MALICIOUS

Classifications: Spyware, Keylogger

Threat Names: Phoenix, Mal/Generic-S, Trojan.GenericKD.37672864, DeepScan:Generic.MSIL.PasswordStealerA.D9D58869

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**RFQ Document.bin.exe**
ID	#2784135
MD5	64468b2ab541687572ce6b435b41f2bd
SHA1	893ae234d351c762ab388a7337c625e4b213da6e
SHA256	d3ac98cf64ca2fca455b2e4f002c3381bcee699cf64bbfaa076222209f834b1a
File Size	336.75 KB
Report Created	2021-09-28 19:32 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (23 rules, 52 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Keylogger, Spyware
	• Rule "PhoenixKeylogger" from ruleset "Malware" has matched on a memory dump for (process #2) rfq document.bin.exe. • Rule "PhoenixKeylogger" from ruleset "Malware" has matched on the function strings for (process #2) rfq document.bin.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: CocCoc, CentBrowser, Maple Studio, Comodo Dragon, Yandex Browser, Orbitum, Sputnik, FileZilla, Am... ...e Chrome, 7Star, Opera, Elements Browser, Uran, Epic Privacy Browser, Microsoft Outlook, Chedot, Torch, Vivaldi, Chromium, Kometa.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nsb2DC0.tmp\tkwj.dll" as "Mal/Generic-S".			
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-
	• Built-in AV detected the sample itself as "Trojan.GenericKD.37672864". • Built-in AV detected a memory dump of (process #1) rfq document.bin.exe as "DeepScan:Generic.MSIL.PasswordStealerA.D9D58869". • Built-in AV detected a memory dump of (process #1) rfq document.bin.exe as "Generic.Malware.SPfVI.5D748CCB".			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #2) rfq document.bin.exe reads the network adapters' addresses by API.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #2) rfq document.bin.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Data Collection	Reads sensitive browser data	20	-
	• (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Yandex Browser" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Torch" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Uran" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "7Star" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Chrome Canary" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Maple Studio" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Sputnik" by file. • (Process #2) rfq document.bin.exe tries to read sensitive data of web browser "Elements Browser" by file.			
2/5	Data Collection	Reads sensitive ftp data	1	-

Score	Category	Operation	Count	Classification
	• (Process #2) rfq document.bin.exe tries to read sensitive data of ftp application "FileZilla" by file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #2) rfq document.bin.exe tries to read sensitive data of application "Pidgin" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #2) rfq document.bin.exe has a thread which sleeps more than 5 minutes.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	3	-
	• (Process #1) rfq document.bin.exe makes a direct system call to "NtUnmapViewOfSection". • (Process #1) rfq document.bin.exe makes a direct system call to "NtWriteVirtualMemory". • (Process #1) rfq document.bin.exe makes a direct system call to "NtResumeThread".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) rfq document.bin.exe modifies memory of (process #2) rfq document.bin.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) rfq document.bin.exe alters context of (process #2) rfq document.bin.exe.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) rfq document.bin.exe starts (process #2) rfq document.bin.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) rfq document.bin.exe reads from (process #2) rfq document.bin.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) rfq document.bin.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #2) rfq document.bin.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #2) rfq document.bin.exe tries to gather information about application "FileZilla" by file. • (Process #2) rfq document.bin.exe tries to gather information about application "Pidgin" by file.			
1/5	Execution	Drops PE file	1	-
	• (Process #1) rfq document.bin.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\nsb2DC0.tmp\tkwj.dll".			
1/5	Execution	Executes itself	1	-
	• (Process #1) rfq document.bin.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\RFQ Document.bin.exe.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #2) rfq document.bin.exe checks external IP by asking IP info service at "http://checkip.dyndns.org/".			
1/5	Network Connection	Performs DNS request	3	-

Score	Category	Operation	Count	Classification
		• (Process #2) rfq document.bin.exe resolves host name "checkip.dyndns.org" to IP "216.146.43.70". • (Process #2) rfq document.bin.exe resolves host name "freegeoip.app" to IP "172.67.188.154". • (Process #2) rfq document.bin.exe resolves host name "api.telegram.org" to IP "149.154.167.220".		
1/5	Network Connection	Connects to remote host	3	-
		• (Process #2) rfq document.bin.exe opens an outgoing TCP connection to host "216.146.43.70:80". • (Process #2) rfq document.bin.exe opens an outgoing TCP connection to host "172.67.188.154:443". • (Process #2) rfq document.bin.exe opens an outgoing TCP connection to host "149.154.167.220:443".		

