MALICIOUS

Classifications: Spyware, Keylogger, Injector

Threat Names: Phoenix, Mal/Generic-S, Mal/HTMLGen-A, Trojan.GenericKD.37661679, DeepScan:Generic.MSIL.PasswordStealerA.84879DCB

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe**
ID	#968645
MD5	905f74fb158b50341e6dc710a60dad37
SHA1	b54645bb347a4c76d73f2ff0e46aa4bd9b010ae0
SHA256	e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335
File Size	11.50 KB
Report Created	2021-09-28 10:07 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (19 rules, 84 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	Keylogger, Spyware
	• Rule "PhoenixKeylogger" from ruleset "Malware" has matched on the function strings for (process #3) regasm.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Yandex Browser, Maple Studio, Opera, CentBrowser, CocCoc, 7Star, Amigo, Chromium, FileZilla, Chro... ...k, Torch, Epic Privacy Browser, Orbitum, Kometa, Vivaldi, Chedot, Comodo Dragon, Sputnik, Pidgin, Elements Browser, Google Chrome.			
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-
	• Built-in AV detected the sample itself as "Trojan.GenericKD.37661679". • Built-in AV detected "DeepScan:Generic.MSIL.PasswordStealerA.84879DCB" in the PCAP of the analysis. • Built-in AV detected "DeepScan:Generic.MSIL.PasswordStealerA.84879DCB" in the response data of URL "https://cdn.discordapp.com/attachments/889935662827044904/889981640498090054/runpe.pdf".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious URL	2	-
	• Reputation analysis labels the URL "https://cdn.discordapp.com/attachments/889615282304352289/890378116634144818/MMCHIA.exe" which was contacted by (process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://cdn.discordapp.com/attachments/889935662827044904/889981640498090054/runpe.pdf" which was contacted by (process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe as "Mal/HTMLGen-A".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe modifies memory of (process #3) regasm.exe.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #3) regasm.exe tries to read sensitive data of mail application "Microsoft Outlook" by registry.			
2/5	Data Collection	Reads sensitive browser data	20	-

Score	Category	Operation	Count	Classification
	• (Process #3) regasm.exe tries to read sensitive data of web browser "Yandex Browser" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Amigo" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Kometa" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Google Chrome" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "CocCoc" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Orbitum" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Vivaldi" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Chromium" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "CentBrowser" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Chedot" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Comodo Dragon" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Torch" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Opera" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Uran" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "7Star" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Chrome Canary" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Maple Studio" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Sputnik" by file. • (Process #3) regasm.exe tries to read sensitive data of web browser "Elements Browser" by file.		
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #3) regasm.exe tries to read sensitive data of ftp application "FileZilla" by file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #3) regasm.exe tries to read sensitive data of application "Pidgin" by file.			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe enables process privilege "SeDebugPrivilege". • (Process #3) regasm.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe starts (process #3) regasm.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe reads from (process #3) regasm.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.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	2	-
	• (Process #3) regasm.exe tries to gather information about application "FileZilla" by file. • (Process #3) regasm.exe tries to gather information about application "Pidgin" by file.			
1/5	Network Connection	Performs DNS request	4	-

Score	Category	Operation	Count	Classification
	• (Process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe resolves host name "cdn.discordapp.com" to IP "162.159.133.233". • (Process #3) regasm.exe resolves host name "checkip.dyndns.org" to IP "132.226.8.169". • (Process #3) regasm.exe resolves host name "freegeoip.app" to IP "172.67.188.154". • (Process #3) regasm.exe resolves host name "ftp.servicoscisi.shop" to IP "104.219.248.99".			
1/5	Network Connection	Connects to remote host	28	-
	• (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12098". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12068". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12041". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12031". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12099". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12045". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12095". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12108". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12110". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12059". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12096". • (Process #3) regasm.exe accepts an incoming TCP connection from host "104.219.248.99:12036". • (Process #1) e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe opens an outgoing TCP connection to host "162.159.133.233:443". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12098". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12068". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12041". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12031". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12099". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12045". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12095". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12108". • (Process #3) regasm.exe opens an outgoing TCP connection to host "132.226.8.169:80". • (Process #3) regasm.exe opens an outgoing TCP connection to host "172.67.188.154:443". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12110". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12059". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12096". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:21". • (Process #3) regasm.exe opens an outgoing TCP connection to host "104.219.248.99:12036".			
1/5	Network Connection	Tries to connect using an uncommon port	12	-
	• (Process #3) regasm.exe tries to connect to TCP port 12098 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12068 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12041 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12031 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12099 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12045 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12095 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12108 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12110 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12059 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12096 at 104.219.248.99. • (Process #3) regasm.exe tries to connect to TCP port 12036 at 104.219.248.99.			
1/5	Discovery	Checks external IP address	1	-

Score	Category	Operation	Count	Classification
	• (Process #3) regasm.exe checks external IP by asking IP info service at "http://checkip.dyndns.org/".			

