MALICIOUS

Classifications: Injector, Spyware

Threat Names: Mal/Generic-S, Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe**
ID	#3199310
MD5	7de3896baf12500f3e1cd311e2340806
SHA1	500b906981aaa4810848643f1d8c17efa87bad20
SHA256	213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e
File Size	4294.00 KB
Report Created	2021-12-29 10:38 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (35 rules, 75 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: Exodus Cryptocurrency Wallet, Electrum Bitcoin Wallet, Internet Explorer / Edge, Cyberfox, Mozilla Thunderbird, Total Commander, k-Meleon, Comodo IceDragon, The Bat!, Opera, Mozilla Firefox.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S". • Reputation analysis labels file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\build.exe" as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "https://cdn.discordapp.com/attachments/919960898020466752/924051735893377094/vvzz67_build.exe" which was contacted by (process #2) applaunch.exe as "Mal/HTMLGen-A".			
4/5	Injection	Writes into the memory of another process	5	Injector
	• (Process #1) 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe modifies memory of (process #2) applaunch.exe. • (Process #6) build.exe modifies memory of (process #8) explorer.exe. • (Process #6) build.exe modifies memory of (process #9) bfsvc.exe. • (Process #11) reghost.exe modifies memory of (process #13) explorer.exe. • (Process #11) reghost.exe modifies memory of (process #14) bfsvc.exe.			
4/5	Injection	Modifies control flow of another process	5	-
	• (Process #1) 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe alters context of (process #2) applaunch.exe. • (Process #6) build.exe alters context of (process #8) explorer.exe. • (Process #6) build.exe alters context of (process #9) bfsvc.exe. • (Process #11) reghost.exe alters context of (process #13) explorer.exe. • (Process #11) reghost.exe alters context of (process #14) bfsvc.exe.			
3/5	Data Collection	Reads cryptocurrency wallet locations	2	-
	• (Process #2) applaunch.exe tries to read the cryptocurrency wallet "Electrum Bitcoin Wallet" for "BTC". • (Process #2) applaunch.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet".			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #2) applaunch.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntivirusProduct".			
3/5	Defense Evasion	Tries to detect the presence of anti-spyware software	1	-
	• (Process #2) applaunch.exe tries to detect anti-spyware software via WMI query: "SELECT * FROM AntiSpyWareProduct".			
3/5	Defense Evasion	Tries to detect the presence of firewall software	1	-
	• (Process #2) applaunch.exe tries to detect firewall via WMI query: "SELECT * FROM FirewallProduct".			
3/5	Anti Analysis	Tries to evade debugger	1	-
	• (Process #6) build.exe hides thread via API "NtSetInformationThread".			
2/5	Discovery	Executes WMI query	8	-

Score	Category	Operation	Count	Classification
		• (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM AntivirusProduct. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM AntiSpyWareProduct. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM FirewallProduct. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_OperatingSystem. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_Process Where SessionId='1'.		
2/5	Discovery	Collects hardware properties	1	-
		• (Process #2) applaunch.exe queries hardware properties via WMI.		
2/5	Data Collection	Reads sensitive ftp data	1	-
		• (Process #2) applaunch.exe tries to read sensitive data of ftp application "Total Commander" by file.		
2/5	Data Collection	Reads sensitive mail data	2	-
		• (Process #2) applaunch.exe tries to read sensitive data of mail application "The Bat!" by file. • (Process #2) applaunch.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file.		
2/5	Data Collection	Reads sensitive browser data	8	-
		• (Process #2) applaunch.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #2) applaunch.exe tries to read sensitive data of web browser "Opera" by file. • (Process #2) applaunch.exe tries to read sensitive data of web browser "Mozilla Firefox" by file. • (Process #2) applaunch.exe tries to read sensitive data of web browser "k-Meleon" by file. • (Process #2) applaunch.exe tries to read sensitive data of web browser "Comodo IceDragon" by file. • (Process #2) applaunch.exe tries to read sensitive data of web browser "Cyberfox" by file. • (Process #6) build.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #11) reghost.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.		
2/5	Discovery	Queries OS version via WMI	1	-
		• (Process #2) applaunch.exe queries OS version via WMI.		
2/5	Discovery	Enumerates running processes	3	-
		• (Process #2) applaunch.exe enumerates running processes via WMI. • (Process #8) explorer.exe enumerates running processes. • (Process #13) explorer.exe enumerates running processes.		
2/5	Discovery	Reads network adapter information	1	-
		• (Process #2) applaunch.exe reads the network adapters' addresses by API.		
2/5	Defense Evasion	Sends control codes to connected devices	2	-
		• (Process #6) build.exe controls device "\\.\C:" through API DeviceIOControl. • (Process #11) reghost.exe controls device "\\.\C:" through API DeviceIOControl.		
2/5	Anti Analysis	Tries to detect virtual machine	1	-
		• (Process #1) 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe is possibly trying to detect a VM via rdtsc.		
2/5	Masquerade	Creates a new process from a system binary	1	-

Score	Category	Operation	Count	Classification
	• (Process #6) build.exe creates a new explorer.exe process.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	1	-
	• (Process #1) 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe makes a direct system call to "NtProtectVirtualMemory".			
1/5	Hide Tracks	Creates process with hidden window	5	-
	• (Process #1) 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe starts (process #2) applaunch.exe with a hidden window. • (Process #6) build.exe starts (process #8) explorer.exe with a hidden window. • (Process #6) build.exe starts (process #9) bfsvc.exe with a hidden window. • (Process #11) reghost.exe starts (process #13) explorer.exe with a hidden window. • (Process #11) reghost.exe starts (process #14) bfsvc.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe reads from (process #2) applaunch.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	3	-
	• (Process #1) 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #6) build.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #11) reghost.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	1	-
	• (Process #2) applaunch.exe tries to gather information about application "Steam" by registry.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #2) applaunch.exe enables process privilege "SeDebugPrivilege".			
1/5	Persistence	Installs system startup script or application	2	-
	• (Process #6) build.exe adds "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\RegHost.exe" to Windows startup via registry. • (Process #11) reghost.exe adds "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\RegHost.exe" to Windows startup via registry.			
1/5	Execution	Drops PE file	1	-
	• (Process #2) applaunch.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\build.exe".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\build.exe".			
1/5	Obfuscation	Resolves API functions dynamically	5	-
	• (Process #1) 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe resolves 213 API functions by name. • (Process #2) applaunch.exe resolves 52 API functions by name. • (Process #6) build.exe resolves 478 API functions by name. • (Process #9) bfsvc.exe resolves 47 API functions by name. • (Process #11) reghost.exe resolves 478 API functions by name.			
1/5	Obfuscation	The binary file was created with a packer	1	-
	• File "C:\Users\RDhJ0CNFevzX\Desktop\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe" is packed with "ASProtect v1.23 RC1".			
1/5	Network Connection	Performs DNS request	1	-

Score	Category	Operation	Count	Classification
	• (Process #2) applaunch.exe resolves host name "cdn.discordapp.com" to IP "162.159.135.233".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #2) applaunch.exe opens an outgoing TCP connection to host "162.159.135.233:443". • (Process #2) applaunch.exe opens an outgoing TCP connection to host "103.246.144.29:44301".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) applaunch.exe tries to connect to TCP port 44301 at 103.246.144.29.			

Mitre ATT&CK Matrix

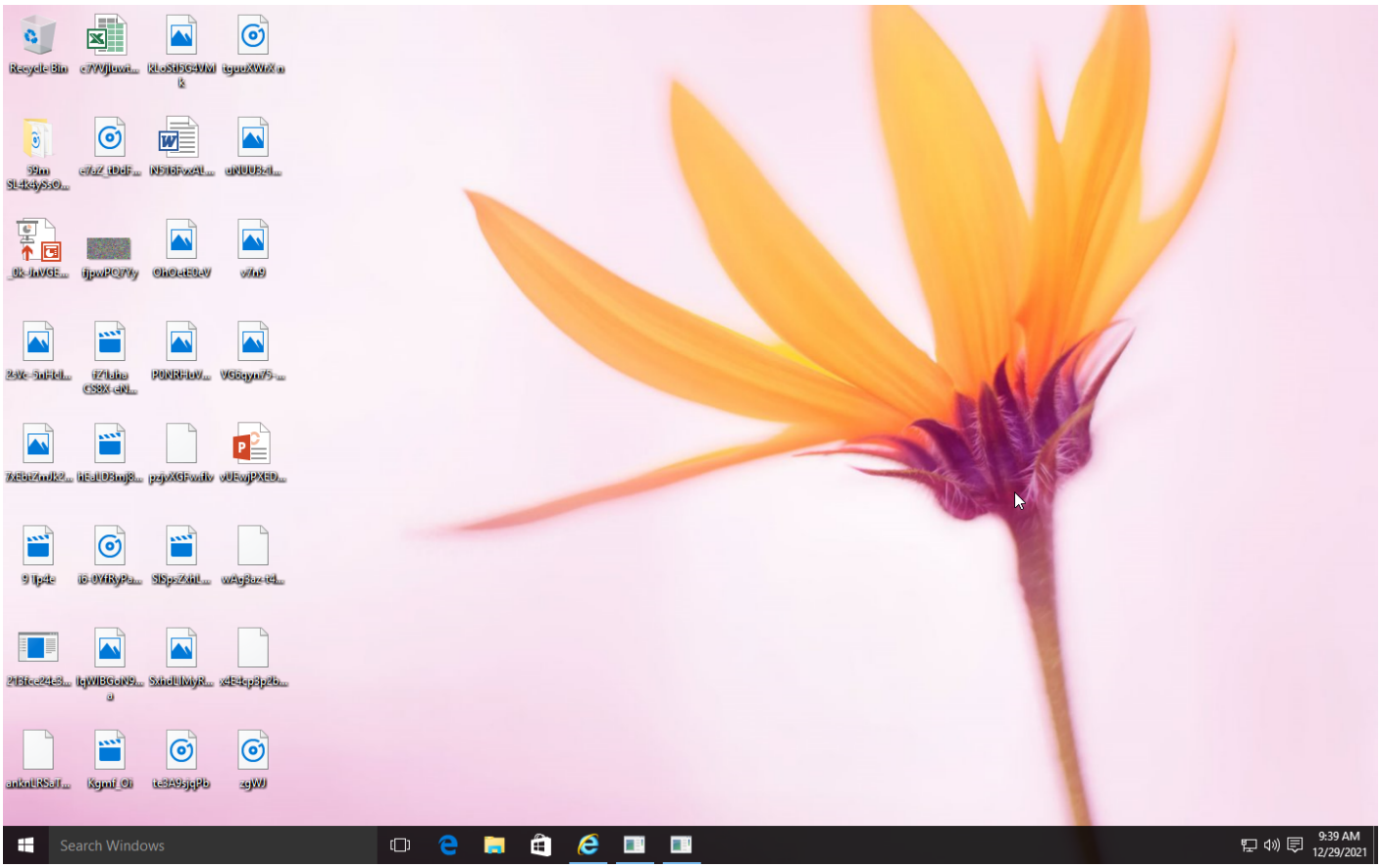
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		
				#T1045 Software Packing		#T1083 File and Directory Discovery		#T1005 Data from Local System			
				#T1112 Modify Registry		#T1063 Security Software Discovery					
				#T1497 Virtualization/ Sandbox Evasion		#T1012 Query Registry					
				#T1027 Obfuscated Files or Information		#T1016 System Network Configuration Discovery					
						#T1057 Process Discovery					
						#T1497 Virtualization/ Sandbox Evasion					
						#T1124 System Time Discovery					

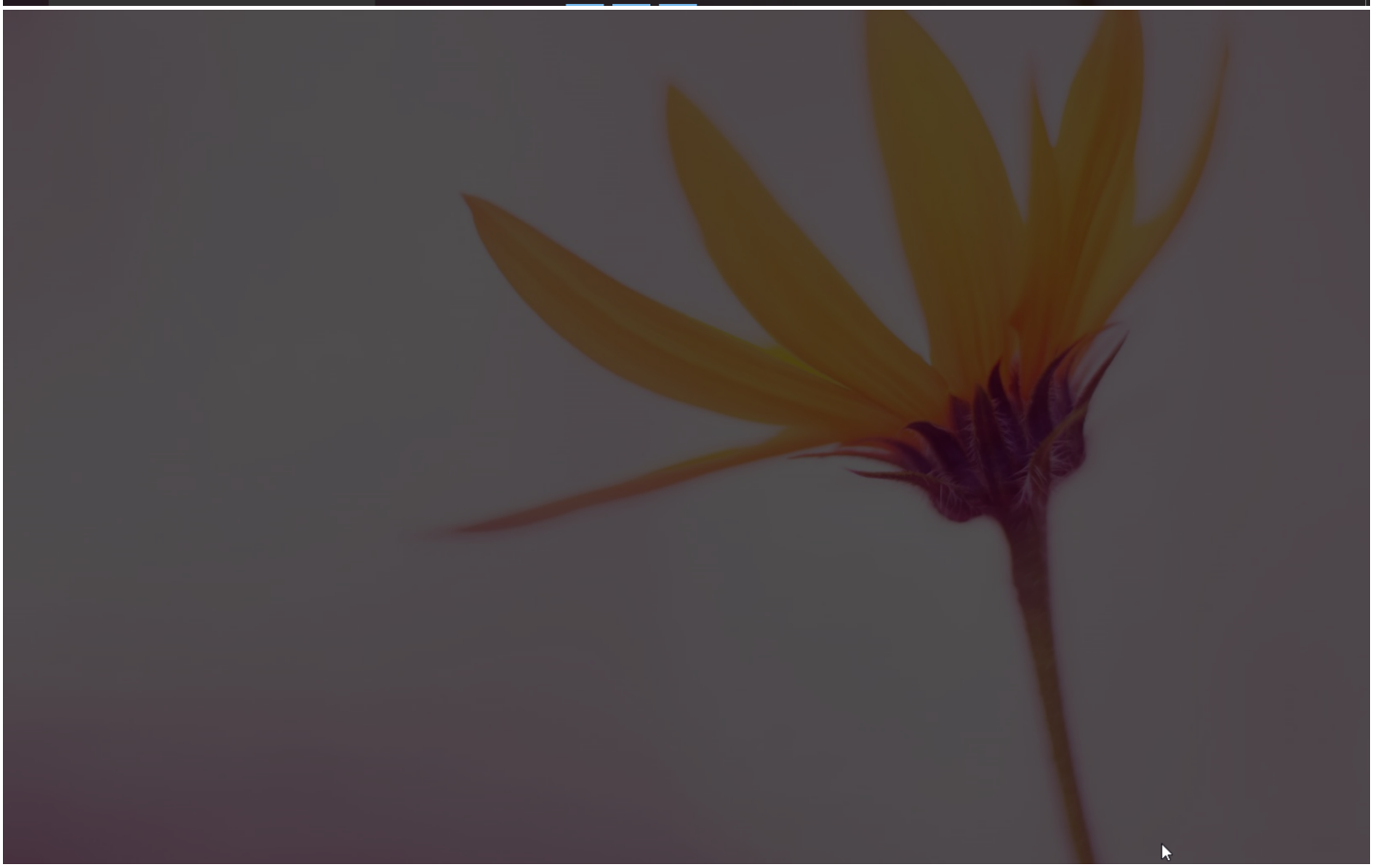
Sample Information

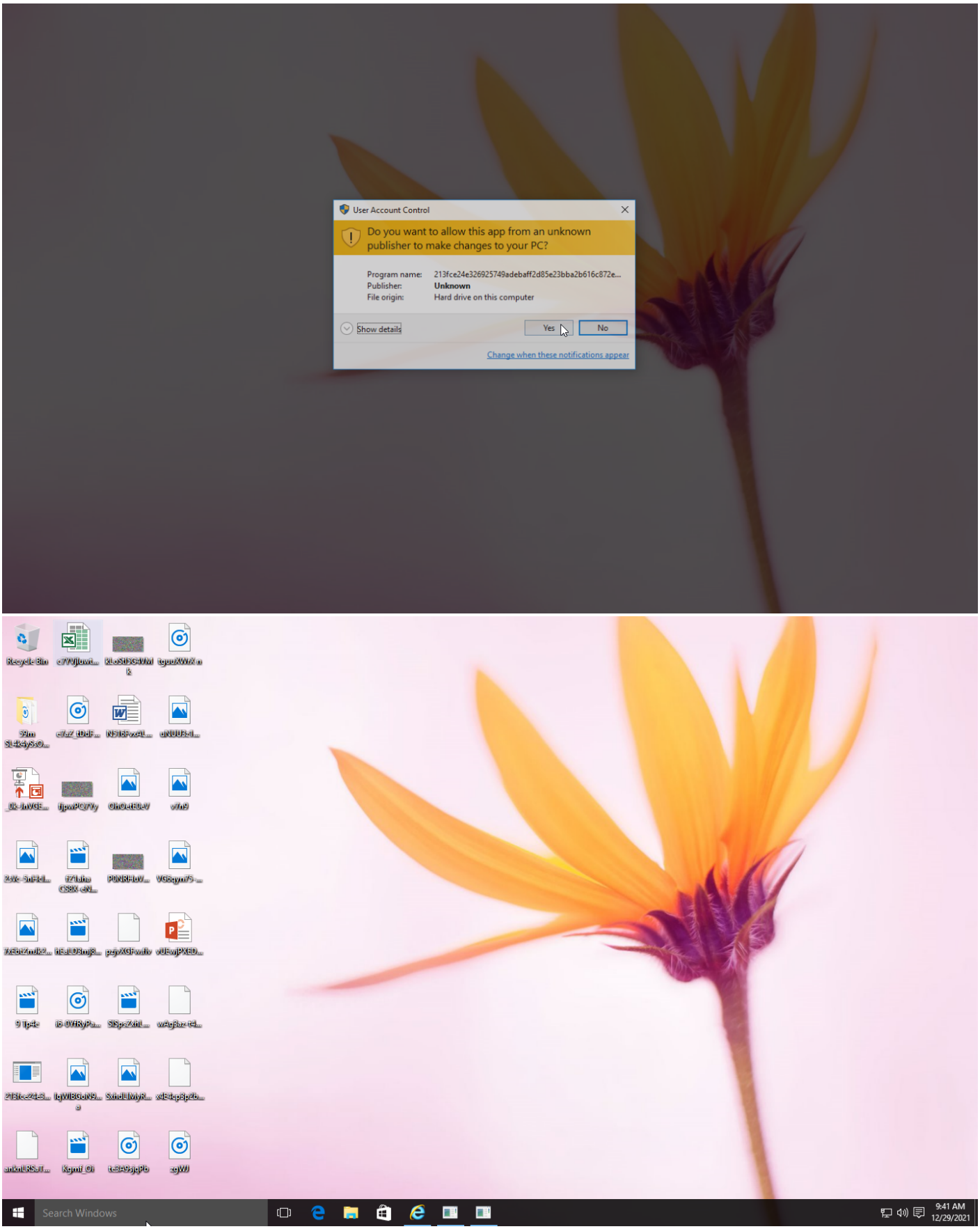
ID	#3199310
MD5	7de3896baf12500f3e1cd311e2340806
SHA1	500b906981aaa4810848643f1d8c17efa87bad20
SHA256	213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e
SSDeep	98304:xmAM03cGX50EXFEACRwiGbJ3hjOQxsaS3XnLUBzEydzEI:xBM03c+0ACRZGNBdONXe5
ImpHash	9a4258c5d218cf6e5c500e8415d5f5ed
File Name	213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe
File Size	4294.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-12-29 10:38 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	8
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Search Windows
9:39 AM
12/29/2021





Screenshots truncated

NETWORK

General

1204.33 KB total sent

9410.95 KB total received

2 ports 443, 44301

3 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 32.11 KB sent, 9403.43 KB received

HTTP Requests

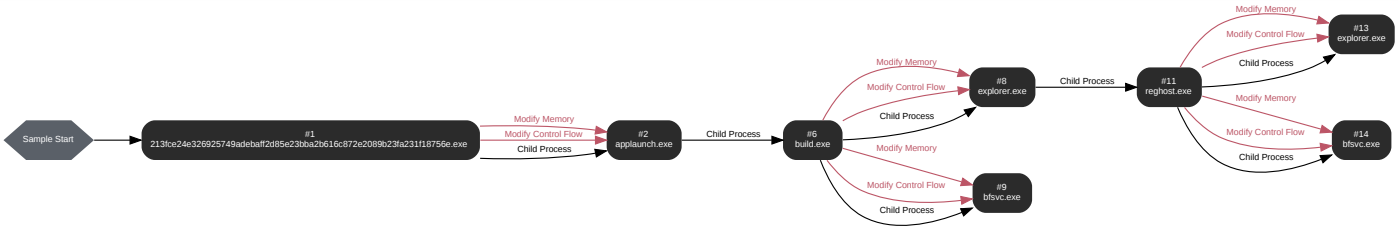
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://cdn.discordapp.com/attachments/919960898020466752/924051735893377094/vvzz67_build.exe	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	cdn.discordapp.com	NoError	162.159.135.233, 162.159.133.233, 162.159.129.233, 162.159.130.233, 162.159.134.233		NA

BEHAVIOR

Process Graph



Process #1: 213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 71862, Reason: Analysis Target
Unmonitor End Time	End Time: 179742, Reason: Terminated
Monitor duration	107.88s
Return Code	0
PID	3740
Parent PID	1560
Bitness	32 Bit

Host Behavior

Type	Count
Module	388
Registry	2
Keyboard	1
System	15
-	1
File	8
Environment	2
Process	1
-	3
-	8

Process #2: applaunch.exe

ID	2
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: 173893, Reason: Child Process
Unmonitor End Time	End Time: 254495, Reason: Terminated
Monitor duration	80.60s
Return Code	0
PID	3504
Parent PID	3740
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\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe	0x39c	0x400000(4194304)	0x20000	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe	0x39c	0x3f1008(4132872)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe	0x39c / 0xfa4	0x77c08fe0(2009108448)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\build.exe	8285.00 KB	c791924544847b19870bd1d9bab29573058de6b1510c5100b9ce4a44676411e5	✗

Host Behavior

Type	Count
Process	1
File	566
Registry	253
User	3
-	13
Module	68
COM	119
-	11
System	155
Window	2
Keyboard	3
Environment	8

Network Behavior

Type	Count
HTTPS	1
DNS	1
TCP	2

Process #6: build.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\build.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 247834, Reason: Child Process
Unmonitor End Time	End Time: 264349, Reason: Terminated
Monitor duration	16.52s
Return Code	0
PID	4444
Parent PID	3504
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\RegHost.exe	8285.00 KB	c791924544847b19870bd1d9bab29573058de6b1510c5100b9ce4a44676411e5	✖

Host Behavior

Type	Count
Module	794
System	77
File	364
-	5
-	1
User	1
-	1
Registry	13
Environment	1
Process	2
-	6
-	34

Process #8: explorer.exe

ID	8
File Name	c:\windows\explorer.exe
Command Line	"C:\Windows\explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 261184, Reason: Child Process
Unmonitor End Time	End Time: 276963, Reason: Terminated
Monitor duration	15.78s
Return Code	1
PID	240
Parent PID	4444
Bitness	64 Bit

Injection Information (10)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140000000(5368709120)	0x400	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140001000(5368713216)	0xf400	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x319010(3248144)	0x8	✓	7
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140011000(5368778752)	0x9c00	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x14001b000(5368819712)	0xc00	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x14001d000(5368827904)	0x1200	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x14001f000(5368836096)	0x200	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140020000(5368840192)	0x200	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140021000(5368844288)	0x800	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160 / 0x388	0x7ffd5052c230(140725951054384)	-	✓	1

Host Behavior

Type	Count
Module	12
File	3
Environment	1
Process	252

Process #9: bfsvc.exe

ID	9
File Name	c:\windows\bfsvc.exe
Command Line	C:\Windows\bfsvc.exe -log 0 -ftime 60 -pool eu1-etc.ethermine.org:4444 -wal 0xa6ceE57d9638dA506ff99899c6C018292Ef4826C -coin etc -worker EasyMiner_Bot -mi 14
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 262534, Reason: Child Process
Unmonitor End Time	End Time: 273473, Reason: Terminated
Monitor duration	10.94s
Return Code	8
PID	2312
Parent PID	4444
Bitness	64 Bit

Injection Information (11)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140000000(5368709120)	0x400	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140001000(5368713216)	0x422a00	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x24a010(2400272)	0x8	✓	8
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140424000(5373050880)	0x35c400	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x140781000(5376577536)	0x56a00	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x1407e1000(5376970752)	0x28600	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x14080a000(5377138688)	0x200	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x14080b000(5377142784)	0x1000	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x14080c000(5377146880)	0x200	✓	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160	0x14080d000(5377150976)	0x8000	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	0x1160 / 0xfe4	0x7ffd5052c230(140725951054384)	-	✓	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗

Host Behavior

Type	Count
Module	86
File	157
System	12
Environment	7
-	2
Registry	2

Process #11: reghost.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\RegHost.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 274540, Reason: Child Process
Unmonitor End Time	End Time: 288015, Reason: Terminated
Monitor duration	13.47s
Return Code	0
PID	1684
Parent PID	240
Bitness	64 Bit

Host Behavior

Type	Count
Module	793
System	66
File	364
-	5
-	1
User	1
-	1
Registry	13
Environment	1
Process	2
-	6
-	34

Process #13: explorer.exe

ID	13
File Name	c:\windows\explorer.exe
Command Line	"C:\Windows\explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 285127, Reason: Child Process
Unmonitor End Time	End Time: 288049, Reason: Terminated
Monitor duration	2.92s
Return Code	1073807364
PID	1268
Parent PID	1684
Bitness	64 Bit

Injection Information (10)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x140000000(5368709120)	0x400	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x140001000(5368713216)	0xf400	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x3fa010(4169744)	0x8	✓	7
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x140011000(5368778752)	0x9c00	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x14001b000(5368819712)	0xc00	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x14001d000(5368827904)	0x1200	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x14001f000(5368836096)	0x200	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x140020000(5368840192)	0x200	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x140021000(5368844288)	0x800	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c / 0xefc	0x7ffd5052c230(140725951054384)	-	✓	1

Host Behavior

Type	Count
Module	12
File	3

Type	Count
Environment	1
Process	254

Process #14: bfsvc.exe

ID	14
File Name	c:\windows\bfsvc.exe
Command Line	C:\Windows\bfsvc.exe -log 0 -ftime 60 -pool eu1-etc.ethermine.org:4444 -wal 0xa6ceE57d9638dA506ff99899c6C018292Ef4826C -coin etc -worker EasyMiner_Bot -mi 14
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\
Monitor Start Time	Start Time: 285163, Reason: Child Process
Unmonitor End Time	End Time: 289068, Reason: Terminated
Monitor duration	3.90s
Return Code	1073807364
PID	1252
Parent PID	1684
Bitness	64 Bit

Injection Information (10)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x140000000(5368709120)	0x400	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x226010(2252816)	0x8	✓	8
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x140424000(5373050880)	0x35c400	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x140781000(5376577536)	0x56a00	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x1407e1000(5376970752)	0x28600	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x14080a000(5377138688)	0x200	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x14080b000(5377142784)	0x1000	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x14080c000(5377146880)	0x200	✓	1
Modify Memory	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c	0x14080d000(5377150976)	0x8000	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	0x63c / 0x980	0x7ffd5052c230(140725951054384)	-	✓	1

Host Behavior

Type	Count
Module	11

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e	C:\Users\RDhJ0CNFevzX\Desktop\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe	Sample File	4294.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
c791924544847b19870bd1d9bab29573058de6b1510c5100b9ce4a44676411e5	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\build.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\RegHost.exe	Dropped File	8285.00 KB	application/vnd.microsoft.portable-executable	Create, Access, Read, Write	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe	Sample 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:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YaAddon	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\031fl.docx	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4s_Ki_KH8PK2U7oIT2yY.docx	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\66hlA9d.docx	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\D IlQpZjo2_VlnF3V.docx	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\NR_hHMnBOg9X.docx	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\OLaL9DVQ8 bzl_.doc	Accessed File	Read, Access	CLEAN
C:\Program Files\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\build.exe	Dropped File	Create, Access, Read, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp	Accessed File	Access	CLEAN
\??\c:\users\rdhj0cnfevzx\appdata\local\temp\build.exe	Accessed File	Create, Access, Read	CLEAN
\\.\C:	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\temp\80EB2F5C	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\RegHost.exe	Dropped File	Create, Access, Read	CLEAN
C:\Windows\explorer.exe	Accessed File	Access	CLEAN
C:\Windows\bfsvc.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\07A8E gA XPTpUH6q.docx	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\2sr840Dgzq3V.bmp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\3z31Zds.gif	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\7Mla2TjakLT.rtf	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\960NsfJkE0.bmp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\9r8pRiczDN0.gif	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\a95WAC.avi	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\b dl7t.pptx	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\bNcEV.wav	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\dZjGE7ohnSMV0P16.wav	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\F0yKB9SQcTesgyb.mp3	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\fNqhTG9Xak1Etlj7H5v.ots	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\fv8otpMka Wg.m4a	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\gen_py	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\H-wcra.bmp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\I-2nm5-X4q.wav	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\I8X2TxPpjjqAS3.mkv	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\IoeGM.ots	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\kC aUQz.mp3	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\KnoB88.tmp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Kzlu2xjDYc.mp3	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Low	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\ltfBgcZqVqf_y.png	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Nj5Ecq5SeR8t.mp3	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\nZtaga69KA6WZPDv.flv	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\pNar6q-oOp1.bmp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\Sdy83DydyPsPS_PB_.doc	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\UIfpAwOH_o8OFjt3.mp3	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\wXMLRISp5zrw_qj72WX.csv	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\yP4F9.bmp	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp_MqYImgEvKDoR.gif	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp_qInLp46kQ1zTXWm.m4a	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\~DFD54D056689FA94D6.TMP	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\~DFDA4D730673A5F8D5.TMP	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\??\c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\reghost.exe	Accessed File	Create, Access, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://cdn.discordapp.com/attachments/919960898020466752/924051735893377094/vvzz67_build.exe	-	162.159.135.233	-	GET	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
cdn.discordapp.com	162.159.130.233, 162.159.134.233, 162.159.135.233, 162.159.129.233, 162.159.133.233	-	DNS, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	DNS, UDP	CLEAN
162.159.135.233	cdn.discordapp.com	-	DNS, TCP, HTTPS	CLEAN
103.246.144.29	-	Netherlands	TCP	CLEAN
162.159.133.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.129.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.130.233	cdn.discordapp.com	-	DNS	CLEAN
162.159.134.233	cdn.discordapp.com	-	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	applaunch.exe	CLEAN
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	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Clients\StartMenuInternet\IEXPLORE.EXE\shell\open\command	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayVersion	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayName	read, access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayName	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\DisplayVersion	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\Software\Valve\Steam	access	applaunch.exe	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe	"C:\Users\RDhJ0CNFevzX\Desktop\213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e.exe"	MALICIOUS
build.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\build.exe"	MALICIOUS
reghost.exe	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\RegHost.exe"	MALICIOUS
applaunch.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"	SUSPICIOUS
explorer.exe	"C:\Windows\explorer.exe"	SUSPICIOUS
bfsvc.exe	C:\Windows\bfsvc.exe -log 0 -ftime 60 -pool eu1-etc.ethermine.org:4444 -wal 0xa6ceE57d9638dA506ff99899c6C018292Ef4826C -coin etc -worker EasyMiner_Bot -mi 14	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	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

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