Mitre ATT&CK Matrix

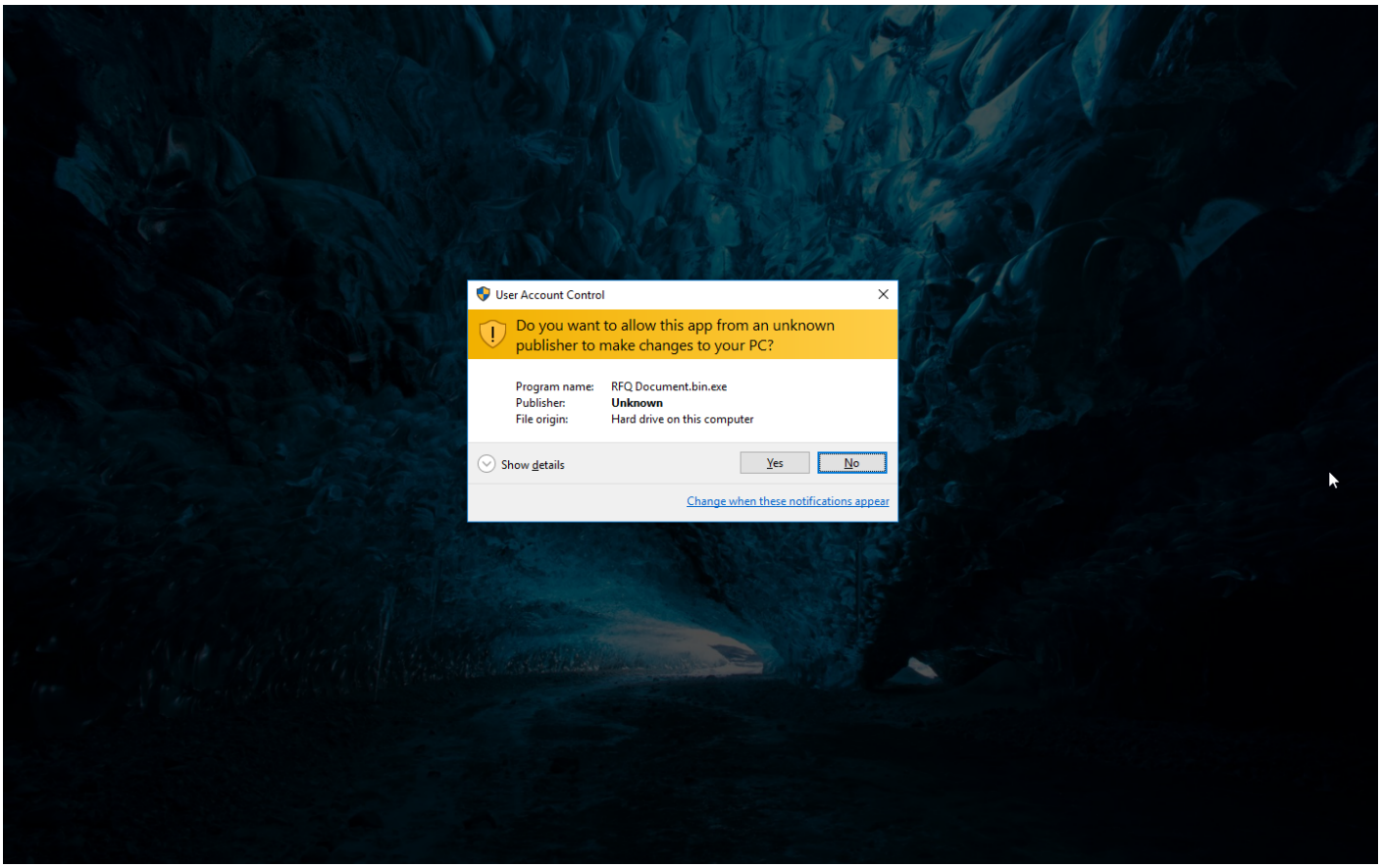
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1214 Credentials in Registry	#T1016 System Network Configuration Discovery		#T1119 Automated Collection			
				#T1045 Software Packing	#T1081 Credentials in Files	#T1012 Query Registry		#T1005 Data from Local System			
						#T1083 File and Directory Discovery					

