ID: 452545
Sample Name: URGENT REQUEST FOR QUOTATION.exe
Cookbook: default.jbs
Time: 15:06:32
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

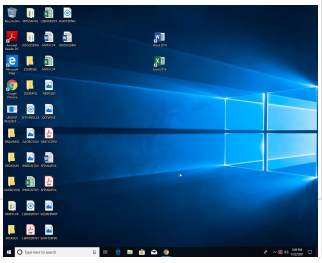
Windows Analysis Report URGENT REQUEST FOR QUO…

Overview

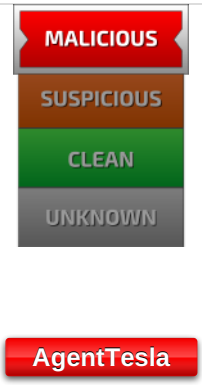
General Information

Sample Name:	URGENT REQUEST FOR QUOTATION.exe
Analysis ID:	452545
MD5:	436f3797fc4c39d..
SHA1:	1a93b32908c5de..
SHA256:	f7b11103bbd791d.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



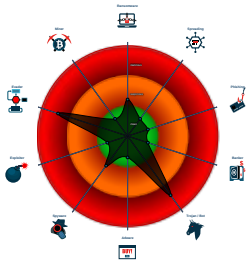
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- .NET source code contains very larg…
- Adds a directory exclusion to Windo…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- URGENT REQUEST FOR QUOTATION.exe (PID: 5464 cmdline: 'C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe' MD5: 436F3797FC4C39D1A2319196BC15C1C3)
  - powershell.exe (PID: 5516 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5788 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CCxRZUAFy.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4836 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CCxRZUAFy' /XML 'C:\Users\user\AppData\Local\Temp\tmpD0B6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6156 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CCxRZUAFy.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - URGENT REQUEST FOR QUOTATION.exe (PID: 6180 cmdline: C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe MD5: 436F3797FC4C39D1A2319196BC15C1C3)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "brucechuks212@vivaldi.net",
  "Password": "23456789@@@@",
  "Host": "smtp.vivaldi.net"
}
```


Yara Overview

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

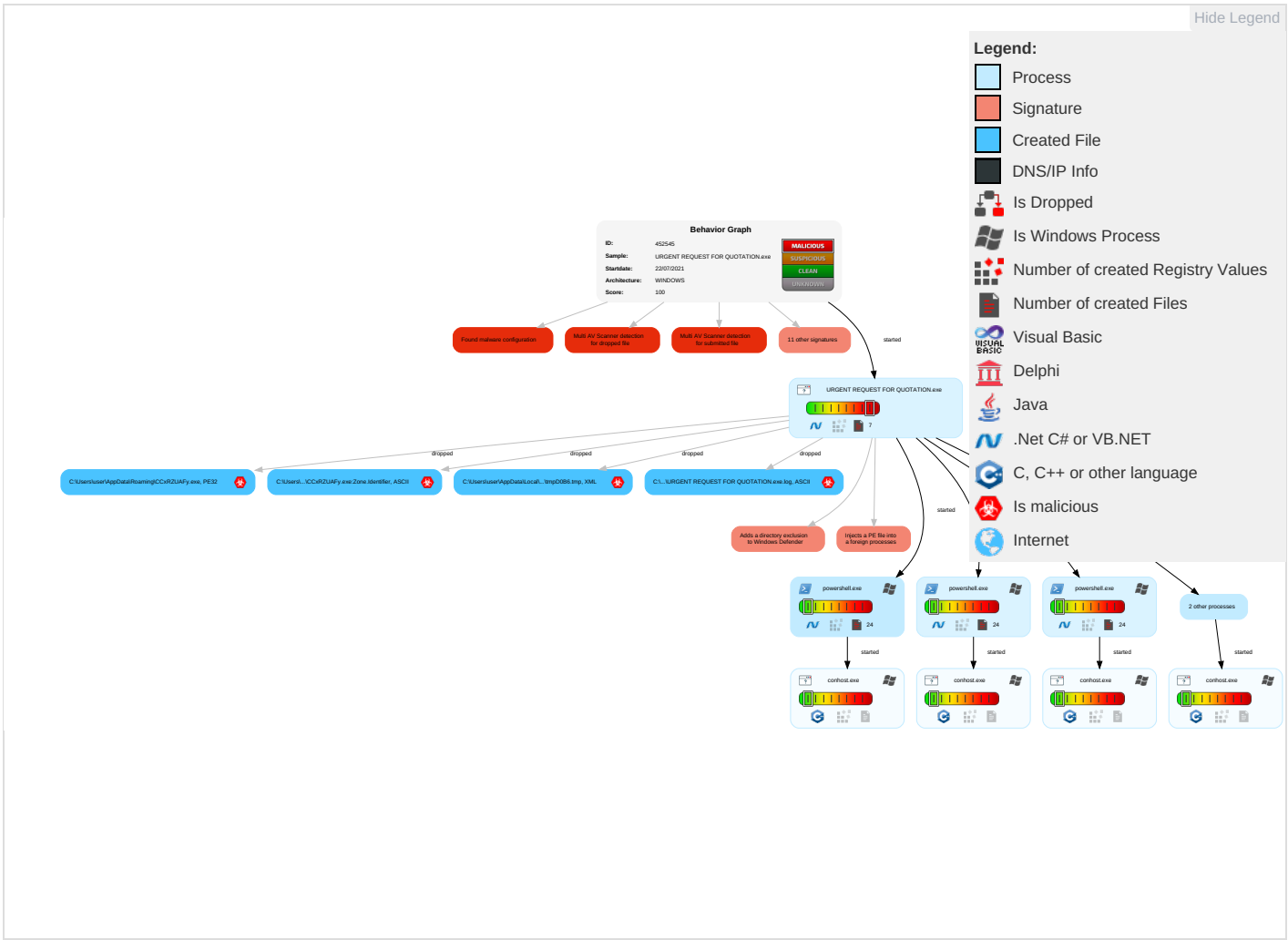
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	I
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	I
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	I
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	I
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	.
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	I

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
URGENT REQUEST FOR QUOTATION.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
URGENT REQUEST FOR QUOTATION.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\CCxRZUAFy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\CCxRZUAFy.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.URGENT REQUEST FOR QUOTATION.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Webd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/r	0%	Avira URL Cloud	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.microsoft.	0%	URL Reputation	safe	
http://www.carterandcone.comarT	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.y	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ers	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/roso	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdV	0%	Avira URL Cloud	safe	
http://qxLqgV.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://crl.microsof	0%	URL Reputation	safe	
http://crl.microsof	0%	URL Reputation	safe	
http://crl.microsof	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.fontbureau.comessedD	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.carterandcone.comadi	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.carterandcone.comlay	0%	Avira URL Cloud	safe	