Mitre ATT&CK Matrix

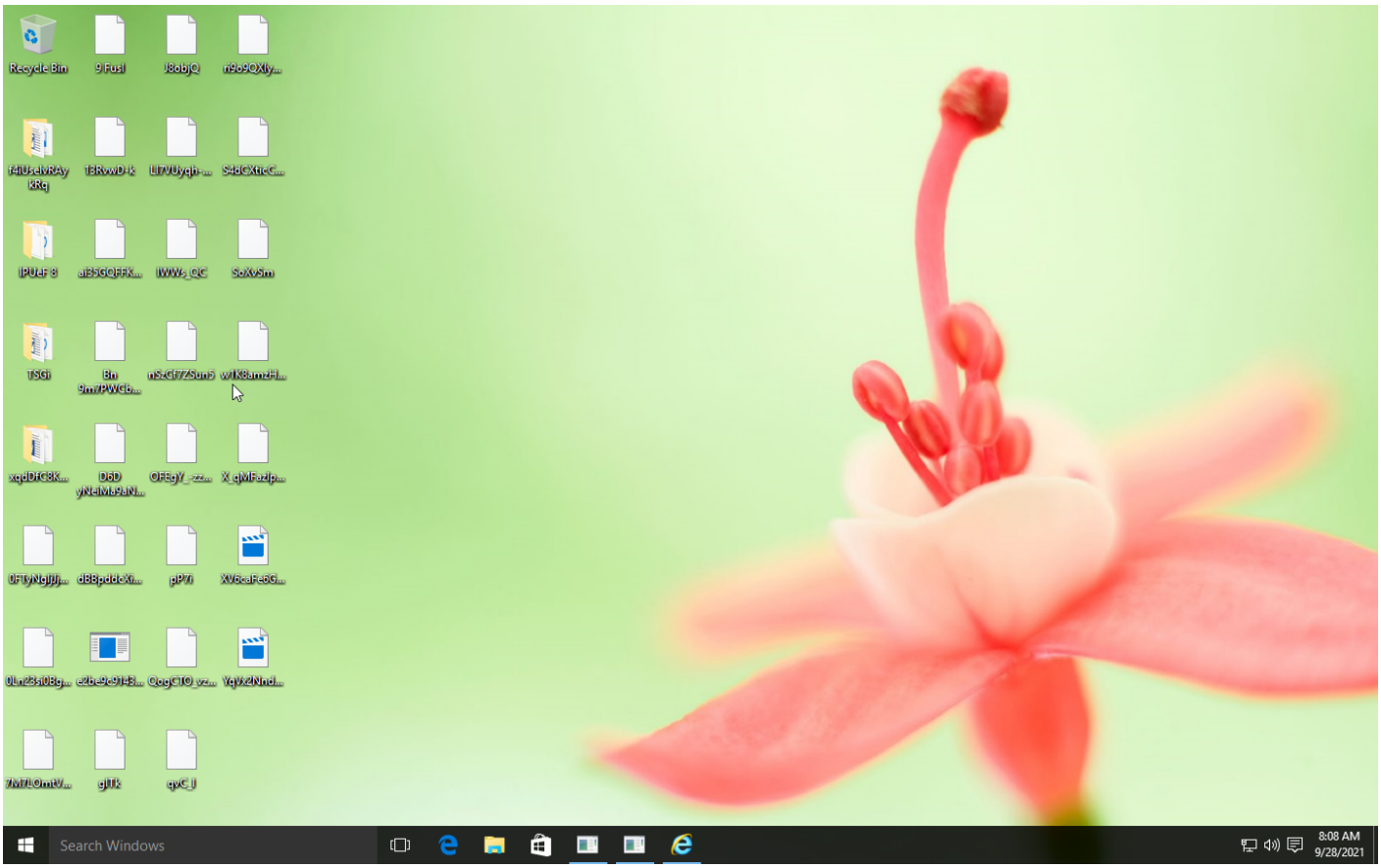
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1214 Credentials in Registry	#T1012 Query Registry		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1045 Software Packing	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1005 Data from Local System			
						#T1016 System Network Configuration Discovery					