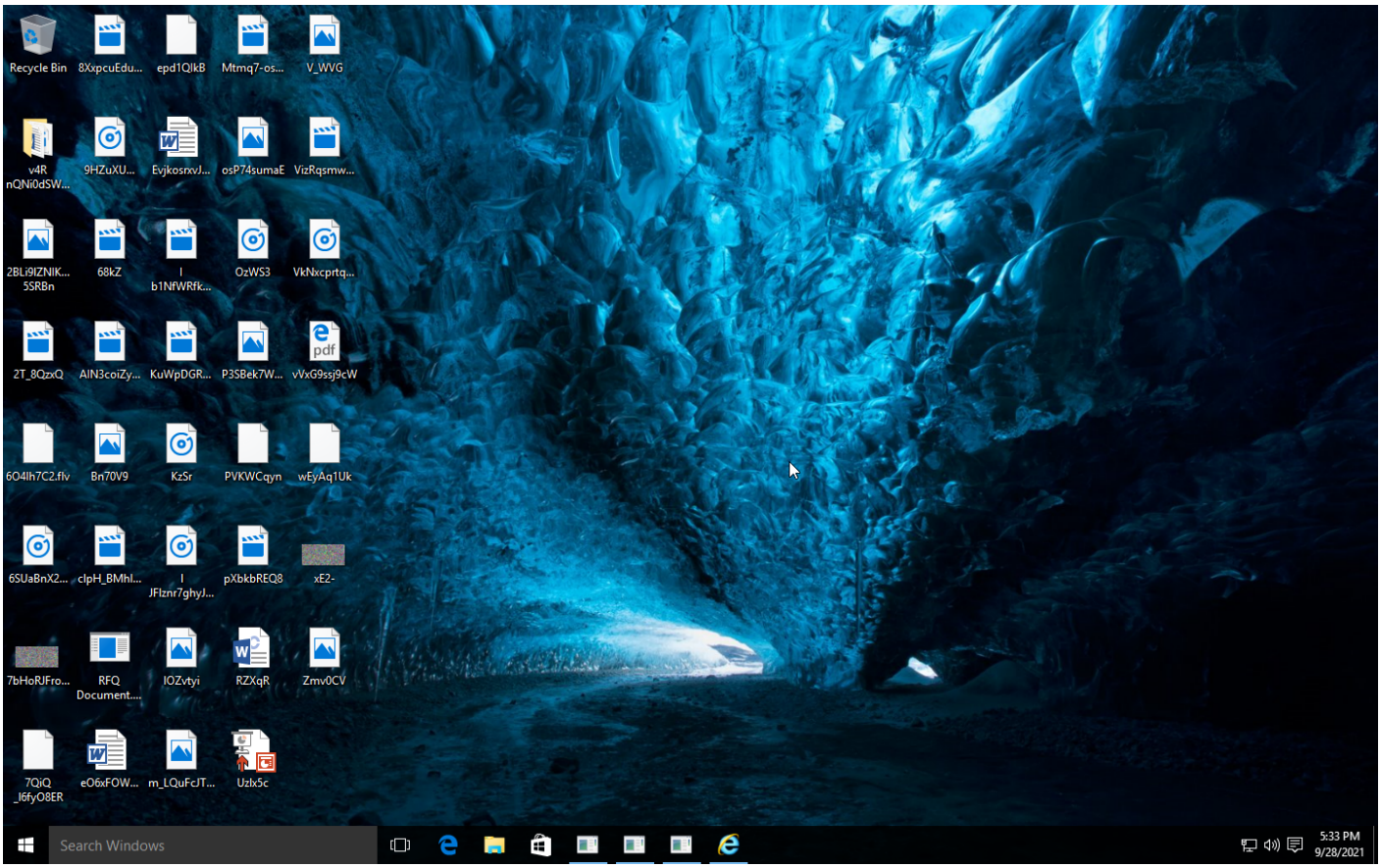
Sample Information

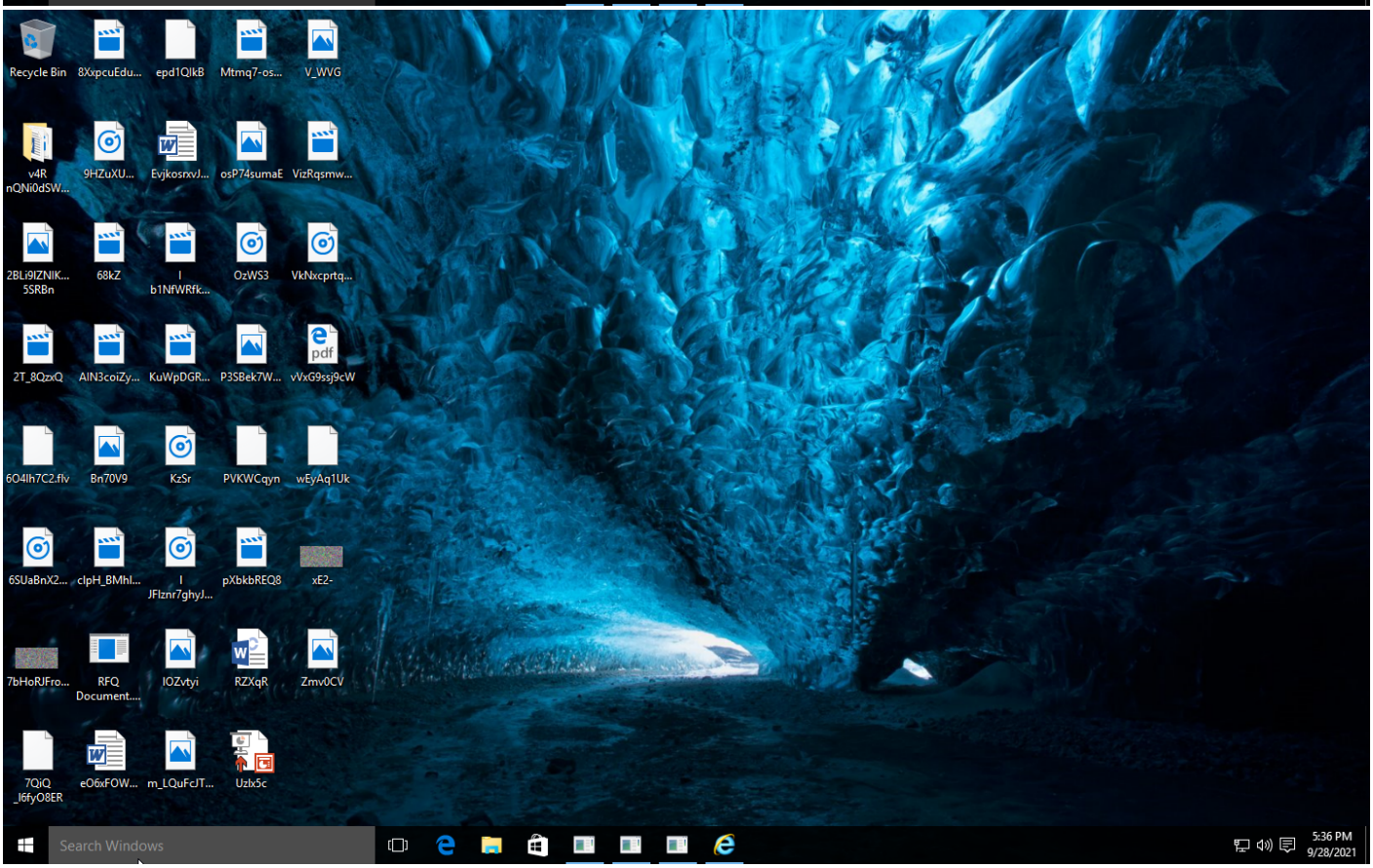
ID	#2784135
MD5	64468b2ab541687572ce6b435b41f2bd
SHA1	893ae234d351c762ab388a7337c625e4b213da6e
SHA256	d3ac98cf64ca2fca455b2e4f002c3381bcee699cf64bbfaa076222209f834b1a
SSDeep	6144:P8LxBkKFd08vwYfiEqj9LEW4AKkYMFO1UT489rSAZwghFmxGmf7qvce:BKFdLi1j9LEYKkNO1648JDwghFkFkce
ImpHash	b76363e9cb88bf9390860da8e50999d2
File Name	RFQ Document.bin.exe
File Size	336.75 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 19:32 (UTC+2)
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	2
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	8


