MALICIOUS

Classifications: Injector

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe**
ID	#3862173
MD5	7700a0d1b07e63f054a730fbf9156ef0
SHA1	6995f2e5f4544b3e99489364bccc56084198c61d
SHA256	99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770
File Size	4242.50 KB
Report Created	2022-03-21 15:15 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (21 rules, 29 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) 99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe modifies memory of (process #3) applaunch.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) 99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.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	Heuristics	Executable is signed with a revoked certificate	1	-
	• C:\Users\RDhJ0CNFevzX\Desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe is signed with a certificate of Nvidia Corporation that has been revoked.			
2/5	Discovery	Executes WMI query	4	-
	• (Process #3) applaunch.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #3) applaunch.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #3) applaunch.exe executes WMI query: Select * from Win32_ComputerSystem. • (Process #3) applaunch.exe executes WMI query: Select * From Win32_Process.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #3) applaunch.exe queries hardware properties via WMI.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #3) applaunch.exe reads the network adapters' addresses by API.			
2/5	Anti Analysis	Tries to detect application sandbox	3	-
	• (Process #3) applaunch.exe tries to detect "Sandboxie" by checking for existence of module "SbieDll.dll". • (Process #3) applaunch.exe tries to detect "AVAST Sandbox" by checking for existence of module "snxhk.dll". • (Process #3) applaunch.exe tries to detect "Comodo Sandbox" by checking for existence of module "cmdvrt32.dll".			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #3) applaunch.exe tries to detect a debugger via API "CheckRemoteDebuggerPresent".			
2/5	Discovery	Enumerates running processes	1	-
	• (Process #3) applaunch.exe enumerates running processes via WMI.			
2/5	Heuristics	Signed executable failed signature validation	1	-
	• C:\Users\RDhJ0CNFevzX\Desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe is signed, but signature validation failed.			
2/5	Reputation	Contacts known suspicious URL	2	-
	• (Process #3) applaunch.exe contacted known malicious URL "https://api.telegram.org/bot5183965885:AAHPcqaz1eLIs2BSjY2FjzIgl9pxizYDm4s/getMe". • Contacted URL "api.telegram.org" is a known suspicious URL.			

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe starts (process #3) applaunch.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe reads from (process #3) applaunch.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Mutex	Creates mutex	1	-
	• (Process #3) applaunch.exe creates mutex with name "9D16FBEF0D8A8F87529DE06A1C43C737".			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #3) applaunch.exe enables process privilege "SeDebugPrivilege".			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #3) applaunch.exe resolves host name "ip-api.com" to IP "208.95.112.1". • (Process #3) applaunch.exe resolves host name "api.telegram.org" to IP "149.154.167.220".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #3) applaunch.exe opens an outgoing TCP connection to host "208.95.112.1:80". • (Process #3) applaunch.exe opens an outgoing TCP connection to host "149.154.167.220:443".			
1/5	Crash	A monitored process crashed	1	-
	• (Process #3) applaunch.exe crashed.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #3) applaunch.exe resolves 49 API functions by name.			