http://www.carterandcone.cometh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/b	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/b	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/b	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452545
Start date:	22.07.2021
Start time:	15:06:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	URGENT REQUEST FOR QUOTATION.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:	32
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@15/18@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 1.3%) • Quality average: 66% • Quality standard deviation: 21.7%
HCA Information:	• Successful, ratio: 100% • 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
15:07:53	API Interceptor	388x Sleep call for process: URGENT REQUEST FOR QUOTATION.exe modified
15:08:00	API Interceptor	158x 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\URGENT REQUEST FOR QUOTATION.exe.log	
Process:	C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

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):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
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):	22352
Entropy (8bit):	5.602835259520916
Encrypted:	false
SSDEEP:	384:YtCDruDPEN94WkJKIC+RoSBKnGultIuP7Y9gxSTi1BMrm/Z1AV7kv8w564I+JzYB:UEcWgq4KGultxrxA24A9I
MD5:	158CE3622E7B2A3A0171CA62C6A5D08F
SHA1:	C79CC7E0C9AB10DDB443CB017895C198700C6D34
SHA-256:	824F3D803040C23A6FEAA5C567991AACA29B03DE10901F77AD78399C398AA3F9
SHA-512:	BB73F448250057E4705F1BE6C47D522F68F87570BC0FF8E185512379B4F4AD56285E5407B1A38C845ACD508BFB87837FE4997938DB92A251F9532FF1F8246D0C
Malicious:	false
Preview:	@...e.....R.y...q.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....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__PSScriptPolicyTest_atfsddvg.sju.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_atfsddvg.sju.ps1	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cfw4f2kf.lgt.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mby5lfvb.ykp.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uj2qse0o.fof.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w2ozaui5.3in.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w2ozaui5.3in.psm1	
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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xk3kxaoj.0rb.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
Preview:	 1

C:\Users\user\AppData\Local\Temp\tmpD0B6.tmp	
Process:	C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.178889471468902
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBcYtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3Z
MD5:	904F58B2E90F4AB00574DE411A33549F
SHA1:	CF3C774C3B00515D2CBD0A9AC6D26473832EB35D
SHA-256:	BC8A6B40FDCD693079716DF2B9743443C60565CF085811392BC151918296E3C9
SHA-512:	FB68C70FE0A9324C76439FB5220C285A5C34304723ECD6BB66906259253BA43B646DCE8B89376FA28D47AB26877F4FFD14EBD117D437B93C9DC7D84A076249B
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\CCxRZUAFy.exe	
Process:	C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	738304
Entropy (8bit):	7.598227533280257
Encrypted:	false
SSDEEP:	12288:fj1iM6WqpSH5vdGGmEKhJmrNX1xZ7/VY606/S0shF7XsyaUVKnp:fj1lV4SHvJmEKhKlL7K606Hshpzahp
MD5:	436F3797FC4C39D1A2319196BC15C1C3
SHA1:	1A93B32908C5DEF6129F192FD096F129EA575220
SHA-256:	F7B11103BBD791D5C2452275FF23FE51EFF41BA5071BA015EF50672138C9B459
SHA-512:	B7322A3A65D5493DF020B8746C3277511A103298FB8F985F8F13567B4967428CBD1D6F3071970C8E8BD027F071DF808EEA3D24F38F030F61BD3D256563292CE8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%

C:\Users\user\AppData\Roaming\CCxRZUAFy.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J..`.....P..8.....fW... ...`....@.. ....@.....W..O....`..... ..... ..H.....text....7... ...8..... ..`.rsrc.....`.....:.....@..@.rel oc.....B.....@..B.....HW.....H.....(.....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(. ...oE...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<..... ...~.....(4.....,!r...p.....(5...o6...s7.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\CCxRZUAFy.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.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**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210722\PowerShell_transcript.887849.2t_TENv_.20210722150759.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):	5825
Entropy (8bit):	5.391778186192845
Encrypted:	false
SSDEEP:	96:BZ1z6eNqqDo1ZfGZMA6eNqqDo1ZoyQ6jZ16eNqqDo1ZoLKK9Za:z
MD5:	268E84561ABAE4E11F17AAFDA39D1CFF
SHA1:	CB45B544D2815DA8A8ECF3A447B0083720106940
SHA-256:	847AEAE2110031F51A2FA6C5DDFA6B7D6906FD1BD2F94E67D1BC4D3A67ABF331
SHA-512:	B8374A3F7405ADBFE0E49A707D4DF775108EDB419FFA43E59503B8EB3CA5DF9838FE40E9F3AA36C43AA08CA486D567B47E4E7E18FE4C3546ED64655C95D62E D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210722150800..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\CCxRZUAFy.exe..Process ID: 6156..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: 20210722150800..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\CCxRZUAFy.exe..**********..Windows PowerShell transcript start..Start time: 20210722151326..Username: computer\user..RunAs User: DE

C:\Users\user\Documents\20210722\PowerShell_transcript.887849.CmVMk4On.20210722150759.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):	5825
Entropy (8bit):	5.394986426732518
Encrypted:	false
SSDEEP:	96:BZN6eN4qDo1ZSZk6eN4qDo1ZTyQ6jZo6eN4qDo1ZDLKKBTZLq:Qdq
MD5:	E20587313F3F7E8F2B3EF7C979594AD6
SHA1:	9787A4E54DF0F78145A83E53A160CEB8293CD1AA
SHA-256:	EFB3FEDFFB49E1D9B9D739E6E0AC8C2BFE0F5D0BFBF528D076E03FF56C4D9EE5
SHA-512:	DC304FFE413296EDC92FFD3C175B08820E408CE34EAF513F81ADB28B9436C1FD029CA55A4593AEEE6156C1427C2C84F32454E859C58530AC256C407738FE540
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210722150826..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\CCxRZUAFy.exe..Process ID: 5788..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: 20210722150826..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\CCxRZUAFy.exe..**********..Windows PowerShell transcript start..Start time: 20210722151626..Username: computer\user..RunAs User: DE

C:\Users\user\Documents\20210722\PowerShell_transcript.887849.tSO3nJDl.20210722150757.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped

C:\Users\user\Documents\20210722\PowerShell_transcript.887849.tSO3nJDl.20210722150757.txt	
Size (bytes):	3563
Entropy (8bit):	5.381517724278677
Encrypted:	false
SSDEEP:	96:BZx6eNKUqDo1ZMaZU6eNKUqDo1ZZqmEg0cEg0cEg0yZF:20dgAgAgF
MD5:	DB87767DD4402D72A44DAE34A7C1FFA5
SHA1:	2CAE9062D732301ACF9A8CD7B8F8D6EF1231D104
SHA-256:	2CD691AE85743FB44AFA8916B57FC39BE151164A9C748EFD244F7B8DDF8B6899
SHA-512:	FBF13E51D7D3689C8B50182099B021A4AC63D7FCD76354E34CFCD8982369F98ED4117A9AD194C60DA7B07817CACD6684EDB3082839D2A966E9B6BC682574A9
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210722150822..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 887849 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe..Process ID: 5516..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: 20210722150822..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe..**********..Command start time: 20210722151529..**********..PS>TerminatingError(Add-MpPreferen

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.598227533280257
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	URGENT REQUEST FOR QUOTATION.exe
File size:	738304
MD5:	436f3797fc4c39d1a2319196bc15c1c3
SHA1:	1a93b32908c5def6129f192fd096f129ea575220
SHA256:	f7b11103bbd791d5c2452275ff23fe51eff41ba5071ba015ef50672138c9b459
SHA512:	b7322a3a65d5493df020b8746c3277511a103298fb8f985f8f13567b4967428cbd1d6f3071970c8e8bd027f071df808eea3d24f38f030f61bd3d256563292ce8
SSDEEP:	12288:fj1iM6WqpSH5vdGGmEKhJmrNX1xZ7/VY606/S0shF7XsyaUVKnp:fj1lV4SHvJmEKhKlL7K606Hshpzahp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J..`.....P..8.....fW... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b5766
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F8CA4A [Thu Jul 22 01:30:50 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

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	0xb3784	0xb3800	False	0.784774057712	data	7.60723196503	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x608	0x800	False	0.3330078125	data	3.46823340289	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	0xc	0x200	False	0.044921875	data	0.101910425663	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: URGENT REQUEST FOR QUOTATION.exe PID: 5464 Parent PID: 5640

General

Start time:	15:07:24
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe'
Imagebase:	0xa70000
File size:	738304 bytes
MD5 hash:	436F3797FC4C39D1A2319196BC15C1C3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5516 Parent PID: 5464

General

Start time:	15:07:54
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe'
Imagebase:	0x1110000
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: 5816 Parent PID: 5516

General

Start time:	15:07:55
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: powershell.exe PID: 5788 Parent PID: 5464

General

Start time:	15:07:55
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CCxRZUAFy.exe'
Imagebase:	0x1110000
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: 3264 Parent PID: 5788

General

Start time:	15:07:56
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: schtasks.exe PID: 4836 Parent PID: 5464

General

Start time:	15:07:55
Start date:	22/07/2021

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CCxRZUAFy' /XML 'C:\Users\user\AppData\Local\Temp\tmpD0B6.tmp'
Imagebase:	0x290000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 2104 Parent PID: 4836

General

Start time:	15:07:56
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: powershell.exe PID: 6156 Parent PID: 5464

General

Start time:	15:07:57
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\CCxRZUAFy.exe'
Imagebase:	0x1110000
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: URGENT REQUEST FOR QUOTATION.exe PID: 6180 Parent PID: 5464

General

Start time:	15:07:57
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\URGENT REQUEST FOR QUOTATION.exe
Imagebase:	0xec0000
File size:	738304 bytes
MD5 hash:	436F3797FC4C39D1A2319196BC15C1C3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: conhost.exe PID: 6188 Parent PID: 6156

General

Start time:	15:07:57
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis