MALICIOUS

Classifications: Spyware | Injector

Threat Names: RedLine | RedLine.A | Trojan.GenericKDZ.79353

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe**
ID	#1091260
MD5	3645676180db7e06664a53e0ac6317b5
SHA1	caa35a080f3e5b2d7f2672b08533fae7350cb71e
SHA256	9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd
File Size	4259.50 KB
Report Created	2021-10-29 18:55 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (30 rules, 46 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	2	Spyware
	• Rule "RedLine_SOAPCommunication" from ruleset "Malware" has matched on response data of URL "http://185.154.13.159:34854/". • Rule "RedLine_A" from ruleset "Malware" has matched on a memory dump for (process #2) applaunch.exe.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Mozilla Firefox, Electrum Bitcoin Wallet, Exodus Cryptocurrency Wallet, Comodo IceDragon, k-Meleon, Internet Explorer / Edge, Cyberfox, Total Commander, Opera, Mozilla Thunderbird, The Bat!.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe modifies memory of (process #2) applaunch.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe alters context of (process #2) applaunch.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.79353".			
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	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".			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #2) applaunch.exe reads the network adapters' addresses by API.			
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	Discovery	Executes WMI query	8	-

Score	Category	Operation	Count	Classification
	• (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_Processor. • (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_Process Where SessionId='1'. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_VideoController. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_DiskDrive. • (Process #2) applaunch.exe executes WMI query: SELECT * FROM Win32_OperatingSystem.			
2/5	Discovery	Collects hardware properties	1	-
	• (Process #2) applaunch.exe queries hardware properties via WMI.			
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	6	-
	• (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.			
2/5	Discovery	Enumerates running processes	1	-
	• (Process #2) applaunch.exe enumerates running processes via WMI.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #2) applaunch.exe queries OS version via WMI.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• Multiple processes are possibly trying to detect a VM via rdtsc.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	1	-
	• (Process #1) 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe makes a direct system call to "NtProtectVirtualMemory".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe starts (process #2) applaunch.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe reads from (process #2) applaunch.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.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.			

Score	Category	Operation	Count	Classification
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #2) applaunch.exe enables process privilege "SeDebugPrivilege".			
1/5	Execution	Executes itself	1	-
	• (Process #1) 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #2) applaunch.exe resolves host name "api.ip.sb" to IP "104.26.13.31".			
1/5	Network Connection	Connects to remote host	2	-
	• (Process #2) applaunch.exe opens an outgoing TCP connection to host "185.154.13.159:34854". • (Process #2) applaunch.exe opens an outgoing TCP connection to host "104.26.13.31:443".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) applaunch.exe tries to connect to TCP port 34854 at 185.154.13.159.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #2) applaunch.exe resolves 53 API functions by name.			
1/5	Crash	A monitored process crashed	1	-
	• (Process #1) 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe crashed.			

Mitre ATT&CK Matrix

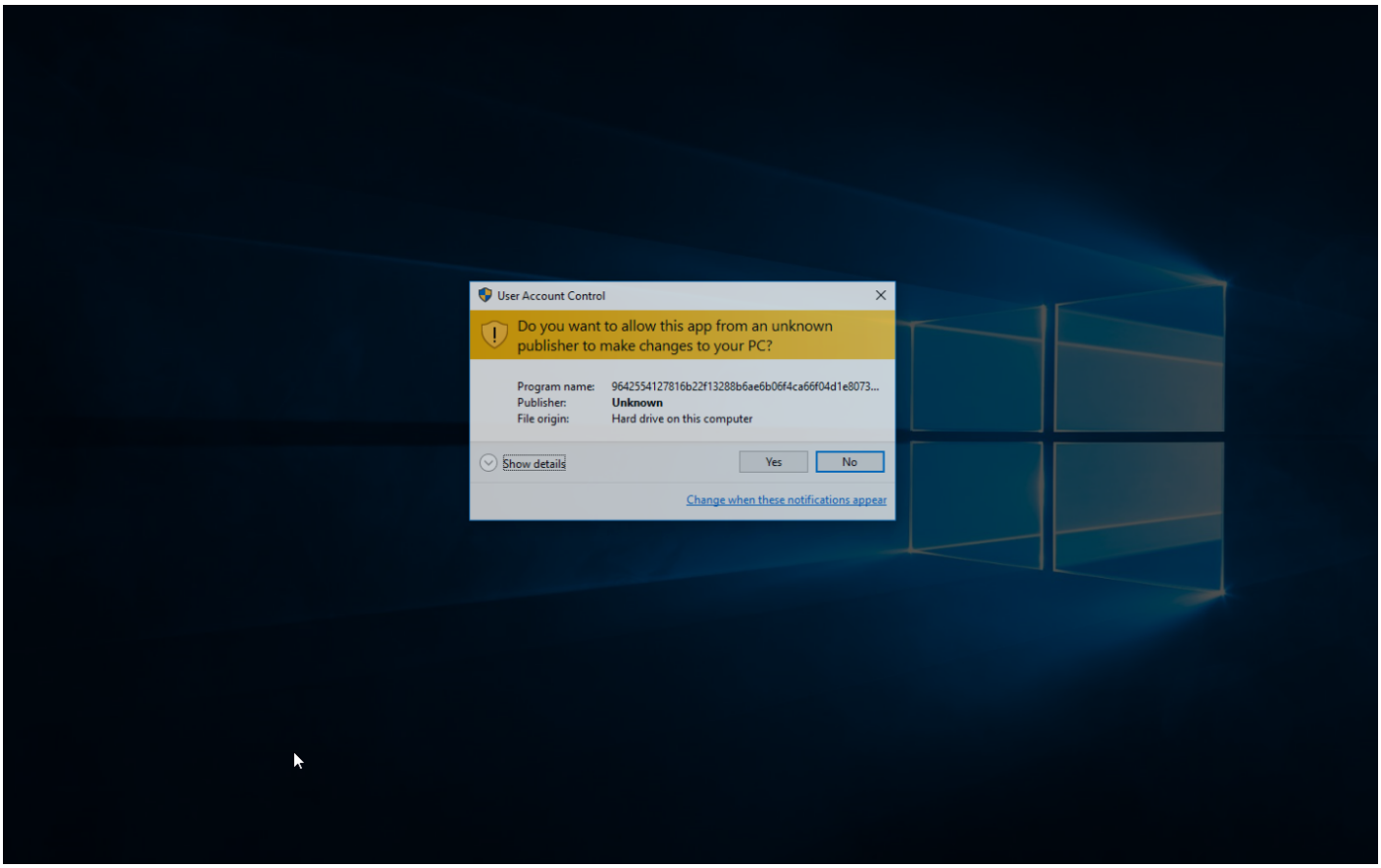
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1143 Hidden Window	#T1081 Credentials in Files	#T1016 System Network Configuration Discovery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