Mitre ATT&CK Matrix

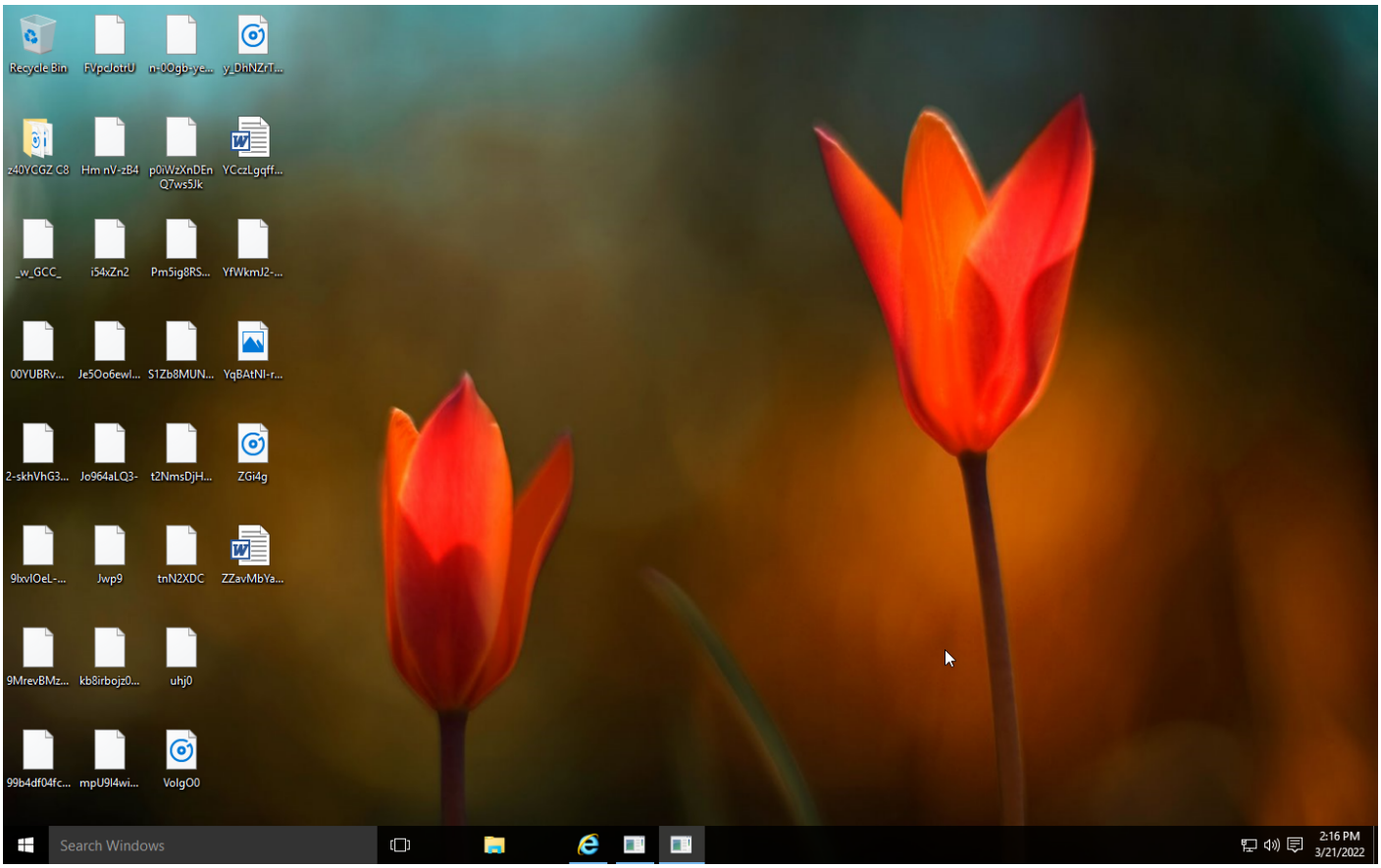
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window		#T1082 System Information Discovery					
				#T1045 Software Packing		#T1016 System Network Configuration Discovery					
				#T1497 Virtualization/ Sandbox Evasion		#T1497 Virtualization/ Sandbox Evasion					

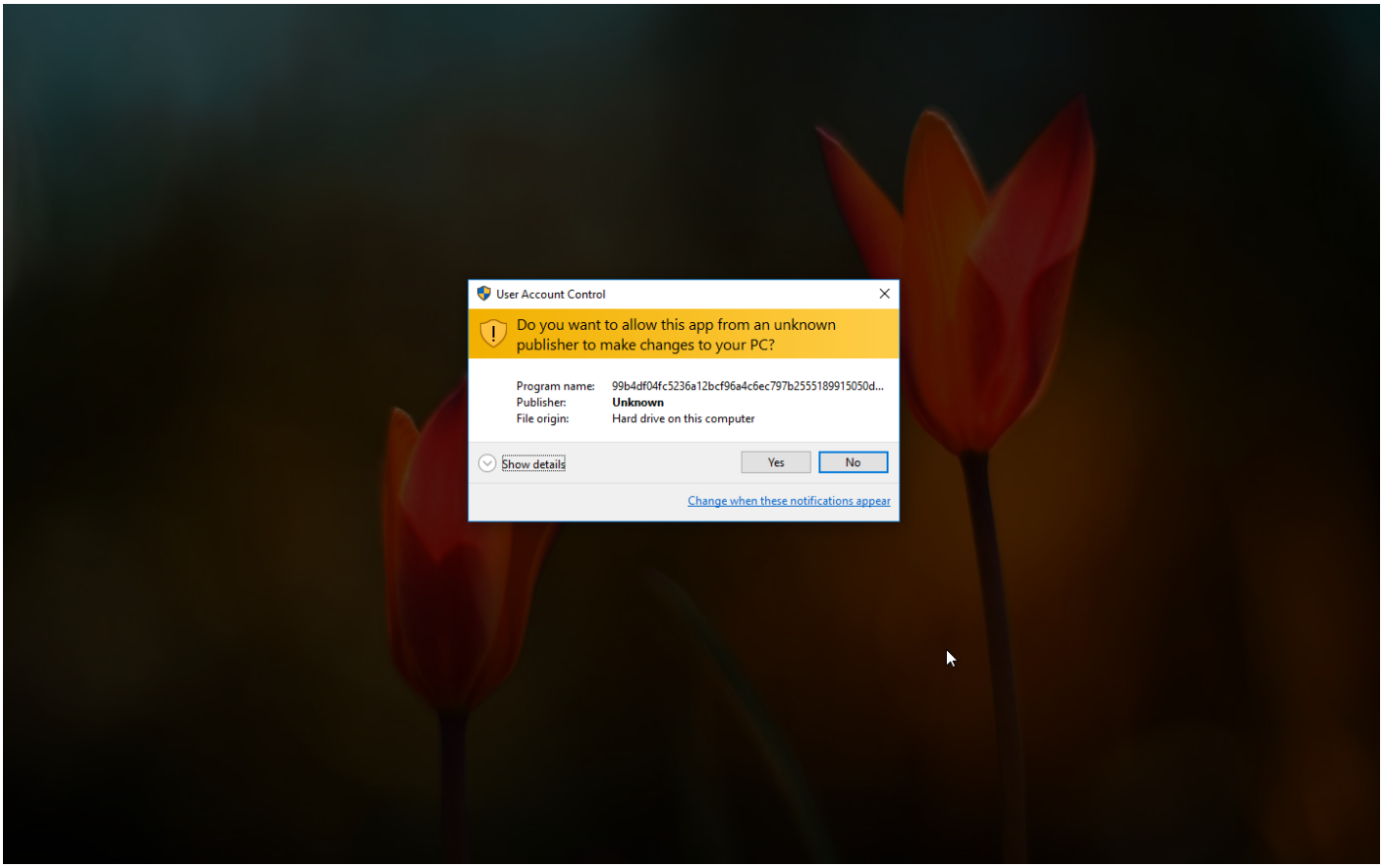
Sample Information

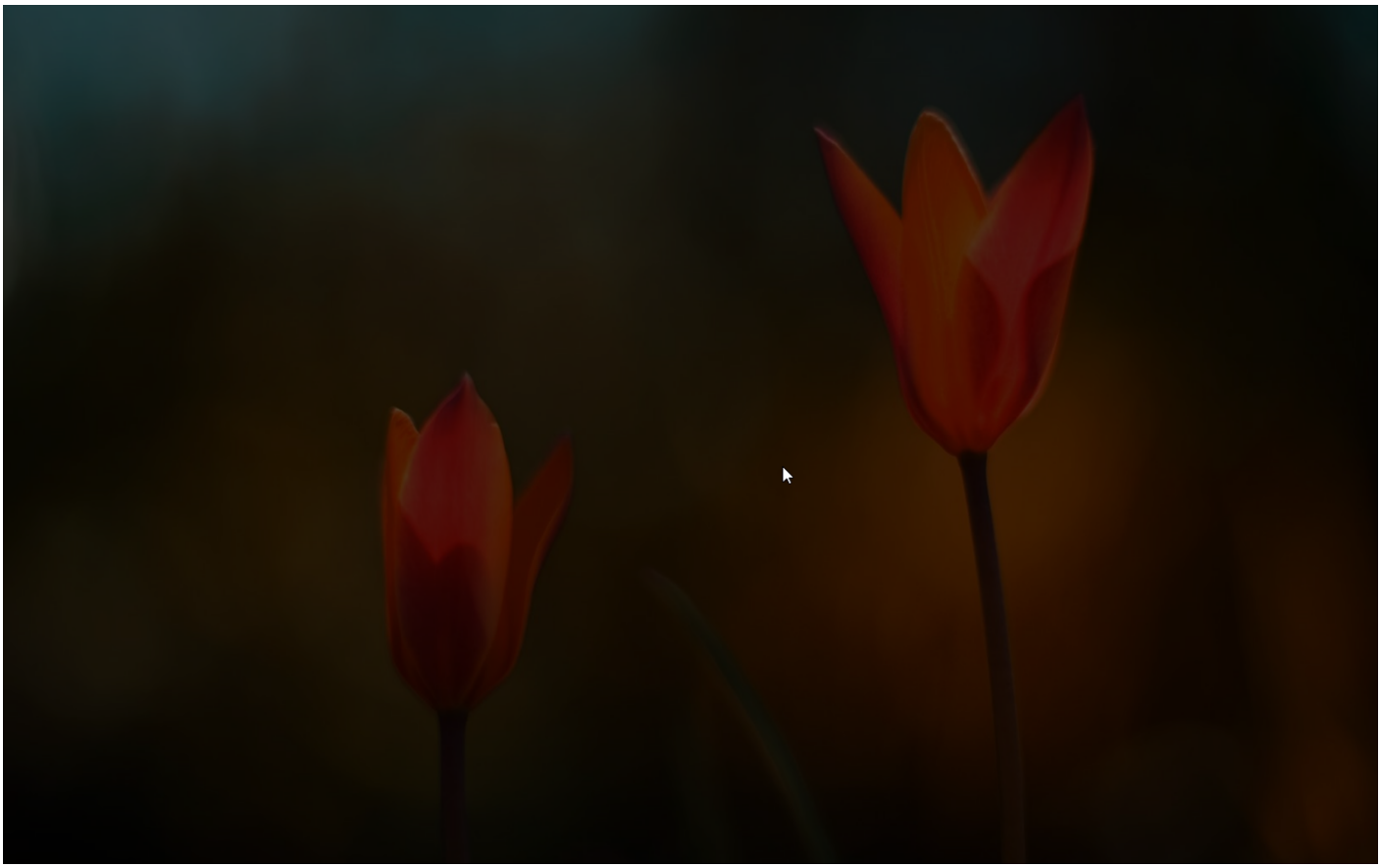
ID	#3862173
MD5	7700a0d1b07e63f054a730fbf9156ef0
SHA1	6995f2e5f4544b3e99489364bccc56084198c61d
SHA256	99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770
SSDeep	98304:IDWrdQJJ6qOobDtlLCSvKBXRAtiX2CVQmYRx6uiNnA9gEEtwPpAK3q2M:D6KPktlvIAtSNn6gFtYrzM
ImpHash	99c2cae0b7316add27de679470515124
File Name	99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe
File Size	4242.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

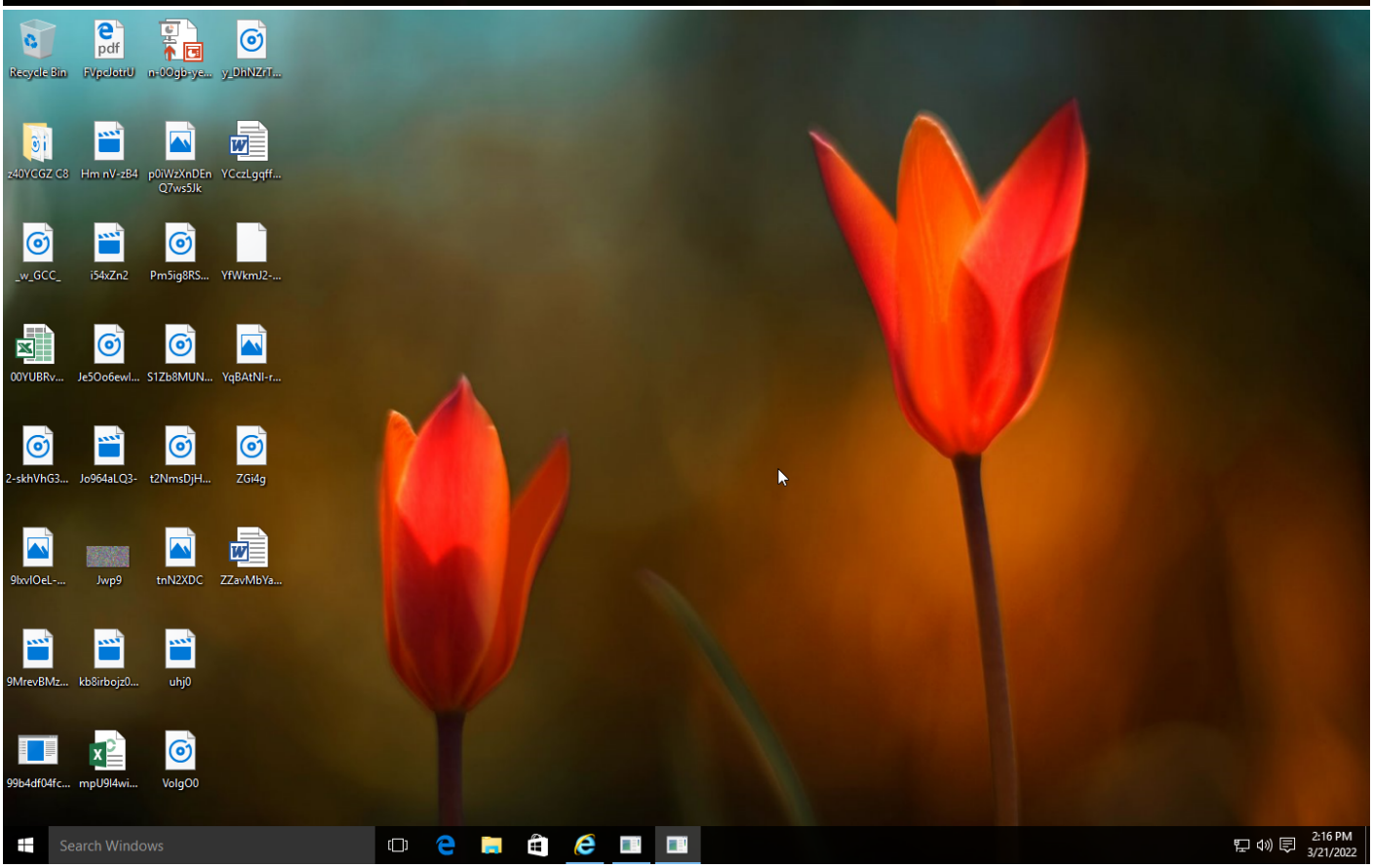
Analysis Information

Creation Time	2022-03-21 15:15 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
FVpcJotrU
n-0Ogb-ye...
y_DhNZrT...
z40YCGZ C8
Hm nV-zB4
p0iWzXnDEn Q7ws5Jk
YCczLgqff...
_w_GCC_
i54xZn2
Pm5ig8RS...
YfWkmJ2-...
00YUBRv...
Je5Oo6ewl...
S1Zb8MUN...
YqBAtNI-r...
2-skhVhG3...
Jo964aLQ3-
t2NmsDjH...
ZGi4g
9lxvlOeL-...
Jwp9
tnN2XDC
ZZavMbYa...
9MrevBMz...
kb8irbojz0...
uhj0
99b4df04fc...
mpU9l4wi...
VolgO0
Search Windows
2:16 PM
3/21/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 99b4df04fc5236a12bcf96a4c6ec797b2555189915050d...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

1.53 KB total sent

13.29 KB total received

2 ports 80, 443

3 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

2 sessions, 1.53 KB sent, 13.29 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://ip-api.com/line/?fields=hosting	-	-		0 bytes	NA
GET	https://api.telegram.org/bot5183965885:AAHPcqaz1eLIs2BSjY2FjzIgI9pxizYDm4s/getMe	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	ip-api.com	NoError	208.95.112.1		NA
A	api.telegram.org	NoError	149.154.167.220		NA

BEHAVIOR

Process Graph

Process #1: 99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 80651, Reason: Analysis Target
Unmonitor End Time	End Time: 111259, Reason: Terminated
Monitor duration	30.61s
Return Code	0
PID	5028
Parent PID	1184
Bitness	32 Bit

Host Behavior

Type	Count
Module	36
File	54
Environment	1
Process	1
-	3
-	8

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: 107853, Reason: Child Process
Unmonitor End Time	End Time: 201448, Reason: Crashed
Monitor duration	93.59s
Return Code	2148734499
PID	1908
Parent PID	5028
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe	0x13b4	0x400000(4194304)	0x92000	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe	0x13b4	0x331008(3346440)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe	0x13b4 / 0xc04	0x77798fe0(2004455392)	-	✓	1

Host Behavior

Type	Count
User	2
System	7
Registry	50
Module	63
-	137
COM	159
-	11
File	130
Mutex	2
Environment	8
-	1

Network Behavior

Type	Count
HTTP	1
HTTPS	1
DNS	2

Type	Count
TCP	2

Process #8: werfault.exe

ID	8
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 1908 -s 1864
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 184075, Reason: Child Process
Unmonitor End Time	End Time: 201307, Reason: Terminated
Monitor duration	17.23s
Return Code	0
PID	1312
Parent PID	1908
Bitness	32 Bit

Host Behavior

Type	Count
Module	69
Environment	21
File	3
Registry	30

Process #9: applaunch.exe

ID	9
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:\Windows\
Monitor Start Time	Start Time: 188287, Reason: Child Process
Unmonitor End Time	End Time: 201183, Reason: Terminated
Monitor duration	12.90s
Return Code	259
PID	5116
Parent PID	1908
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770	C:\Users\RDhJ0CNFevzX\Desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe	Sample File	4242.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe	Sample File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\2f89e0a0b985a2e55d1e4557151ce6ef	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.Config	Accessed File	Read, Access	CLEAN
C:\Windows\system32\winlogon.exe	Accessed File	Access	CLEAN
C:\Windows\system32\lsass.exe	Accessed File	Access	CLEAN
C:\Windows\system32\svchost.exe	Accessed File	Access	CLEAN
C:\Windows\system32\dwm.exe	Accessed File	Access	CLEAN
C:\Windows\System32\svchost.exe	Accessed File	Access	CLEAN
C:\Windows\System32\spoolsv.exe	Accessed File	Access	CLEAN
C:\Windows\system32\sihost.exe	Accessed File	Access	CLEAN
C:\Program Files\WindowsApps\Microsoft.Messaging_1.10.22012.0_x86__8wekyb3d8bbwe\SkypeHost.exe	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Windows\system32\taskhostw.exe	Accessed File	Access	CLEAN
C:\Windows\System32\RuntimeBroker.exe	Accessed File	Access	CLEAN
C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe	Accessed File	Access	CLEAN
C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\wmiprvse.exe	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender\return unit effort.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Journal\peopleemployeegive.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Windows NT\for-nature-want.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Media Player\issue-person.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Photo Viewer\somebody.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\there.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender\between-green-boy.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\surface.exe	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\landtoo.exe	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\as cut.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\without_official.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Media Player\though_chair.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\near she.exe	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\grow.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\newspapertheir.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Portable Devices\keep_education.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\save-total-official.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\3dftp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Photo Viewer\absolutetelnet.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Photo Viewer\alftp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\barca.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender\bitkinex.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows NT\coreftp.exe	Accessed File	Access	CLEAN
C:\Program Files\Uninstall Information\far.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Media Player\filezilla.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Mail\flashfxp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\fling.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\foxmailincmail.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\gmailnotifierpro.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\icq.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Media Player\leechftp.exe	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\ncftp.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Photo Viewer\notepad.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\MSBuild\operamail.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Photo Viewer\outlook.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\pidgin.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\scriptftp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft.NET\skype.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Windows NT\smartftp.exe	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\thunderbird.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\trillian.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\MSBuild\webdrive.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows NT\whatsapp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\winscp.exe	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\yahoomessenger.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\active-charge.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Multimedia Platform\accupos.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\afr38.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender\aldelo.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\ccv_server.exe	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\centralcreditcard.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Photo Viewer\creditservice.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Journal\edcsvr.exe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\fpos.exe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\isspos.exe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\mxslipstream.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Multimedia Platform\omnipos.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\spcwin.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Portable Devices\spgagentservice.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Multimedia Platform\utg2.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\accept.exe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\different_shot_from.exe	Accessed File	Access	CLEAN
C:\Windows\system32\backgroundTaskHost.exe	Accessed File	Access	CLEAN
C:\Windows\system32\msfeedssync.exe	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\2f89e0a0b985a2e55d1e4557151ce6ef\msgid.dat	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WerFault.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.telegram.org/bot5183965885:AAHPcqaz1eLIs2BSjY2FjzIgI9pxizYDm4s/getMe	-	149.154.167.220	-	GET	SUSPICIOUS
http://ip-api.com/line/?fields=hosting	-	208.95.112.1	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
api.telegram.org	149.154.167.220	-	DNS, HTTPS	SUSPICIOUS
ip-api.com	208.95.112.1	-	DNS, HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
208.95.112.1	ip-api.com	United States	DNS, TCP, HTTP	CLEAN
149.154.167.220	api.telegram.org	United Kingdom	DNS, TCP, HTTPS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
9D16FBEF0D8A8F87529DE06A1C43C737	access	applaunch.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\TZI	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST\FirstEntry	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST\LastEntry	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST\2010	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST\2011	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST\2012	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST\2013	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST\2014	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\Dynamic DST\2015	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\MUI_Display	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\MUI_Std	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\Russian Standard Time\MUI_Dlt	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework	access	werfault.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	werfault.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgDACSkipVerifyDlls	read, access	werfault.exe	CLEAN

Process

Process Name	Commandline	Verdict
99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe	"C:\Users\RDhJ0CNFevzX\Desktop\99b4df04fc5236a12bcf96a4c6ec797b2555189915050d7a0a1704f4f69ab770.exe"	MALICIOUS
applaunch.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"	SUSPICIOUS
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 1908 -s 1864	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

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

Platform Information

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

Software Information

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

System Information

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