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


Recycle Bin
8XxpcuEdu...
epd1QlkB
Mtmq7-os...
V_WVG
v4R nQNi0dSW...
9HZuXU...
EvjkosrxvJ...
osP74sumaE
VizRqsmw...
2BLi9IZNIK... 5SRBn
68kZ
I b1NfWRfk...
OzWS3
VkNxcprtq...
2T_8QzxQ
AIN3coiZy...
KuWpDGR...
P3SBek7W...
vVxG9ssj9cW
6O4lh7C2.flv
Bn70V9
KzSr
PVKWCqyn
wEyAq1Uk
6SUaBnX2...
clpH_BMhl...
I JFlznr7ghyJ...
pXbkbREQ8
xE2-
7bHoRJFro...
RFQ Document....
IOZvtyi
RZXqR
Zmv0CV
7QjQ_l6fyO8ER
eO6xFOW...
m_LQuFcJT...
Uzlx5c
Search Windows
5:33 PM
9/28/2021


Recycle Bin
8XxpcuEdu...
epd1QlkB
Mtmq7-os...
V_WVG
v4R nQNi0dSW...
9HZuXU...
EvjkosrxvJ...
osP74sumaE
VizRqsmw...
2BLi9IZNIK... 5SRBn
68kZ
I b1NfWRfk...
OzWS3
VkNxcprtq...
2T_8QzxQ
AIN3coiZy...
KuWpDGR...
P3SBek7W...
vVxG9ssj9cW
6O4lh7C2.flv
Bn70V9
KzSr
PVKWCqyn
wEyAq1Uk
6SUaBnX2...
clpH_BMhl...
I JFlznr7ghyJ...
pXbkbREQ8
xE2-
7bHoRJFro...
RFQ Document....
IOZvtyi
RZXqR
Zmv0CV
7QjQ_l6fyO8ER
eO6xFOW...
m_LQuFcJT...
Uzlx5c
Search Windows
5:36 PM
9/28/2021