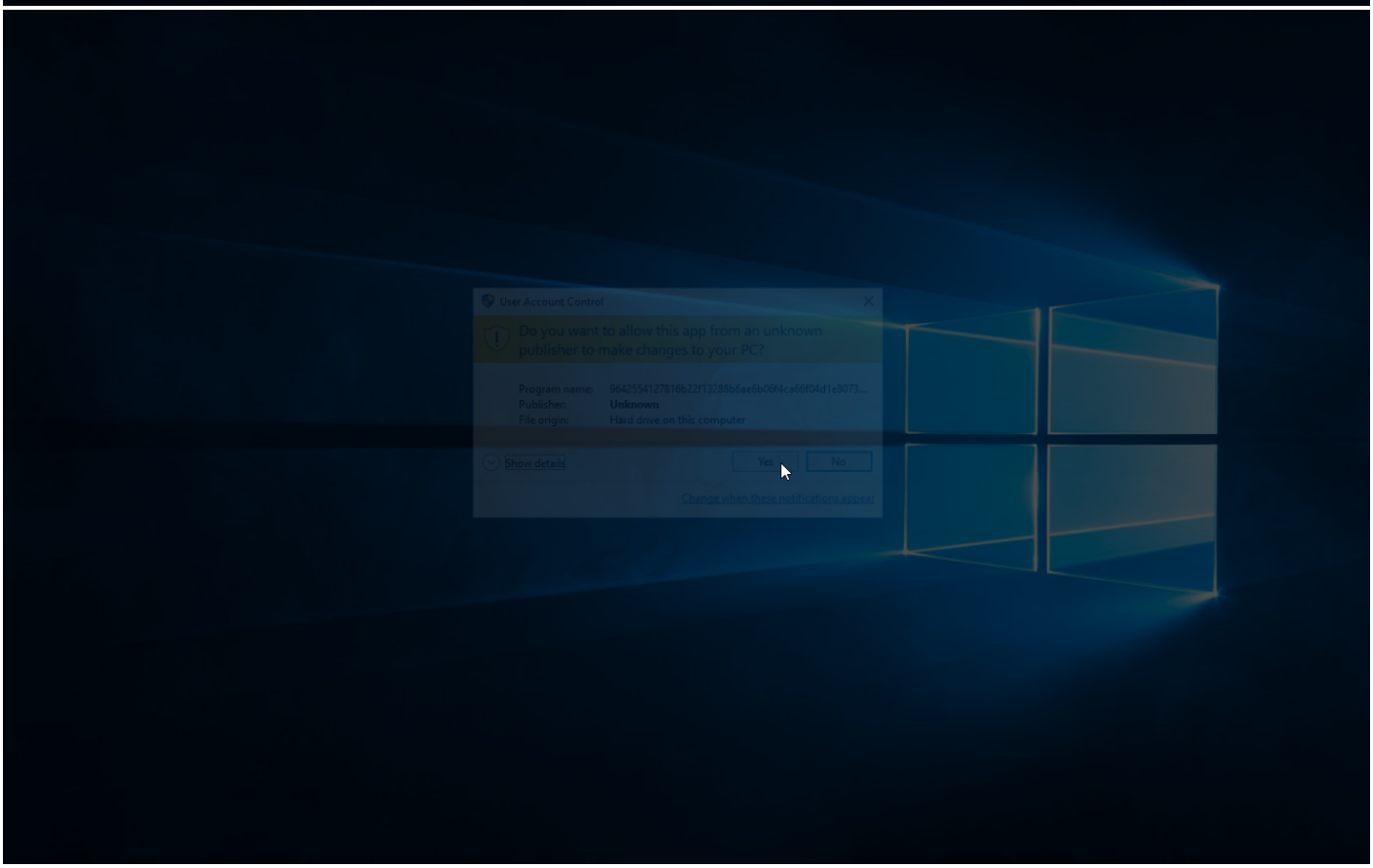
Sample Information

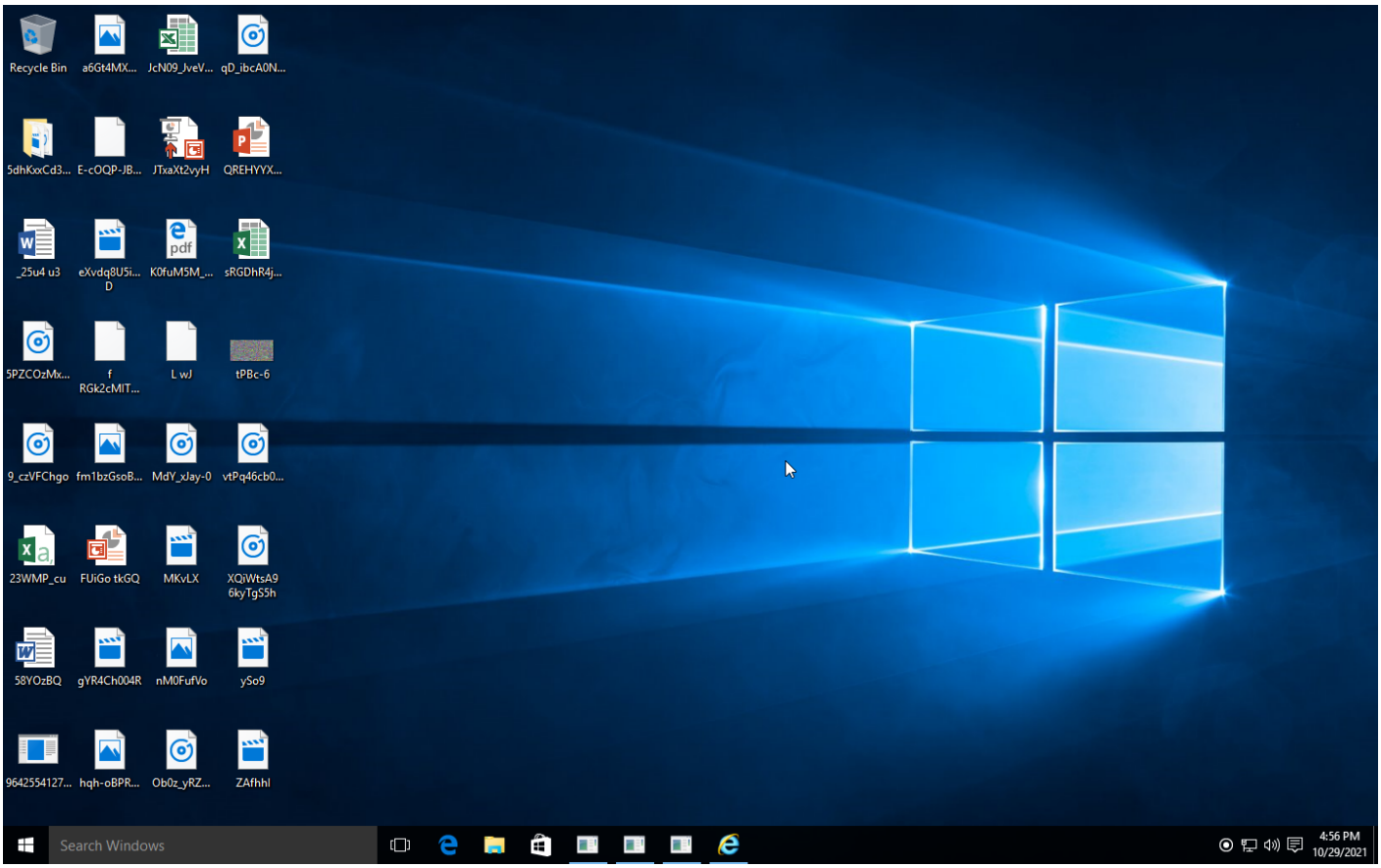
ID	#1091260
MD5	3645676180db7e06664a53e0ac6317b5
SHA1	caa35a080f3e5b2d7f2672b08533fae7350cb71e
SHA256	9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd
SSDeep	98304:q74x9tum8OvcqReP2V827sYfB4qdSW/NdVlMElOTGnO2:ZbtMqReP2VTvfB4slVdrMzOT8
ImpHash	908bea7ee71339f1c35ba419da3ba679
File Name	9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe
File Size	4259.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

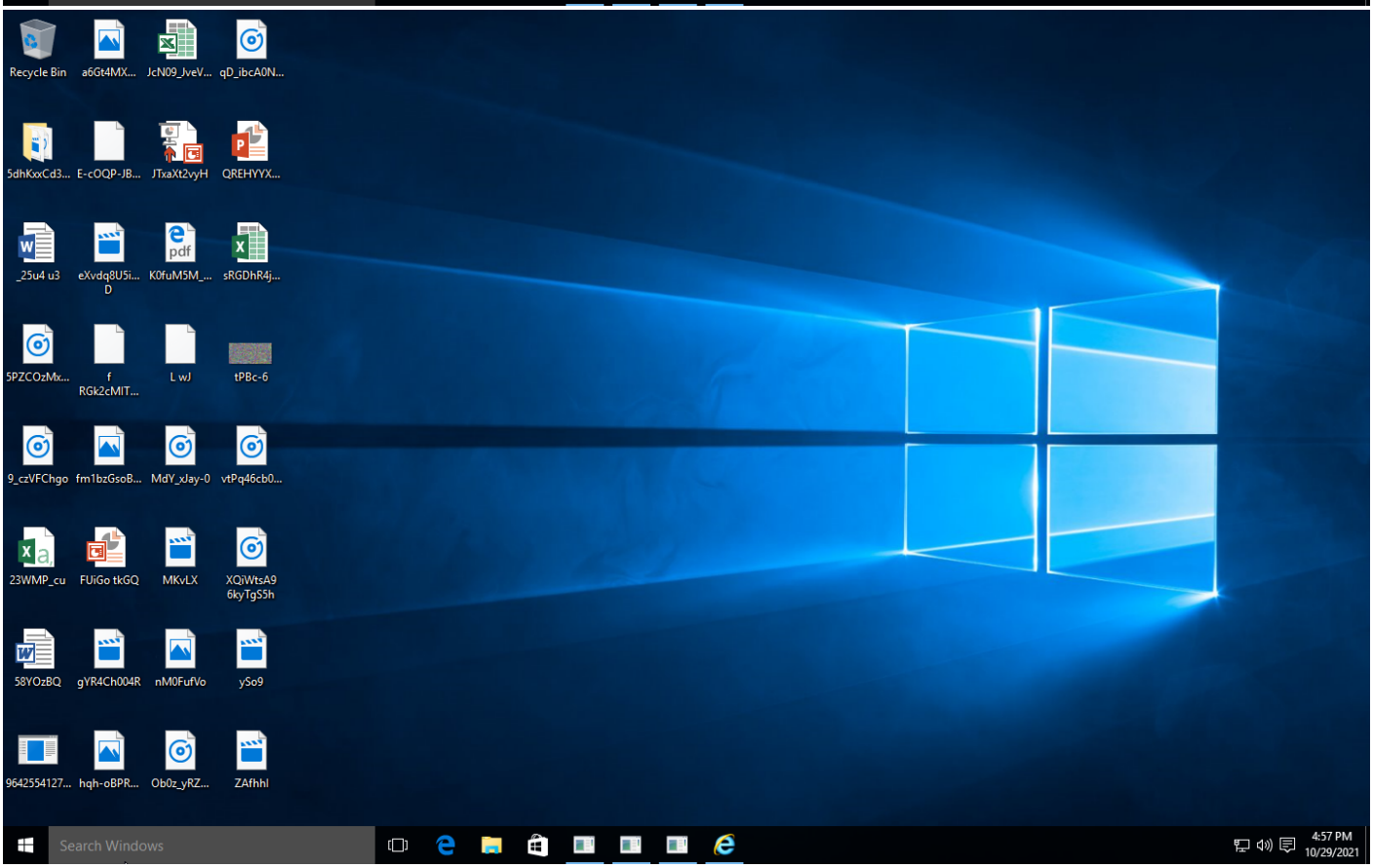
Analysis Information

Creation Time	2021-10-29 18:55 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Sample crashed
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	3


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear







Screenshots truncated

NETWORK

General

1892.90 KB total sent

24.06 KB total received

2 ports 443, 34854

3 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

2 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

2 sessions, 1892.90 KB sent, 24.06 KB received

HTTP Requests

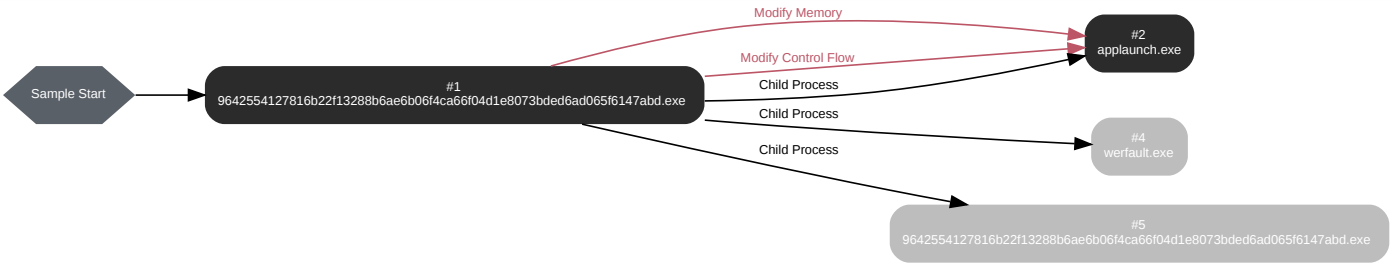
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://185.154.13.159:34854/	-	-		0 bytes	NA
GET	https://api.ip.sb/geoip	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.ip.sb, api.ip.sb.cdn.cloudflare.net	NoError	104.26.13.31, 172.67.75.172, 104.26.12.31	api.ip.sb.cdn.cloudflare.net	NA
-	api.ip.sb	-	104.26.13.31, 172.67.75.172, 104.26.12.31		NA

BEHAVIOR

Process Graph



Process #1: 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 60128, Reason: Analysis Target
Unmonitor End Time	End Time: 155274, Reason: Crashed
Monitor duration	95.15s
Return Code	3221225477
PID	4588
Parent PID	1636
Bitness	32 Bit

Host Behavior

Type	Count
Module	87
System	10
Environment	2
File	6
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: 77411, Reason: Child Process
Unmonitor End Time	End Time: 194886, Reason: Terminated
Monitor duration	117.47s
Return Code	0
PID	3660
Parent PID	4588
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\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe	0x1230	0x400000(4194304)	0x1e000	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe	0x1230	0x242008(2367496)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe	0x1230 / 0xe64	0x772d8fe0(1999474656)	-	✓	1

Dropped Files (7)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpC80C.tmp	48.83 KB	07323e082ec156cabc3333329f8c56d62e8e21d6a4f393d7197a9bee61e01989	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCCEF.tmp	32.50 KB	35c3d17c5c87c29a3b2b8056dec916bc92a8b26e8e0eec7add026cc978373d50	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCCFF.tmp	44.08 KB	5087e8ac5272b1465b512a35e251fc910b07339e0ee28f3281d7c2edb1e9573d	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD10.tmp	84.65 KB	5e83d0f9bb7c1830acb21973fc8e43956e1146568ad3f80c16abf7e586ccdc93	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD40.tmp	6.32 KB	e6bfa6a7623cd9a7ea1118a0e10f290a3d07e00f5096e38f466b4d93139d5c55	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD50.tmp	52.54 KB	1f6c2c1bc2db465f6783e9eb8cc6aa570fbb3bbad5ea7d2e56668130d06f4997	✗
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD61.tmp	73.51 KB	2468e43c68642d0e932d6169c15048f8e50f794b370e0a9c77bef76443863cdc	✗

Host Behavior

Type	Count
Module	67
Window	2
File	244
-	13

Type	Count
System	108
Registry	253
Environment	8
COM	206
-	12
User	3
Keyboard	3

Network Behavior

Type	Count
HTTP	4
HTTPS	1
DNS	2
TCP	2

Process #4: werfault.exe

ID	4
File Name	c:\windows\syswow64\werfault.exe
Command Line	C:\Windows\SysWOW64\WerFault.exe -u -p 4588 -s 176
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 84622, Reason: Child Process
Unmonitor End Time	End Time: 155177, Reason: Terminated
Monitor duration	70.56s
Return Code	0
PID	824
Parent PID	4588
Bitness	32 Bit

Process #5: 9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 108133, Reason: Child Process
Unmonitor End Time	End Time: 155107, Reason: Terminated
Monitor duration	46.97s
Return Code	259
PID	1964
Parent PID	4588
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd	C:\Users\RDhJ0CNFevzX\Desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe	Sample File	4259.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
07323e082ec156cabc3333329f8c56d62e8e21d6a4f393d7197a9bee61e01989	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpC80C.tmp, C:\Users\RDhJ0CNFevzX\Desktop_25u4 u3.docx	Dropped File	48.83 KB	application/zip	Write, Create, Delete, Read, Access	CLEAN
35c3d17c5c87c29a3b2b8056dec916bc92a8b26e8e0eec7add026cc978373d50	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCCEF.tmp, C:\Users\RDhJ0CNFevzX\Documents\C0CC wXtnQbxcIx0Yw.docx	Dropped File	32.50 KB	application/zip	Write, Create, Delete, Read, Access	CLEAN
5087e8ac5272b1465b512a35e251fc910b07339e0ee28f3281d7c2edb1e9573d	C:\Users\RDhJ0CNFevzX\Documents\lRxOx1U0aktspsok.docx, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCCFF.tmp	Dropped File	44.08 KB	application/zip	Write, Create, Delete, Read, Access	CLEAN
5e83d0f9bb7c1830acb21973fc8e43956e1146568ad3f80c16abf7e586ccdc93	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD10.tmp, C:\Users\RDhJ0CNFevzX\Documents\O2cncwJj9.docx	Dropped File	84.65 KB	application/zip	Write, Create, Delete, Read, Access	CLEAN
e6bfa6a7623cd9a7ea1118a0e10f290a3d07e00f5096e38f466b4d93139d5c55	C:\Users\RDhJ0CNFevzX\Documents\oJr6ZesmKU IzSK.docx, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD40.tmp	Dropped File	6.32 KB	application/zip	Write, Create, Delete, Read, Access	CLEAN
1f6c2c1bc2db465f6783e9eb8cc6aa570fbb3bbad5ea7d2e56668130d06f4997	C:\Users\RDhJ0CNFevzX\Documents\x87mVcjjbZa.docx, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD50.tmp	Dropped File	52.54 KB	application/zip	Write, Create, Delete, Read, Access	CLEAN
2468e43c68642d0e932d6169c15048f8e50f794b370e0a9c77bef76443863cdc	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD61.tmp, C:\Users\RDhJ0CNFevzX\Documents\YFe19.docx	Dropped File	73.51 KB	application/zip	Write, Create, Delete, Read, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.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\Desktop_25u4 u3.docx	Dropped File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpC80C.tmp	Dropped File	Write, Create, Delete, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\C0CC wXtnQbxcIx0Yw.docx	Dropped File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCCEF.tmp	Dropped File	Write, Create, Delete, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\lRxOx1U0aktspsok.docx	Dropped File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCCFF.tmp	Dropped File	Write, Create, Delete, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\O2cncwJj9.docx	Dropped File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD10.tmp	Dropped File	Write, Create, Delete, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\oJr6ZesmKU IzSK.docx	Dropped File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD40.tmp	Dropped File	Write, Create, Delete, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\x87mVcjjbZa.docx	Dropped File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD50.tmp	Dropped File	Write, Create, Delete, Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\YFe19.docx	Dropped File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpCD61.tmp	Dropped File	Write, Create, Delete, Read, Access	CLEAN
C:\Program Files\Internet Explorer\iexplore.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex\YaAddon	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Yandex	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://185.154.13.159:34854	-	185.154.13.159	-	POST	MALICIOUS
https://api.ip.sb/geoip	-	104.26.13.31	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
api.ip.sb	172.67.75.172, 104.26.12.31, 104.26.13.31	-	HTTPS, DNS	CLEAN
api.ip.sb.cdn.cloudflare.net	172.67.75.172, 104.26.12.31, 104.26.13.31	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
185.154.13.159	-	Netherlands	HTTP, TCP	CLEAN
104.26.13.31	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	HTTPS, TCP, DNS	CLEAN
172.67.75.172	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	DNS	CLEAN
104.26.12.31	api.ip.sb.cdn.cloudflare.net, api.ip.sb	United States	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	applaunch.exe	CLEAN
HKEY_CURRENT_USER	access	applaunch.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	applaunch.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\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\.NETFramework\v4.0.30319	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	applaunch.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	applaunch.exe	CLEAN
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

Registry Key	Operations	Parent Process Name	Verdict
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
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

Registry Key	Operations	Parent Process Name	Verdict
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
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

Registry Key	Operations	Parent Process Name	Verdict
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
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

Registry Key	Operations	Parent Process Name	Verdict
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
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

Registry Key	Operations	Parent Process Name	Verdict
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
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

Reduced dataset

Process

Process Name	Commandline	Verdict
9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe"	MALICIOUS
applaunch.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"	SUSPICIOUS
werfault.exe	C:\Windows\SysWOW64\WerFault.exe -u -p 4588 -s 176	CLEAN

YARA / AV

YARA (3)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	RedLine_SOAPCommunication	RedLine Stealer SOAP response	Web Request	-	Spyware	5/5
Malware	RedLine_SOAPCommunication	RedLine Stealer SOAP response	Web Request	-	Spyware	5/5
Malware	RedLine_A	RedLine Stealer, RedLine.A variant	Memory Dump	-	Spyware	5/5

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.79353	C:\Users\RDhJ0CNFevzX\Desktop\9642554127816b22f13288b6ae6b06f4ca66f04d1e8073bded6ad065f6147abd.exe	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	4.3.1
Dynamic Engine Version	4.3.1 / 10/25/2021 03:57
Static Engine Version	4.3.1.0 / 2021-10-25 03:00:16
AV Exceptions Version	4.3.1.6 / 2021-09-21 13:25:28
Link Detonation Heuristics Version	4.3.1.6 / 2021-09-21 13:25:28
Signature Trust Store Version	4.3.1.6 / 2021-09-21 13:25:28
VMRay Threat Identifiers Version	4.3.1.18 / 2021-10-22 15:07:52
YARA Built-in Ruleset Version	4.3.1.17

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	2021-10-29 13:16:28+00:00
Built-in AV Database Records	11081332

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