	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
lgYctlHZz	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Foxmail.url.mailto\Shell\open\command	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	CLEAN

Process

Process Name	Commandline	Verdict
221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	"C:\Users\RDhJ0CNFevzX\Desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe"	MALICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\IFNGRZH" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp16B3.tmp"	SUSPICIOUS
221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe	"C:\Users\RDhJ0CNFevzX\Desktop\221e4f5c1f12b340bde3be53c3ab9bdbf4940b4d9d22aa5a451a06a06572c171.exe"	SUSPICIOUS
sihost.exe	sihost.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskhostw.exe	taskhostw.exe SYSTEM	CLEAN
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\IFNGRZH.exe"	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	SnakeKeylogger	Snake Keylogger	Memory Dump	-	Spyware	5/5

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	2023.1.0
Dynamic Engine Version	2023.1.0 / 01/31/2023 04:27
Static Engine Version	2023.1.0.0 / 2023-01-31 03:00:19
AV Exceptions Version	2023.1.1.6 / 2023-02-03 15:34:21
Link Detonation Heuristics Version	2023.1.1.12 / 2023-02-20 08:47:29
Smart Memory Dumping Rules Version	2023.1.1.6 / 2023-02-03 15:34:21
Config Extractors Version	2023.1.1.16 / 2023-03-09 20:16:03
Signature Trust Store Version	2023.1.1.7 / 2023-02-06 18:37:42
VMRay Threat Identifiers Version	2023.1.1.16 / 2023-03-09 20:16:03
YARA Built-in Ruleset Version	2023.1.1.16

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
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	8.0.1710.11

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