NETWORK

General

36.32 KB total sent

53.97 KB total received

2 ports 80, 443

4 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

4 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

3 URLs contacted, 3 servers

4 sessions, 36.32 KB sent, 53.97 KB received

HTTP Requests

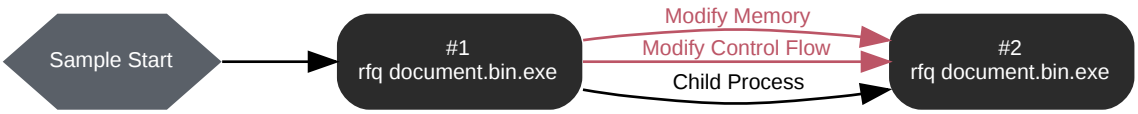
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://checkip.dyndns.org/	-	-		0 bytes	NA
GET	https://freegeoip.app/xml/88.153.199.169	-	-		0 bytes	NA
POST	https://api.telegram.org/bot1926537393:AAHGSUhtLeQU8qms_2blDH9qpvo-fEuwi9E/sendDocument	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	checkip.dyndns.org, checkip.dyndns.com	NoError	216.146.43.70, 216.146.43.71, 132.226.8.169, 193.122.130.0, 158.101.44.242, 193.122.6.168, 132.226.247.73	checkip.dyndns.com	NA
A	freegeoip.app	NoError	172.67.188.154, 104.21.19.200		NA
A	api.telegram.org	NoError	149.154.167.220		NA
-	checkip.dyndns.org	-	216.146.43.70, 216.146.43.71, 132.226.8.169, 158.101.44.242, 132.226.247.73, 193.122.130.0, 193.122.6.168		NA

BEHAVIOR

Process Graph



Process #1: rfq document.bin.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RFQ Document.bin.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 77017, Reason: Analysis Target
Unmonitor End Time	End Time: 126457, Reason: Terminated
Monitor duration	49.44s
Return Code	0
PID	4984
Parent PID	1600
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsb2DC0.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\trhfchm3wzuw7	284.00 KB	2180416e95180b0f3bc245ff4660ed8b6f6c3ad6014053c043c3ee487dd3be41	✗
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsb2DC0.tmp\tkwj.dll	47.50 KB	15aef55d8e9f0d4ad435e111dc346fdeb294a77ea06b8b053424b11c3cd6fbcd	✗

Host Behavior

Type	Count
System	57
Module	32
File	207
Process	1
-	3
-	9

Process #2: rfq document.bin.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RFQ Document.bin.exe"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 123854, Reason: Child Process
Unmonitor End Time	End Time: 323071, Reason: Terminated by Timeout
Monitor duration	199.22s
Return Code	Unknown
PID	3100
Parent PID	4984
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe	0x148	0x400000(4194304)	0x400	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe	0x148	0x401000(4198400)	0xac00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe	0x148	0x40c000(4243456)	0x5a00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe	0x148	0x412000(4268032)	0x800	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe	0x148	0x414000(4276224)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe	0x148	0x415000(4280320)	0x35c00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe	0x148	0x2a7008(2781192)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\rfq document.bin.exe	0x148 / 0xe9c	0x77968fe0(2006355936)	-	✓	1

Host Behavior

Type	Count
Module	32
File	125
System	27
Environment	12
User	49
Registry	75
-	16
Window	6

Network Behavior

Type	Count
HTTP	2
HTTPS	17
DNS	4
TCP	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d3ac98cf64ca2fca455b2e4f002c3381bcee699cf64bbfaa076222209f834b1a	C:\Users\RDhJ0CNFevzX\Desktop\RFQ Document.bin.exe	Sample File	336.75 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
15aef55d8e9f0d4ad435e111dc346fdeb294a77ea06b8b053424b11c3cd6fbcd	C:\Users\RDHJ0C~1\AppData\Local\Temp\nsb2DC0.tmp\tkwj.dll	Dropped File	47.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	MALICIOUS
2180416e95180b0f3bc245ff4660ed8b6f6c3ad6014053c043c3ee487dd3be41	C:\Users\RDHJ0C~1\AppData\Local\Temp\trhfchm3wzuw7	Dropped File	284.00 KB	application/octet-stream	Access, Write, Read, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsi2572.tmp	Accessed File	Access, Delete, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\RFQ Document.bin.exe	Sample File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsb2DC0.tmp	Accessed File	Access, Delete, Create	CLEAN
C:\Users	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Access, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\trhfchm3wzuw7	Dropped File	Access, Write, Read, Create	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsb2DC0.tmp\tkwj.dll	Dropped File	Access, Write, Create	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\RFQ Document.bin.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Default\Ya Login Data	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:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Nichrome\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Tencent\QQBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Default\Login Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Slimjet\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\GhostBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Xvast\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\SuperBird\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Browser\Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\UCBrowser\User Data_i18n\Default\UC Login Data.18	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Blisk\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera\Opera\profile\wand.dat	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\FileZilla\recentservers.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.purple\accounts.xml	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Liebao7\User Data\Default\EncryptedStorage	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\AVAST Software\Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kinza\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BlackHawk\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Default\Login Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome SxS\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\SalamWeb\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\discord\Local Storage\leveldb\	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://checkip.dyndns.org	-	216.146.43.70	-	GET	CLEAN
https://freegeoip.app/xml/88.153.199.169	-	172.67.188.154	-	GET	CLEAN
https://api.telegram.org/bot1926537393:AAHGSUhtLeQU8qms_2blDH9qpvo-fEuwi9E/sendDocument	-	149.154.167.220	-	POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
checkip.dyndns.org	193.122.6.168, 216.146.43.71, 216.146.43.70, 158.101.44.242, 132.226.247.73, 132.226.8.169, 193.122.130.0	-	HTTP, DNS	CLEAN
checkip.dyndns.com	216.146.43.70, 158.101.44.242, 193.122.6.168, 132.226.247.73, 132.226.8.169, 193.122.130.0, 216.146.43.71	-	DNS	CLEAN
freegeoip.app	104.21.19.200, 172.67.188.154	-	HTTPS, DNS	CLEAN
api.telegram.org	149.154.167.220	-	HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
216.146.43.70	checkip.dyndns.org, checkip.dyndns.com	United States	HTTP, DNS, TCP	CLEAN
172.67.188.154	freegeoip.app	United States	HTTPS, DNS, TCP	CLEAN
149.154.167.220	api.telegram.org	United Kingdom	HTTPS, DNS, TCP	CLEAN
216.146.43.71	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN
132.226.8.169	checkip.dyndns.org, checkip.dyndns.com	Japan	DNS	CLEAN
193.122.130.0	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
158.101.44.242	checkip.dyndns.org, checkip.dyndns.com	United States	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	CLEAN
104.21.19.200	freegeoip.app	-	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER	access	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	rfq document.bin.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	access, read	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Foxmail.url.mailto\Shell\open\command	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	rfq document.bin.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	rfq document.bin.exe	CLEAN

Process

Process Name	Commandline	Verdict
rfq document.bin.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RFQ Document.bin.exe"	MALICIOUS

YARA / AV

YARA (8)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	PhoenixKeylogger	Phoenix Keylogger	Memory Dump	-	Keylogger, Spyware	5/5
Malware	PhoenixKeylogger	Phoenix Keylogger	Memory Dump	-	Keylogger, Spyware	5/5
Malware	PhoenixKeylogger	Phoenix Keylogger	Memory Dump	-	Keylogger, Spyware	5/5
Malware	PhoenixKeylogger	Phoenix Keylogger	Memory Dump	-	Keylogger, Spyware	5/5
Malware	PhoenixKeylogger	Phoenix Keylogger	Memory Dump	-	Keylogger, Spyware	5/5
Malware	PhoenixKeylogger	Phoenix Keylogger	Memory Dump	-	Keylogger, Spyware	5/5
Malware	PhoenixKeylogger	Phoenix Keylogger	Memory Dump	-	Keylogger, Spyware	5/5
Malware	PhoenixKeylogger	Phoenix Keylogger	Function Strings	function_strings_process_2.txt	Keylogger, Spyware	5/5

Antivirus (2)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKD.37672864	C:\Users\RDhJ0CNFevzX\Desktop\RFQ Document.bin.exe	MALICIOUS
Memory Dump	DeepScan:Generic.MSIL.PasswordStealerA.D9D58869	-	MALICIOUS

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	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 13:44:31+00:00
Built-in AV Database Records	10482690

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