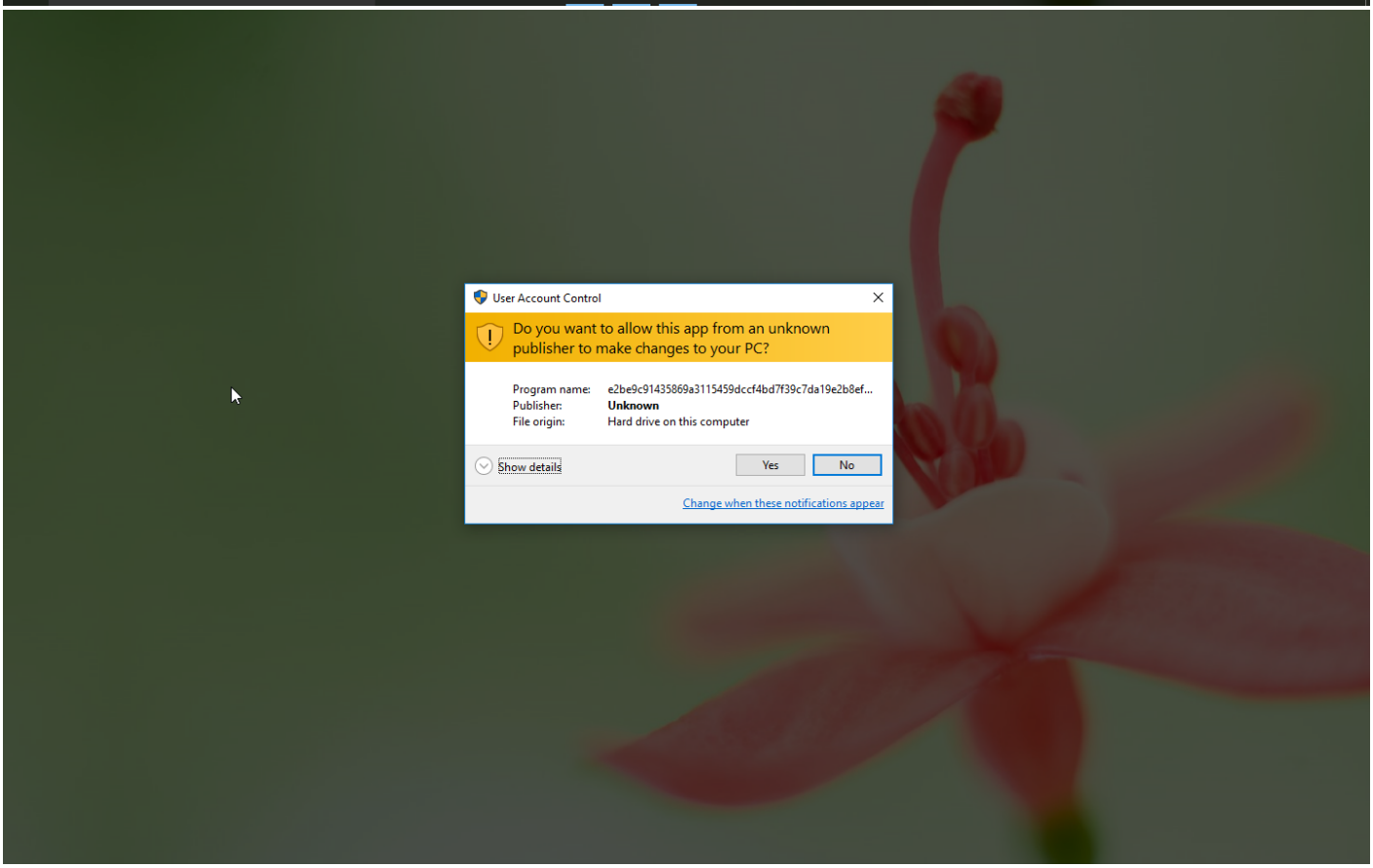
Sample Information

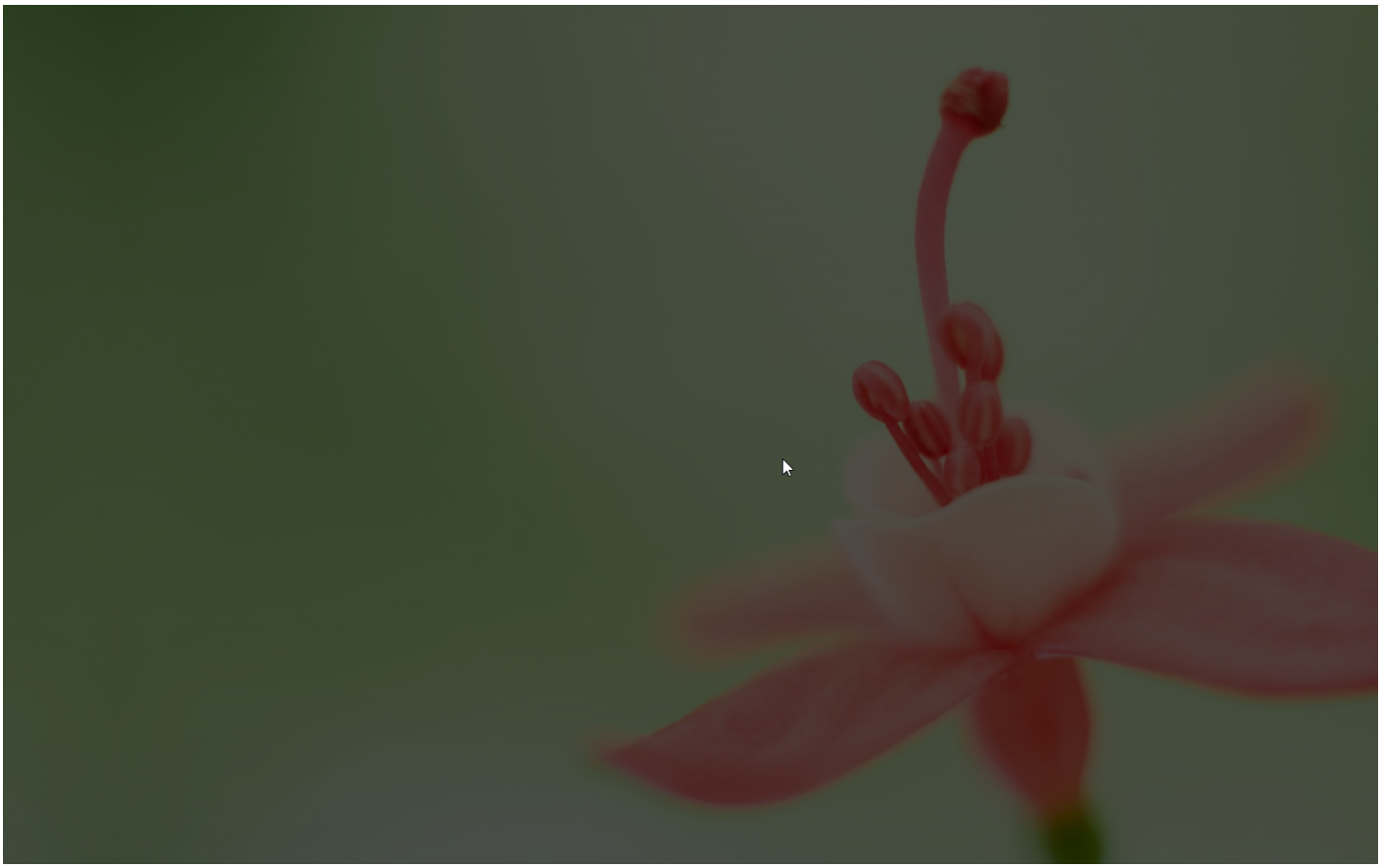
ID	#968645
MD5	905f74fb158b50341e6dc710a60dad37
SHA1	b54645bb347a4c76d73f2ff0e46aa4bd9b010ae0
SHA256	e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335
SSDeep	192:jLJh5u6VcVAgygoOwiigkHXw72Hkp/d3G2btK4Ji:xhzgygoOwiigwXwXp/dLtK4J
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe
File Size	11.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

