ID: 483055
Sample Name: ASGT(Al Sahoo General Trading) - RFQ.exe
Cookbook: default.jbs
Time: 13:33:41
Date: 14/09/2021
Version: 33.0.0 White Diamond

Table of Contents

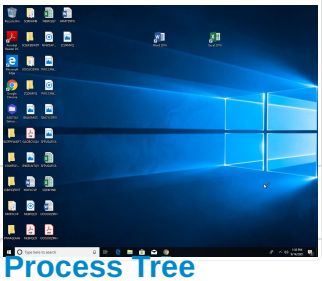
Windows Analysis Report ASGT(Al Sahoo General Trad…

Overview

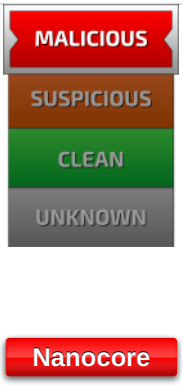
General Information

Sample Name:	ASGT(Al Sahoo General Trading) - RFQ.exe
Analysis ID:	483055
MD5:	f981ae4dae49248.
SHA1:	680901b0a898a6..
SHA256:	ef45c55d9b3fd18..
Tags:	exe nanocore
Infos:	

Most interesting Screenshot:



Detection

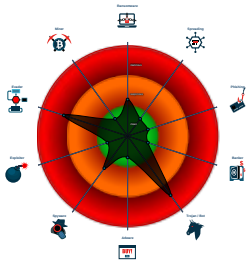


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Writes to foreign memory regions
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Creates an undocumented autostart …
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- ASGT(Al Sahoo General Trading) - RFQ.exe (PID: 6864 cmdline: 'C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe' MD5: F981AE4DAE49248C03DD86B5508EC434)
  - powershell.exe (PID: 7012 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 20 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AdvancedRun.exe (PID: 5352 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\sc.exe' /WindowState 0 /CommandLine 'stop WinDefend' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6648 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 5352 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - AdvancedRun.exe (PID: 6952 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' /WindowState 0 /CommandLine 'rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 5316 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 6952 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - ASGT(Al Sahoo General Trading) - RFQ.exe (PID: 3164 cmdline: C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe MD5: F981AE4DAE49248C03DD86B5508EC434)
  - ASGT(Al Sahoo General Trading) - RFQ.exe (PID: 4492 cmdline: C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe MD5: F981AE4DAE49248C03DD86B5508EC434)
  - ASGT(Al Sahoo General Trading) - RFQ.exe (PID: 6928 cmdline: C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe MD5: F981AE4DAE49248C03DD86B5508EC434)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.638149839.00000000069B0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
00000018.00000002.638149839.00000000069B0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
00000018.00000002.634473391.00000000056B0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000018.00000002.634473391.00000000056B0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000018.00000002.638232760.00000000069D0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
Click to see the 48 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
24.2.ASGT(Al Sahoo General Trading) - RFQ.exe.56b0000.15.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
24.2.ASGT(Al Sahoo General Trading) - RFQ.exe.56b0000.15.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
24.2.ASGT(Al Sahoo General Trading) - RFQ.exe.2ed1d4c.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
24.2.ASGT(Al Sahoo General Trading) - RFQ.exe.2ed1d4c.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
24.2.ASGT(Al Sahoo General Trading) - RFQ.exe.3fbbf69.10.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
Click to see the 128 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Used To Disable Windows Defender AV Security Monitoring

Sigma detected: PowerShell Script Run in AppData

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Creates an undocumented autostart registry key