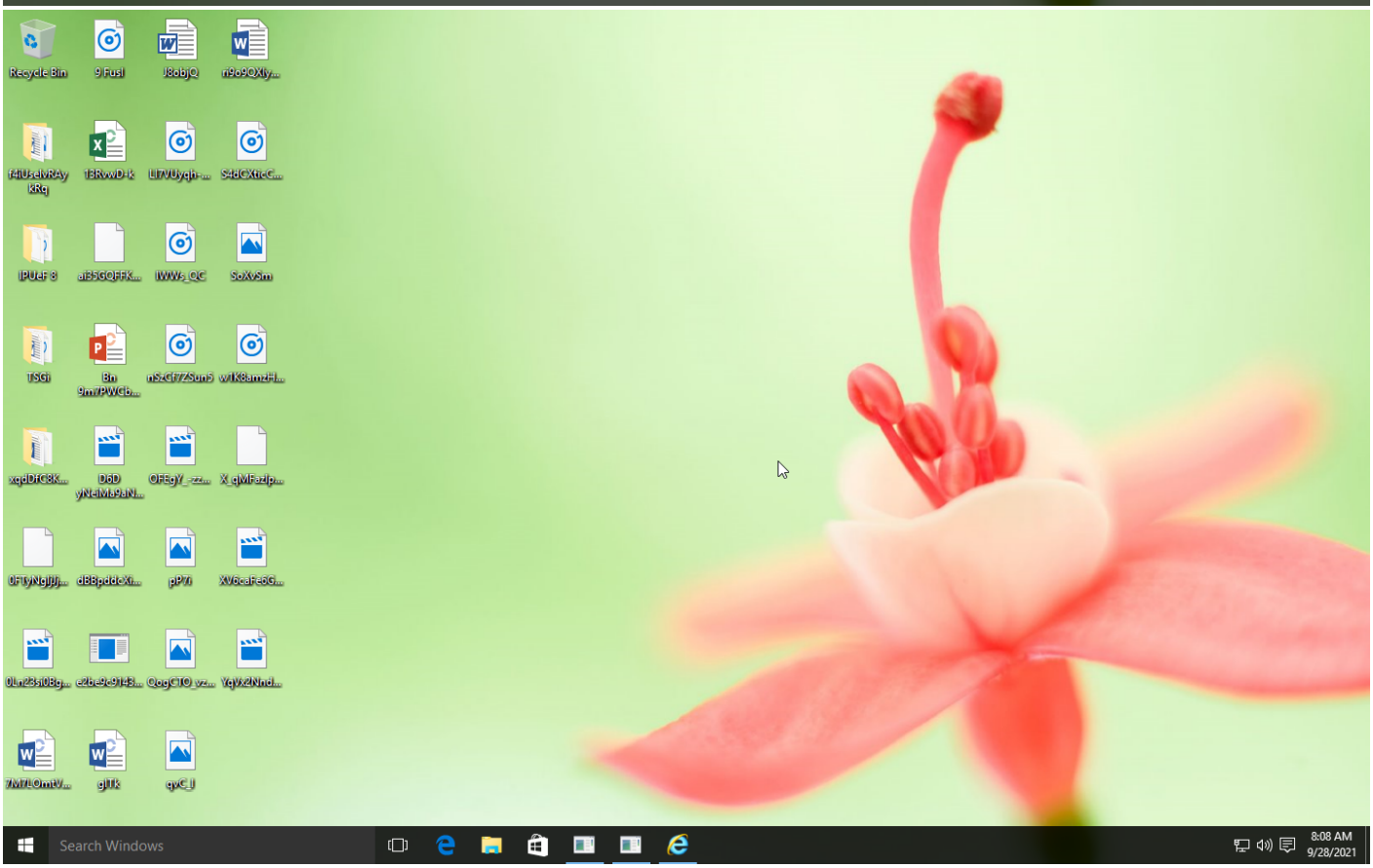
Analysis Information

Creation Time	2021-09-28 10:07 (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	1


Recycle Bin
Search Windows
8:08 AM
9/28/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

17.08 KB total sent

1114.82 KB total received

15 ports 12059, 12096, 12098, 12099, 12036, 12068, 12041, 12108, 12045, 12110, 80, 21, 12095, 443, 12031

5 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

5 DNS requests for 4 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 3 servers

3 sessions, 6.54 KB sent, 1109.90 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://cdn.discordapp.com/attachments/889615282304352289/890378116634144818/MMCHIA.exe	-	-		0 bytes	NA
GET	https://cdn.discordapp.com/attachments/889935662827044904/889981640498090054/runpe.pdf	-	-		0 bytes	NA
GET	https://freegeoip.app/xml/88.153.199.169	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	cdn.discordapp.com	NoError	162.159.133.233, 162.159.130.233, 162.159.129.233, 162.159.134.233, 162.159.135.233		NA
A	checkip.dyndns.org, checkip.dyndns.com	NoError	132.226.8.169, 216.146.43.71, 132.226.247.73, 193.122.6.168, 158.101.44.242, 216.146.43.70, 193.122.130.0	checkip.dyndns.com	NA
A	freegeoip.app	NoError	172.67.188.154, 104.21.19.200		NA
A	ftp.servicoscisi.shop	NoError	104.219.248.99		NA
-	checkip.dyndns.org	-	132.226.8.169, 216.146.43.71, 132.226.247.73, 158.101.44.242, 216.146.43.70, 193.122.6.168, 193.122.130.0		NA

BEHAVIOR

Process Graph

Process #1: e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 56973, Reason: Analysis Target
Unmonitor End Time	End Time: 107122, Reason: Terminated
Monitor duration	50.15s
Return Code	0
PID	5088
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Process	1
File	18
-	10
Registry	24
Environment	8
Module	791
User	1
-	3
-	7

Network Behavior

Type	Count
HTTPS	2
DNS	1
TCP	1

Process #3: regasm.exe

ID	3
File Name	c:\windows\microsoft.net\framework\v4.0.30319\regasm.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 104401, Reason: Child Process
Unmonitor End Time	End Time: 297062, Reason: Terminated by Timeout
Monitor duration	192.66s
Return Code	Unknown
PID	2804
Parent PID	5088
Bitness	32 Bit

Injection Information (5)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	0x13d8	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	0x13d8	0x402000(4202496)	0x1e600	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	0x13d8	0x422000(4333568)	0x1200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	0x13d8	0x424000(4341760)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	0x13d8	0x2ca008(2924552)	0x4	✓	1

Host Behavior

Type	Count
User	15
System	24
Registry	78
Module	13
File	128
-	17
Environment	11
Mutex	2
Window	6

Network Behavior

Type	Count
HTTP	2
HTTPS	1
DNS	4
TCP	17

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335	C:\Users\RDhJ0CNFevzX\Desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	Sample File	11.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	Sample File	Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSCOREE.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\KERNEL32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\KERNELBASE.dll	Accessed File	Access	CLEAN
C:\Windows\system32\apphelp.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ADVAPI32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\msvcrt.dll	Accessed File	Access	CLEAN
C:\Windows\system32\sechost.dll	Accessed File	Access	CLEAN
C:\Windows\system32\RPCRT4.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll	Accessed File	Access	CLEAN
C:\Windows\system32\SHLWAPI.dll	Accessed File	Access	CLEAN
C:\Windows\system32\combase.dll	Accessed File	Access	CLEAN
C:\Windows\system32\bcryptPrimitives.dll	Accessed File	Access	CLEAN
C:\Windows\system32\GDI32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\IMM32.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\kernel.appcore.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\VERSION.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MSVCR120_CLR0400.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\e24742a3939bece9db8105d99720b0e0\mscorlib.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ole32.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll	Accessed File	Access	CLEAN
C:\Windows\system32\OLEAUT32.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\cb0700ff6398b8e9d0d936cfc4894ba1\System.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\5290f26e6772518e2dd9d9c55bcc9a10\System.Core.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\7ad6bc6ee277d5eed690e8c1c9400ff7\System.Configuration.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\c0ce652aa04bc1fee99308a0a2ac79f8\System.Xml.ni.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\rasapi32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\rasman.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\rtutils.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ws2_32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\mswsock.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\winhttp.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ondemandconnroutehelper.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\IPHLPAPI.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\NSI.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\dhcpcsvc6.DLL	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\dhcpcsvc.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\shell32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\cfgmgr32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\windows.storage.dll	Accessed File	Access	CLEAN
C:\Windows\system32\shcore.dll	Accessed File	Access	CLEAN
C:\Windows\system32\powrprof.dll	Accessed File	Access	CLEAN
C:\Windows\system32\profapi.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\DNSAPI.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\WINNSI.DLL	Accessed File	Access	CLEAN
C:\Windows\System32\rasadhlp.dll	Accessed File	Access	CLEAN
C:\Windows\System32\fwpuclnt.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\secur32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\SSPICLI.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\schannel.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\CRYPT32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\MSASN1.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\mskeyprotect.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ncrypt.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\SYSTEM32\NTASN1.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ncryptsslp.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\07904e28a4042013cf2850aa829d512c\System.Drawing.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\b3ed3a5b3196c07e3a9165328654c5de\System.Windows.Forms.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\psapi.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml.Linq\be062827a780971b99602f86ad7eea06\System.Xml.Linq.ni.dll	Accessed File	Access	CLEAN
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\7884a60a278642bf6137c183790dfde3\Microsoft.VisualBasic.ni.dll	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\RegAsm.exe.Config	Accessed File	Read, 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
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

File Name	Category	Operations	Verdict
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
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

File Name	Category	Operations	Verdict
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
https://cdn.discordapp.com/attachments/889615282304352289/890378116634144818/MMCHIA.exe	-	162.159.133.233	-	GET	MALICIOUS
https://cdn.discordapp.com/attachments/889935662827044904/889981640498090054/runpe.pdf	-	162.159.133.233	-	GET	MALICIOUS
http://checkip.dyndns.org	-	132.226.8.169	-	GET	CLEAN
https://freegeoip.app/xml/88.153.199.169	-	172.67.188.154	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
cdn.discordapp.com	162.159.135.233, 162.159.129.233, 162.159.133.233, 162.159.134.233, 162.159.130.233	-	DNS, HTTPS	CLEAN
checkip.dyndns.org	216.146.43.70, 132.226.247.73, 158.101.44.242, 132.226.8.169, 216.146.43.71, 193.122.130.0, 193.122.6.168	-	DNS, HTTP	CLEAN
checkip.dyndns.com	216.146.43.71, 193.122.130.0, 216.146.43.70, 132.226.247.73, 158.101.44.242, 193.122.6.168, 132.226.8.169	-	DNS	CLEAN
freegeoip.app	104.21.19.200, 172.67.188.154	-	DNS, HTTPS	CLEAN
ftp.servicoscisi.shop	104.219.248.99	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
162.159.133.233	cdn.discordapp.com	-	DNS, HTTPS, TCP	CLEAN
104.219.248.99	ftp.servicoscisi.shop	United States	DNS, TCP	CLEAN
132.226.8.169	checkip.dyndns.org, checkip.dyndns.com	Japan	DNS, HTTP, TCP	CLEAN
172.67.188.154	freegeoip.app	United States	DNS, HTTPS, TCP	CLEAN
162.159.130.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.129.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.134.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.135.233	cdn.discordapp.com	-	DNS	CLEAN
216.146.43.71	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN
132.226.247.73	checkip.dyndns.org, checkip.dyndns.com	Brazil	DNS	CLEAN
193.122.6.168	checkip.dyndns.org, checkip.dyndns.com	Germany	DNS	CLEAN
158.101.44.242	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN
216.146.43.70	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN
193.122.130.0	checkip.dyndns.org, checkip.dyndns.com	United States	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
104.21.19.200	freegeoip.app	-	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_CURRENT_USER	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Connections	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Connections	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows \CurrentVersion\Internet Settings	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\ LegacyWPADSupport	read, access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\ v4.0.30319	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\ v4.0.30319\HWRPortReuseOnSocketBind	read, access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\ AppContext	access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\ v4.0.30319\SchUseStrongCrypto	read, access	regasm.exe, e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender	access	regasm.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware	write, read, access	regasm.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676	access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password	read, access	regasm.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password	read, access	regasm.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Foxmail.url.mailto\Shell\open\command	access	regasm.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	regasm.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	regasm.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	regasm.exe	CLEAN

Process

Process Name	Commandline	Verdict
e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	"C:\Users\RDhJ0CNFevzX\Desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe"	MALICIOUS
regasm.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	SUSPICIOUS

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	PhoenixKeylogger	Phoenix Keylogger	Function Strings	function_strings_process_3.txt	Keylogger, Spyware	5/5

Antivirus (2)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKD.37661679	C:\Users\RDhJ0CNFevzX\Desktop\e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335.exe	MALICIOUS
Web Request	DeepScan:Generic.MSIL.PasswordStealerA.84879DCB	-	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 01:56:46+00:00
Built-in AV Database Records	10476967

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