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

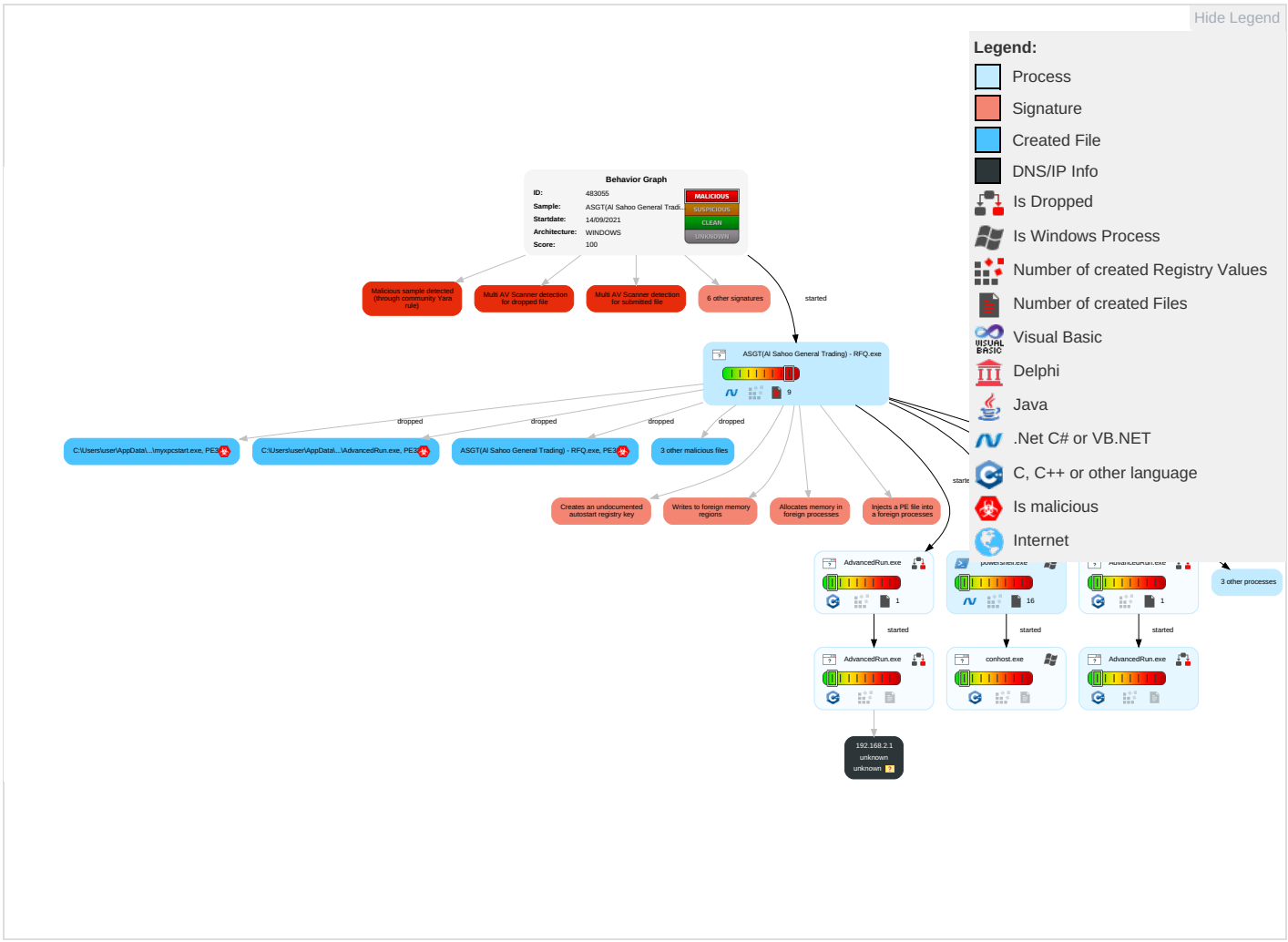
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Service Execution 2	Windows Service 1	Exploitation for Privilege Escalation 1	Masquerading 1	Input Capture 1 1	Security Software Discovery 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Com
Default Accounts	Native API 1	Registry Run Keys / Startup Folder 1 1	Access Token Manipulation 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Remote Access Software 1	Explo Redir Calls
Domain Accounts	At (Linux)	Application Shimming 1	Windows Service 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Explo Track Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 3	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1 1	Process Injection 3 1 3	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devic Com
Replication Through Removable Media	Launchd	Rc.common	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Protc

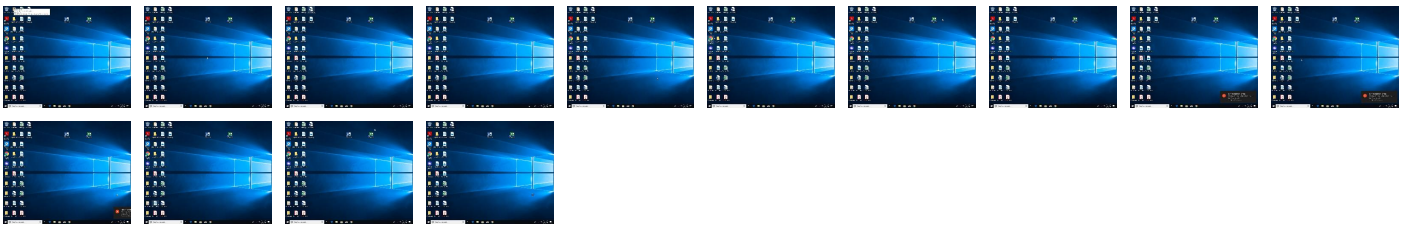
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ASGT(Al Sahoo General Trading) - RFQ.exe	34%	Virustotal		Browse
ASGT(Al Sahoo General Trading) - RFQ.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\myxpcstart.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe	34%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\myxpcstart.exe	34%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.ASGT(Al Sahoo General Trading) - RFQ.exe.57d0000.17.unpack	100%	Avira	TR/NanoCore.fadte		Download File
24.2.ASGT(Al Sahoo General Trading) - RFQ.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483055
Start date:	14.09.2021
Start time:	13:33:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ASGT(Al Sahoo General Trading) - RFQ.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/11@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.5% (good quality ratio 13.7%) • Quality average: 82.1% • Quality standard deviation: 27.1%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:35:19	API Interceptor	33x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ASGT(Al Sahoo General Trading) - RFQ.exe.log	
Process:	C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D 8
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	17204
Entropy (8bit):	5.5632462558313565
Encrypted:	false
SSDEEP:	384:1t9/Ry0Lw0ij+9o0d0iRnYSBKnIZ2p7Y9gbpkcQp7TDqYKy:H8gvY4KIk5SRVDjd
MD5:	736133EBC2327594F7697C74660F6042
SHA1:	3FE6CB14AC3EBD2FDEFC63117C9FF7400BEDE209

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SHA-256:	6BB5DCE8996BC7253F473835E6BF84D595C4E75B2D41BC93073DC4254C6B192E
SHA-512:	A56C21FAB04E999A5DCEC10DE07ED86B381DDCB40808407954D095A319C1B6AF149B3D6A9EA2A3E794405072B01B071B458E3204AB615D483ABB026336EF3D16
Malicious:	false
Reputation:	unknown
Preview:	@...e.....#.....@.....H.....<@.^.L."My...:'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)S.....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]..... %.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe	
Process:	C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1012736
Entropy (8bit):	6.838484477012448
Encrypted:	false
SSDEEP:	12288:D/gecNU2zqX6lUB2Ake6KZMimr+MONraliDayqLhpe8/DUC/:EDNgWUB2Ake5MihNWgWxlT/D
MD5:	F981AE4DAE49248C03DD86B5508EC434
SHA1:	680901B0A898A68FF04CBAAFB851E28294D06D03
SHA-256:	EF45C55D9B3FD183F6C9B4E0359005FA6052FA4155DE07129B839056B7CC26E9
SHA-512:	704C35423789F768C7323C4FCF83B1D50DB8C12ADB138995C7DA07FC22721A2C70D2A09EBDF6D3EE128A5434F4B24BBC775BED587273C5015204E2B18A67CCC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 34%, Browse
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....@a..... .....@.. .....@.....x...W..... ....H.....text..... ....`.rsrc.....@..@.reloc.....r.....@..B.....H.....\.....6....+..0.....0.....-.&(....+.&+.*....0.....s....(....t....-.&+.....+.*....~....*..0.....-.&(....+.&+.*....0.....-.&{....+.&+.*....0.....-.&&+.}....+.*....0.....-.&{....+.&+.*....0.....-.&&+.}....+.*....0.....-.&{....+.&+.*....0.....-.&{....+.&+.*....0.....-.&&+.}....+.*....0.....,.&(....+.&+.*....0.....-.&{....+.&+.*....0..

C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\AdvancedRun.exe	
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2icawshj.zys.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ufcdmgif.vi3.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\myxpcstart.exe	
Process:	C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1012736
Entropy (8bit):	6.838484477012448
Encrypted:	false
SSDEEP:	12288:D/gecNU2zqX6lUB2Ake6KZMimr+MONraliDayqLhpe8/DUC/:EDNgWUB2Ake5MihNWgWxlT/D
MD5:	F981AE4DAE49248C03DD86B5508EC434
SHA1:	680901B0A898A68FF04CBAAFB851E28294D06D03
SHA-256:	EF45C55D9B3FD183F6C9B4E0359005FA6052FA4155DE07129B839056B7CC26E9
SHA-512:	704C35423789F768C7323C4FCF83B1D50DB8C12ADB138995C7DA07FC22721A2C70D2A09EBDF6D3EE128A5434F4B24BBC775BED587273C5015204E2B18A67CC C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 34%, Browse
Reputation:	unknown

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\myxpcstart.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....@a..... .....@.. ....@.....x...W..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....r.....@..B.....H.....\.....6....+..0.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0.....-.&(....+.&+.*....0 .....-.&{....+.&+.*....0.....-.&&+.}....+.*....0.....-.&{....+.&+.*....0.....-.&&+.}....+.*....0.....-.&{....+.&+.*....0.....-.&{....+.&+.*....0.....-.&&+.}....+.*. ...0.....,.&(....+.&+.*....0.....-.&{....+.&+.*....0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\myxpcstart.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210914\PowerShell_transcript.899552.sqqflWff.20210914133456.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	945
Entropy (8bit):	5.006609758970908
Encrypted:	false
SSDEEP:	24:BxSAFz317vBVLazx2DOXUWM1WUHjeTKKjX4CIym1ZJXtz3NUnxSAZhcS:BZFz39vTL0oOZUqDYB1ZLz3NiZZhZ
MD5:	3CF0C2CD563CDEA7A335E08DC7129AE0
SHA1:	6C9E22DE32CE5B9B96B6590DE168A2AFEA33A052
SHA-256:	6FEAF0C4098D5FD3410244251297C05964534CE28CE91F917C9EF82BA6E3A40D
SHA-512:	357C5AFDE3FB4BCBD2D1D5E199A4EECB59D8DB24B666DC34F70F4AF265299FEE0CF89BC39DB41AE30803D44314FA9846B76E245FBA06C47B2A5BA78AAF67F9D9
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210914133513..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 899552 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Start-Sleep -s 20..Process ID: 7012..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210914133513..**********..PS>Start-Sleep -s 20..**********..Command start time: 20210914133946..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20210914133947..**********..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.838484477012448
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	ASGT(Al Sahoo General Trading) - RFQ.exe
File size:	1012736
MD5:	f981ae4dae49248c03dd86b5508ec434
SHA1:	680901b0a898a68ff04cbaafb851e28294d06d03
SHA256:	ef45c55d9b3fd183f6c9b4e0359005fa6052fa4155de07129b839056b7cc26e9

General

SHA512:	704c35423789f768c7323c4fcf83b1d50db8c12adb138995c7da07fc22721a2c70d2a09ebdf6d3ee128a5434f4b24bbc775bed587273c5015204e2b18a67cc1c
SSDEEP:	12288:D/gecNU2zqX6lUB2Ake6KZMimr+MONraliDayqLhpe8/DUC/:EDNgWUB2Ake5MihNWgWxlT/D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....@a..... .....@.. .....@.....

File Icon

Icon Hash:	30f8f8e8e8e8f030

Static PE Info

General

Entrypoint:	0x4cead2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61401AAB [Tue Sep 14 03:44:43 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xccad8	0xccc00	False	0.645968072726	data	7.1425786043	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x2a30c	0x2a400	False	0.128397744083	data	3.79520894455	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfc000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ASGT(Al Sahoo General Trading) - RFQ.exe PID: 6864 Parent PID: 4744

General

Start time:	13:34:42
Start date:	14/09/2021
Path:	C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ASGT(Al Sahoo General Trading) - RFQ.exe'
Imagebase:	0xc70000
File size:	1012736 bytes
MD5 hash:	F981AE4DAE49248C03DD86B5508EC434
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.621578640.0000000004145000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.621578640.0000000004145000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.621578640.0000000004145000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.621361246.0000000004009000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.621361246.0000000004009000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.621361246.0000000004009000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.621456573.00000000040A6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.621456573.00000000040A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.621456573.00000000040A6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Modified

Analysis Process: powershell.exe PID: 7012 Parent PID: 6864

General

Start time:	13:34:53
Start date:	14/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Sleep -s 20
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 7020 Parent PID: 7012

General

Start time:	13:34:53
Start date:	14/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AdvancedRun.exe PID: 5352 Parent PID: 6864

General

Start time:	13:36:16

Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\sc.exe' /WindowState 0 /CommandLine 'stop WinDefend' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: AdvancedRun.exe PID: 6648 Parent PID: 5352

General

Start time:	13:36:29
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 5352
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: AdvancedRun.exe PID: 6952 Parent PID: 6864

General

Start time:	13:36:32
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' /WindowState 0 /CommandLine 'rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: AdvancedRun.exe PID: 5316 Parent PID: 6952

General

Start time:	13:36:41
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 6952
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ASGT(Al Sahoo General Trading) - RFQ.exe PID: 3164 Parent PID: 6864

General

Start time:	13:36:44
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe
Imagebase:	0x40000
File size:	1012736 bytes
MD5 hash:	F981AE4DAE49248C03DD86B5508EC434
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 34%, Virustotal, Browse
Reputation:	low

Analysis Process: ASGT(Al Sahoo General Trading) - RFQ.exe PID: 4492 Parent PID: 6864

General

Start time:	13:36:45
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe
Imagebase:	0x1c0000
File size:	1012736 bytes
MD5 hash:	F981AE4DAE49248C03DD86B5508EC434
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ASGT(Al Sahoo General Trading) - RFQ.exe PID: 6928 Parent PID: 6864

General

Start time:	13:36:46
Start date:	14/09/2021
Path:	C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\ASGT(Al Sahoo General Trading) - RFQ.exe
Imagebase:	0xa60000
File size:	1012736 bytes
MD5 hash:	F981AE4DAE49248C03DD86B5508EC434
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638149839.00000000069B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638149839.00000000069B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.634473391.00000000056B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.634473391.00000000056B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638232760.00000000069D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638232760.00000000069D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638401577.0000000006A00000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638401577.0000000006A00000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.637715725.00000000067E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.637715725.00000000067E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638552630.0000000006A40000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638552630.0000000006A40000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.637951566.0000000006960000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.637951566.0000000006960000.00000004.00020000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.633168438.000000000412A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638002422.0000000006980000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638002422.0000000006980000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638196142.00000000069C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638196142.00000000069C0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638093395.00000000069A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638093395.00000000069A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.632660357.0000000003F0C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.632660357.0000000003F0C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.632241013.0000000003E41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.632241013.0000000003E41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.634690385.00000000057D0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.634690385.00000000057D0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.634690385.00000000057D0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000018.00000002.630682513.0000000002E62000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.625215508.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.625215508.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000018.00000002.625215508.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638041979.0000000006990000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638041979.0000000006990000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.637856242.0000000006930000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.637856242.0000000006930000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.638363567.00000000069F0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000018.00000002.638363567.00000000069F0000.00000004.00020000.sdmp, Author: Florian Roth

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis