ID: 411703
Sample Name:
zUEBMx2U10.exe
Cookbook: default.jbs
Time: 05:21:01
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report zUEBMx2U10.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 6
Threatname: NanoCore 6
Yara Overview 6
Memory Dumps 6
Unpacked PEs 7
Sigma Overview 7
AV Detection: 7
E-Banking Fraud: 7
System Summary: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Signature Overview 7
AV Detection: 8
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Persistence and Installation Behavior: 8
Boot Survival: 8
Hooking and other Techniques for Hiding and Protection: 8
Malware Analysis System Evasion: 8
Anti Debugging: 9
HIPS / PFW / Operating System Protection Evasion: 9
Stealing of Sensitive Information: 9
Remote Access Functionality: 9
Mitre Att&ck Matrix 9
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 11
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 13
Public 14
Private 14
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16

JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 24
General 24
File Icon 24
Static PE Info 24
General 24
Entrypoint Preview 25
Data Directories 26
Sections 27
Resources 27
Imports 27
Version Infos 27
Network Behavior 27
Network Port Distribution 27
TCP Packets 28
UDP Packets 29
DNS Queries 31
DNS Answers 31
Code Manipulations 32
Statistics 32
Behavior 32
System Behavior 32
Analysis Process: zUEBMx2U10.exe PID: 6540 Parent PID: 5980 33
General 33
File Activities 33
File Created 33
File Written 33
File Read 34
Registry Activities 34
Key Created 34
Key Value Created 35
Analysis Process: svchost.exe PID: 6644 Parent PID: 560 35
General 35
File Activities 35
Analysis Process: powershell.exe PID: 6768 Parent PID: 6540 35
General 35
File Activities 36
File Created 36
File Deleted 36
File Written 36
File Read 39
Analysis Process: conhost.exe PID: 6776 Parent PID: 6768 42
General 42
Analysis Process: powershell.exe PID: 6792 Parent PID: 6540 42
General 42
Analysis Process: conhost.exe PID: 6844 Parent PID: 6792 42
General 42
Analysis Process: powershell.exe PID: 6884 Parent PID: 6540 43
General 43
Analysis Process: conhost.exe PID: 6940 Parent PID: 6884 43
General 43
Analysis Process: cmd.exe PID: 7112 Parent PID: 6540 43
General 43
Analysis Process: conhost.exe PID: 7148 Parent PID: 7112 44
General 44
Analysis Process: timeout.exe PID: 5784 Parent PID: 7112 44
General 44
Analysis Process: zUEBMx2U10.exe PID: 2940 Parent PID: 6540 44
General 44
Analysis Process: svchost.exe PID: 6276 Parent PID: 3440 44
General 44
Analysis Process: zUEBMx2U10.exe PID: 3800 Parent PID: 6540 45
General 45
Analysis Process: svchost.exe PID: 6384 Parent PID: 560 45
General 45
Analysis Process: zUEBMx2U10.exe PID: 6516 Parent PID: 6540 45

General 45
Analysis Process: svchost.exe PID: 6480 Parent PID: 3440 46
General 46
Analysis Process: svchost.exe PID: 6728 Parent PID: 560 46
General 46
Analysis Process: WerFault.exe PID: 6680 Parent PID: 6728 46
General 46
Analysis Process: WerFault.exe PID: 6876 Parent PID: 6540 47
General 47
Analysis Process: svchost.exe PID: 6256 Parent PID: 560 47
General 47
Analysis Process: svchost.exe PID: 3224 Parent PID: 560 47
General 47
Analysis Process: svchost.exe PID: 2276 Parent PID: 560 47
General 47
Analysis Process: powershell.exe PID: 3624 Parent PID: 6276 48
General 48
Analysis Process: conhost.exe PID: 7044 Parent PID: 3624 48
General 48
Analysis Process: powershell.exe PID: 1768 Parent PID: 6276 48
General 48
Analysis Process: conhost.exe PID: 4264 Parent PID: 1768 49
General 49
Disassembly 49
Code Analysis 49

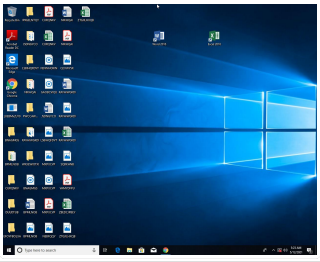
Analysis Report zUEBMx2U10.exe

Overview

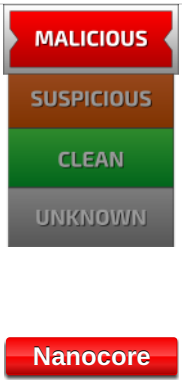
General Information

Sample Name:	zUEBMx2U10.exe
Analysis ID:	411703
MD5:	9b2b7acc05e281..
SHA1:	9316ff35c185dcf…
SHA256:	92781fa0c501e43.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



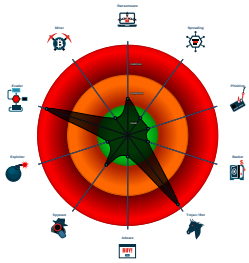
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains very larg…
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…
- Checks for kernel code integrity (NtQ…
- Creates an autostart registry key po…
- Drops PE files with benign system n…
- Drops executables to the windows d…

Classification



Startup

- **System is w10x64**
- zUEBMx2U10.exe (PID: 6540 cmdline: 'C:\Users\user\Desktop\zUEBMx2U10.exe' MD5: 9B2B7ACC05E281C17F978028722B51E9)
  - powershell.exe (PID: 6768 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6792 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\zUEBMx2U10.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6884 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 7112 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5784 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - zUEBMx2U10.exe (PID: 2940 cmdline: C:\Users\user\Desktop\zUEBMx2U10.exe MD5: 9B2B7ACC05E281C17F978028722B51E9)
  - zUEBMx2U10.exe (PID: 3800 cmdline: C:\Users\user\Desktop\zUEBMx2U10.exe MD5: 9B2B7ACC05E281C17F978028722B51E9)
  - zUEBMx2U10.exe (PID: 6516 cmdline: C:\Users\user\Desktop\zUEBMx2U10.exe MD5: 9B2B7ACC05E281C17F978028722B51E9)
  - WerFault.exe (PID: 6876 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6540 -s 1760 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6644 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6276 cmdline: 'C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' MD5: 9B2B7ACC05E281C17F978028722B51E9)
  - powershell.exe (PID: 3624 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1768 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6384 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6480 cmdline: 'C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' MD5: 9B2B7ACC05E281C17F978028722B51E9)
- svchost.exe (PID: 6728 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6680 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 6540 -ip 6540 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6256 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3224 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2276 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-000c0a4c",
  "Group": "backup july",
  "Domain1": "backupjuly.duckdns.org",
  "Domain2": "backupjuly.duckdns.org",
  "Port": 9090,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.680956480.0000000006E35000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10f25:$x1: NanoCore.ClientPluginHost • 0x43d45:$x1: NanoCore.ClientPluginHost • 0x10f62:$x2: IClientNetworkHost • 0x43d82:$x2: IClientNetworkHost • 0x14a95:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x478b5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.680956480.0000000006E35000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.680956480.0000000006E35000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10c8d:$a: NanoCore • 0x10c9d:$a: NanoCore • 0x10ed1:$a: NanoCore • 0x10ee5:$a: NanoCore • 0x10f25:$a: NanoCore • 0x43aad:$a: NanoCore • 0x43abd:$a: NanoCore • 0x43cf1:$a: NanoCore • 0x43d05:$a: NanoCore • 0x43d45:$a: NanoCore • 0x10cec:$b: ClientPlugin • 0x10eee:$b: ClientPlugin • 0x10f2e:$b: ClientPlugin • 0x43b0c:$b: ClientPlugin • 0x43d0e:$b: ClientPlugin • 0x43d4e:$b: ClientPlugin • 0x10e13:$c: ProjectData • 0x43c33:$c: ProjectData • 0x1181a:$d: DESCrypto • 0x4463a:$d: DESCrypto • 0x191e6:$e: KeepAlive
00000001.00000002.651427825.00000000042A1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3bf7ed:$x1: NanoCore.ClientPluginHost • 0x3bf82a:$x2: IClientNetworkHost • 0x3c335d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.651427825.00000000042A1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.zUEBMx2U10.exe.6e35d98.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1.2.zUEBMx2U10.exe.6e35d98.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
1.2.zUEBMx2U10.exe.6e35d98.8.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.zUEBMx2U10.exe.6e35d98.8.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
1.2.zUEBMx2U10.exe.6e68bb8.9.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 9 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

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
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large strings

Persistence and Installation Behavior:

- Drops PE files with benign system names
- Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

- Creates an autostart registry key pointing to binary in C:\Windows

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

Hides threads from debuggers

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 Nanocore RAT

Remote Access Functionality:

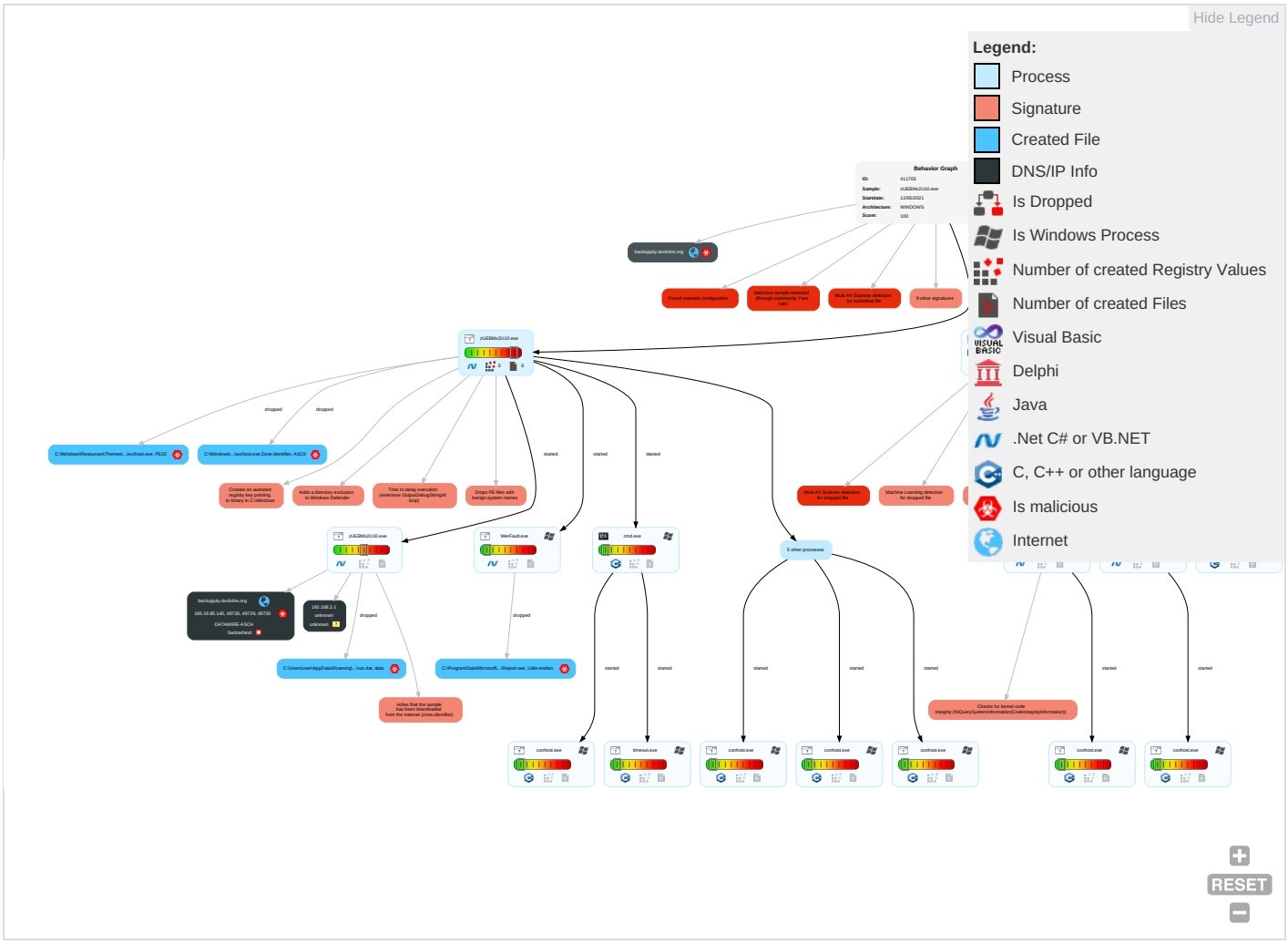
Detected Nanocore Rat

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	Networ Effects
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1 1	Process Injection 1 1 1	Masquerading 2 2 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 4 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 5 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Virtualization/Sandbox Evasion 3 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecur Protocc

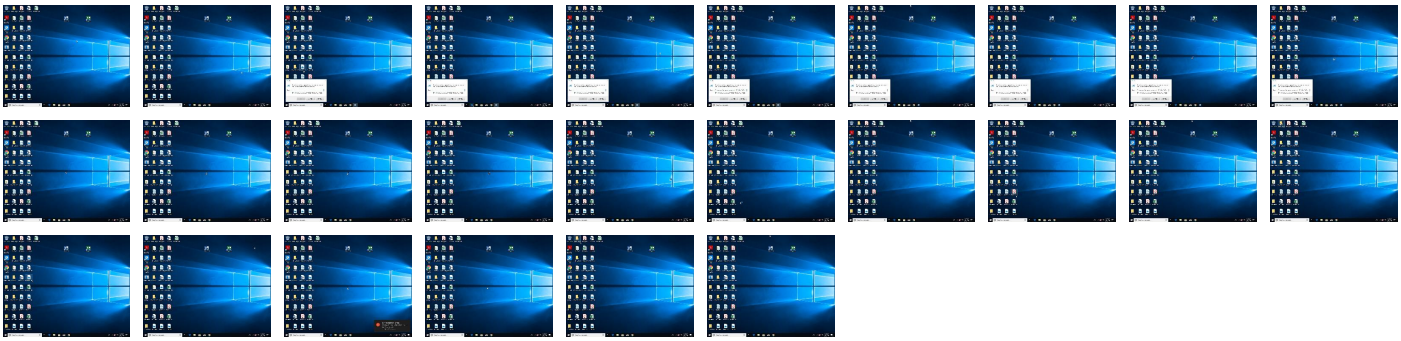
Behavior Graph



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
zUEBMx2U10.exe	43%	Virustotal		Browse
zUEBMx2U10.exe	38%	Metadefender		Browse
zUEBMx2U10.exe	76%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
zUEBMx2U10.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe	100%	Joe Sandbox ML		
C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe	38%	Metadefender		Browse
C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe	76%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
backupjuly.duckdns.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	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://https://go.microd	0%	Avira URL Cloud	safe	
backupjuly.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
backupjuly.duckdns.org	185.19.85.140	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

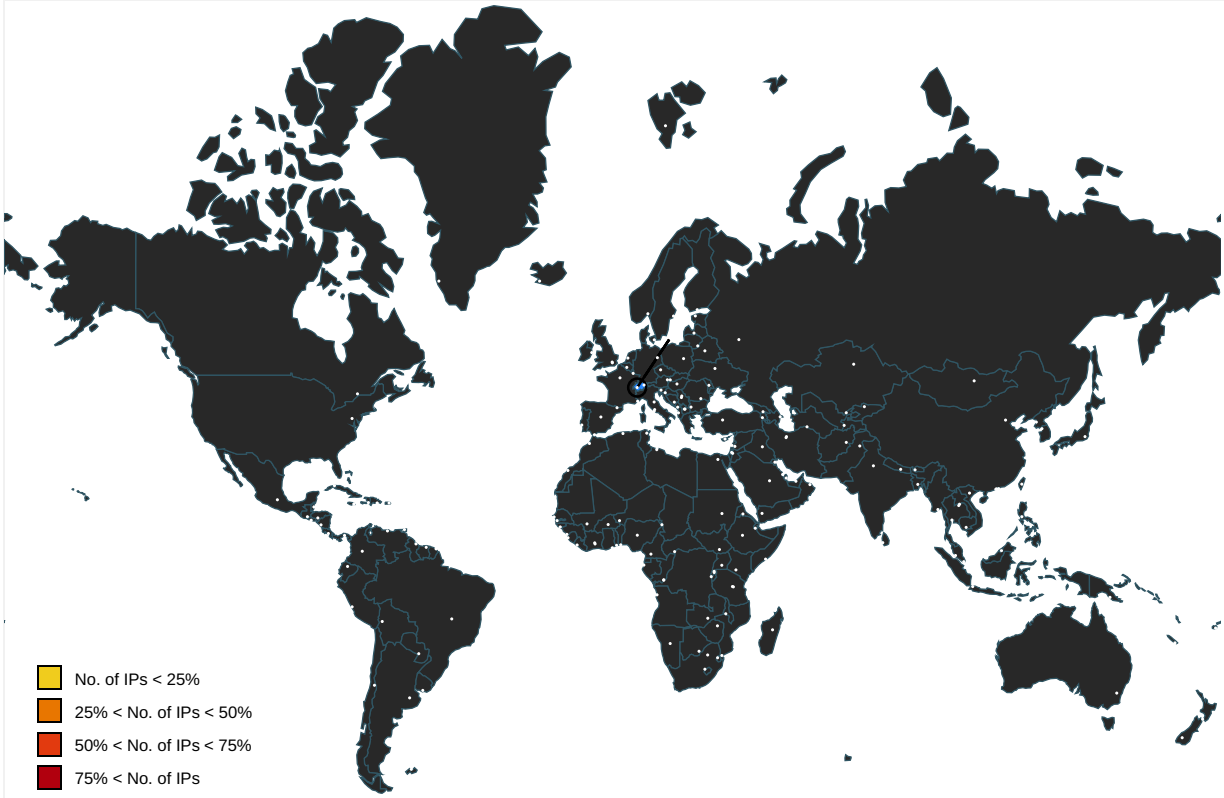
Name	Malicious	Antivirus Detection	Reputation
backupjuly.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 00000016.00000003.457240955.0000000004EA0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 00000016.00000003.457240955.0000000004EA0000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000007.00000003.496753193.0000000007457000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 00000016.00000003.457240955.0000000004EA0000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000007.00000003.496753193.0000000007457000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 0000001D.00000003.512531285.0000020C43573000.00000004.00000001.sdmp, svchost.exe, 0000001D.00000003.512818639.0000020C4358F000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000005.00000003.486985985.0000000005A9B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.roblox.com/develop	svchost.exe, 0000001D.00000003.512531285.0000020C43573000.00000004.00000001.sdmp, svchost.exe, 0000001D.00000003.512818639.0000020C4358F000.00000004.00000001.sdmp	false		high
http://https://instagram.com/hiddencity_	svchost.exe, 0000001D.00000003.497552515.0000020C435A6000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 00000016.00000003.457240955.0000000004EA0000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://https://go.microd	powershell.exe, 00000007.00000 003.507167541.0000000004D32000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://https://corp.roblox.com/parents/	svchost.exe, 0000001D.00000003 .512531285.0000020C43573000.00 000004.00000001.sdmp, svchost.exe, 0000001D.00000003.5128186 39.0000020C4358F000.00000004.0 0000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddressszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000007.00000 003.496753193.0000000007457000 .00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 0000001D.00000003 .497552515.0000020C435A6000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://https://www.roblox.com/info/privacy	svchost.exe, 0000001D.00000003 .512531285.0000020C43573000.00 000004.00000001.sdmp, svchost.exe, 0000001D.00000003.5128186 39.0000020C4358F000.00000004.0 0000001.sdmp	false		high
http://www.g5e.com/termsofservice	svchost.exe, 0000001D.00000003 .497552515.0000020C435A6000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprinthttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 0000001D.00000003 .512531285.0000020C43573000.00 000004.00000001.sdmp, svchost.exe, 0000001D.00000003.5128186 39.0000020C4358F000.00000004.0 0000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	WerFault.exe, 00000016.0000000 3.457240955.0000000004EA0000.0 0000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.85.140	backupjuly.duckdns.org	Switzerland		48971	DATAWIRE-ASCH	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411703
Start date:	12.05.2021
Start time:	05:21:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zUEBMx2U10.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:	40
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@48/28@11/3
EGA Information:	Failed
HDC Information:	Failed
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 • Excluded IPs from analysis (whitelisted): 92.122.145.220, 40.88.32.150, 20.82.210.154, 2.20.143.16, 2.20.142.209, 92.122.213.194, 92.122.213.247, 20.54.26.129, 52.155.217.156, 13.64.90.137, 23.218.208.56, 20.82.209.183, 52.255.188.83, 13.88.21.125 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
05:22:06	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce 9EO342rLb92o62 C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe
05:22:15	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce 9EO342rLb92o62 C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe
05:22:36	API Interceptor	765x Sleep call for process: zUEBMx2U10.exe modified
05:22:50	API Interceptor	177x Sleep call for process: powershell.exe modified
05:23:08	API Interceptor	12x Sleep call for process: svchost.exe modified
05:23:21	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.19.85.140	Memorandum of PCR test.exe	Get hash	malicious	Browse	
	Memorandum of PCR test.pdf.exe	Get hash	malicious	Browse	
	Memorandum on PCR test 001.pdf.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DATAWIRE-ASCH	remittance slip.pdf.exe	Get hash	malicious	Browse	• 185.19.85.139
	968927d6_by_Libranalysis.exe	Get hash	malicious	Browse	• 185.19.85.142
	b98b396b_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 185.19.85.142
	PL-REM-40310EMEA02 (0085).jar	Get hash	malicious	Browse	• 185.19.85.166
	Appraisal.reportl1100445269900.vbs	Get hash	malicious	Browse	• 185.19.85.168
	Appraisal.property..vbs	Get hash	malicious	Browse	• 185.19.85.168
	Appraisal.vbs	Get hash	malicious	Browse	• 185.19.85.168
	Appraisal.vbs	Get hash	malicious	Browse	• 185.19.85.168
	p8Up8qw5.exe	Get hash	malicious	Browse	• 185.19.85.148
	867353735-2021 Presentation Details.vbs	Get hash	malicious	Browse	• 185.19.85.165
	867353735-2021 Presentation Details.vbs	Get hash	malicious	Browse	• 185.19.85.165
	VIS_MAL.txt.ps1	Get hash	malicious	Browse	• 185.19.85.134
	P195 NOVO Cinema#2021.exe	Get hash	malicious	Browse	• 185.19.85.134
	INVOICE_.EXE	Get hash	malicious	Browse	• 185.19.85.171
	New Order 567w43.exe	Get hash	malicious	Browse	• 185.19.85.139
	yZykshDGPX.exe	Get hash	malicious	Browse	• 185.19.85.162
	Cancellation_Request_pdf.hta	Get hash	malicious	Browse	• 185.19.85.169
	sfTZCyMKuC.exe	Get hash	malicious	Browse	• 185.19.85.137
	Booking vouchers.exe	Get hash	malicious	Browse	• 185.19.85.134
	PurchaseOrder_2021676777.exe	Get hash	malicious	Browse	• 185.19.85.141

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5958226129883873
Encrypted:	false
SSDEEP:	6:bIE2k1GaD0JOCEfMuaaD0JOCEfMKQmD411Al/gz2cE0fMbhEZolrRSQ2hyYIIT:bICGaD0JcaaD0JwQQ0Ag/0bjSQJ
MD5:	87306F78951BD3787587D871BEB0576F
SHA1:	EEA20FE290598065D9BFE47EBBC26A754A808A9D

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
SHA-256:	FA205688D9A66BFED57CCB6BAA2F5EE4D9C2AA97B2F5C41F16C3983A255E31BB
SHA-512:	37D2B1EF9F686AB86E9A4EB1BB2AA730FDA3A5409E00ABCC822FAD66391BC281A5EE8731B7E975E74C264A9E1F67088AD8DB30BED8DB440F1DC64FCC7D29B2E1
Malicious:	false
Preview:	....E..h..(.....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x4279f839, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09541840300770617
Encrypted:	false
SSDEEP:	6:/Gzwl/+zYc1RIE11Y8TRXxw8JM/qKdGzwl/+zYc1RIE11Y8TRXxw8JM/qK:e0+ZO4ble8GqKY0+ZO4ble8GqK
MD5:	158B2CE0BAE4BFDB76929BC97D4ED111
SHA1:	15E99D6C6F156E69607BACDD0FDC97D61A8FDEAB
SHA-256:	201C9AECACABF965D1BCC3A96F6C8648131CA20628BA537096BFD4563F9E4463
SHA-512:	4313CFACB946053B6165E4BE52786D76C87B0EE60F0A3D90A0D375D4EB66895BFF1F89EF746EE8D7E54C01949A0A4645B038F62B8DB5EC253BE583AE2EF5A357
Malicious:	false
Preview:	By.9... .....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... ....3...w..... .....}Q\.....y!{.....5.w@.....y!..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11008638410518784
Encrypted:	false
SSDEEP:	3:0Slll1Evx6zpl+uXl/bJdAtijSl8g//ill:NlYY+At4QM/G
MD5:	32BF03765B201C794379B2886F7DFAAA
SHA1:	E08202B3B58DD149B3E0B8D460B76A5626BDC126
SHA-256:	66BEC12E8D18E3B60AF7FDB42B82BC36E55B6EC7D169444D72AA7B5B3FBFDC08
SHA-512:	FABC8E6B3F216D1E5B05DC8B2091277662256F5A44CE7DA3F27D389CB428D6DBA9DDBA4FD597458806594634EF4D60DA5754A81A89A8375F79617B63DB34125
Malicious:	false
Preview:	.....3...w.....y!.....w.....w.....w....:O.....w.....5.w@.....y!..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zUEBMx2U10.exe_78eefa6469bab2f3c8b6995723de54eaa9f64f5_e1271c13_1a835371\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15168
Entropy (8bit):	3.772575452690747
Encrypted:	false
SSDEEP:	192:oKvDOyUlumHBUZMXSaKA6KZDnyK/u7swS274ltP+:ocOhfBUZMXSaNyK/u7swX4ltP+
MD5:	39A5705C28EFF9F9115F765B235D600D
SHA1:	2E507030B705FAE93A036D6BE596005B9ADAB280
SHA-256:	EA0C60CECCD2B89D2155AE9B9794CF7CCF4597E3153B7174B01CFFBA9B142FA4
SHA-512:	BD759F5505DF9D37528825C13056EB6C6E2CEF432F1A224D5F49B35BECB8D8601814E6150116C244BE0DF285B5721A3C8FD6D63DC7A19E23B3A25F6CF144FF2
Malicious:	**true**

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_zUEBMx2U10.exe_78eefa6469bab2f3c8b6995723de54eaa9f64f5_e1271c13_1a835371\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.2.9.5.7.5.7.7.0.3.2.7.8.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.2.9.5.7.9.8.0.4.6.8.3.4.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.b.9.5.a.0.4.a.-.b.5.f.7.-.4.8.f.f.-.9.8.6.6.-.2.c.0.f.b.0.c.5.6.3.9.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.7.a.f.6.e.6.6.-.d.3.b.f.-.4.1.6.f.-.a.b.6.4.-.c.e.0.9.6.0.f.5.7.b.2.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.z.U.E.B.M.x.2.U.1.0...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.f.i.r.s.t.o.f.t.h.e.d.a.y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.8.c.-.0.0.0.1.-.0.0.1.7.-.1.f.d.a.-.5.8.6.3.2.9.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.5.d.1.6.d.f.a.d.6.e.4.2.6.3.2.9.0.4.6.3.0.3.6.0.7.5.2.1.6.9.c.0.0.0.0.0.0.0.0.!.0.0.0.0.9.3.1.6.f.f.3.5.c.1.8.5.d.c.f.3.c.8.0.c.2.c.3.a.b.2.f.f.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER181E.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696982552174106
Encrypted:	false
SSDEEP:	96:9GiZYW6AzLm/xNYpYaVXWYnIKHtYEZFSt6i6Cq1anwbUH1riamDaxTLIoH3:9jZD6hNefIM7K12amDaxTEoH3
MD5:	637D4D0440F4D049456A47DDA2D36250
SHA1:	6E29AE01893B93BB533E749F5987B68DDA79B972
SHA-256:	210076BDA8F549E60A49EC523AFE682E808D23A05E2FCC167CCAD210F137900A
SHA-512:	1097BEE406A188579C9F3220C966EC35667026014A9BABACE5AEB2D8CBD745BF691E927DE196C6BE293340F2040519FE83CF879DE1EC95E1305F67B2ECCC304C
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A36.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	58944
Entropy (8bit):	3.0571025518576973
Encrypted:	false
SSDEEP:	1536:xGHqNPEqc/iKt3BH8ATAYElNbVGZFY2gHfSW8f:xGHqNPEqc/iKt3BH8ATAYEnbVGZFY2g2
MD5:	86E89D5FE7CF3A80FB59420EE8CC4B9B
SHA1:	95C66477998366246D15E8AB999D90AEED6BEB07
SHA-256:	7D5C6325908AE0C057D35338B114364A159E78849803E6CEAE340B2C1A674A4D
SHA-512:	7D84764E1A31915732AC0582A2233E3183908F23386FA5B008CC3D6CFEE3A636DF9724D13F232683F4914655073B44FF875D283872625FE61CD949CD5A9C091F
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER589F.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.697141196280185
Encrypted:	false
SSDEEP:	96:9GiZYWKpvWZvGGYQjYmWn+HxYEZg5t3iAqWfQwIOvaoYyba9uIIZ3:9jZDbQGVj8uAaoYybaTIZ3
MD5:	510C45A6592056553AC63F4968EABAD0
SHA1:	73FBE155F9199A64F2BA782BAF6F6905DB2A74D2
SHA-256:	BB4D39070AC844F489107E8054EF5F1C3BA4BFCC6B14C695435C3691489D23EE
SHA-512:	FE3C03EF6E5F3A14CF81D37E95627ECD4B6CE9375FC73CBBA66C94AE808835E35B5B7117A8BB543F28E91E59645A69DEC6453FA8F4514579791D1B132DCD747D
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6E9.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4753
Entropy (8bit):	4.485781982557908
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9oGWSC8BYb8fm8M4JCiFFR+q8vViBAo80d:uITfhbHSNGYJVKuAo/d
MD5:	B9A973CC04B128D87032237E0E10CC66
SHA1:	B882B98974A8A53B92B54DD941FE771FCF554D01
SHA-256:	03CCC40385E487425ABE03A1C21E498640F3CCDECCFC7E990B6FAD9D8B1FA1D6
SHA-512:	1588F3CCDA280391B683CB10BB89E2F6E5C4CD20CE1E36DF0961F78937B3BC0F47B77D7D8F6C251FF487D3AAA8A3B0333EF5EF551E3FED9BD47DE4F03653B28
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="986253" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER716.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	56228
Entropy (8bit):	3.0625949262184773
Encrypted:	false
SSDEEP:	1536:j6H6MLtKN06xBLeHxAK+vuiXzzFGZCEpJIRNFCG:j6H6MLtKN06xBLeHxAK+v9XzzFGZCEpo
MD5:	3A17C870469D8BB2B909FBA7DED15A03
SHA1:	62E3F24D0E2B3035F3DA819DB45600B4B4B7117A
SHA-256:	6E56C33E71BFCCE9DB722CF225902A1C48A8EA19C6214A3438EAE820AE179C48
SHA-512:	379184342EDF4CF5C6A7D04C9511E03F7C0AE0C4CE37D035B33E52EA5971AD89C1B4DCAD7EA4A77268EE57313DC313BCB9E70CBA6001D93EB1C4AEBCC15D962
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA985.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 12 12:22:55 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	272356
Entropy (8bit):	3.878367992737439
Encrypted:	false
SSDEEP:	3072:I7s5Qu01GOjd+p6p6r5D69gIOgF54d0HUCgUukoZP2fR:P0sLpsJ9RpDSUTjukLZ
MD5:	294145C1B9BF2FA2BA10327C9A1866A0
SHA1:	C5337481A0144CD109270EB56B907BFF63733FDB
SHA-256:	5AC2047BFC75F4BF87B82C00720667A716BAB6D7C4DF5DA059129B5D5B0DD2BF
SHA-512:	110460301EDBBDCA459A3FC4223BD8C30C169AF47DB4BFA466DFE9789A5FE1813C1CA2DF163D3A82198BD794762D3339E0A5BA2AEC45E10E0B708955FE24118
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....t&.....GenuineIntelW.....T....._.`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF842.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8406
Entropy (8bit):	3.698829527938305

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF842.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilU6fj6YJDSUacZZgmfZPSBCprd89bLPsfPtZm:RrlsNiG6fj6YdSUacZZgmfRSjL0fP6
MD5:	A0E276EED1D6DBFCE8D480F8F3449B32
SHA1:	B225F1BDAED285C408DDBC60C8676CBA1EBDE820
SHA-256:	0AEC53F74EE6C6F7B12668DA50C3B560AC8FBDAAED5769862C74CB09FD7A818F
SHA-512:	E359B8C20DE5DDEC8530992DB9FEF26A202076E6480C7FB3425DD09233AC0C823DD5482671509007FD64D108A7F4E2D358DF339B5BA0D2A631A845A5FBFA248
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.5.4.0.<./.P.i.d.>.....

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):	25168
Entropy (8bit):	4.975582086060887
Encrypted:	false
SSDEEP:	768:6BV3IpNBQkj2Lh4iUxQedNYotBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYoI:6BV3CNBQkj2Lh4iUxvdNYotBV3CNBQkx
MD5:	62E1AE94DE84ED9286704EBD6856A263
SHA1:	4888C4CFAA74FA9BCD7339CBF760B1060314246B
SHA-256:	9AC3E181F8EB940093EF7F212696338C30CD1407AF8ECB25610C39D6B00D4C43
SHA-512:	E99B7BA733C622C675AA7944338E994EE0D941663D812D702D986F4C162C4BC40FA2C837C6C761598B826A8CB7157DFBDDC20932B41B3D637209B3333BEEEB3
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\Temp__PSScriptPolicyTest_0ppcodrv.gyz.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_1v0s3drz.b2l.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_bnck3iqu.cd0.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_jxa21zr3.o5a.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_nxvdofi2.t21.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_uludn5pk.srf.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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\zUEBMx2U10.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhL
MD5:	30D23CC577A89146961915B57F408623
SHA1:	9B5709D6081D8E0A570511E6E0AAE96FA041964F
SHA-256:	E2130A72E55193D402B5F43F7F3584ECF6B423F8EC4B1B1B69AD693C7E0E5A9E
SHA-512:	2D5C5747FD04F8326C2CC1FB313925070BC01D3352AFA6C36C167B72757A15F58B6263D96BD606338DA055812E69DDB628A6E18D64DD59697C2F42D1C58CC68
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?. ..A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH }..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f. ..p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\zUEBMx2U10.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:2FNn:2FN
MD5:	B9BC5CD5EAF6A468D168FB442D2E8F9B
SHA1:	7353405914980EEF7C77A9B073F055A3A605A515
SHA-256:	8882268570AB664B41A35932220BB9CA45EB1FC1840433D086861B029055F325
SHA-512:	91D483A09B0924C53076BE4D8EA83A3CF882145A4802AAE50F3B9FF93261BABE34152EBA8568274CDA7355A73D28A0514878B22E47BB1EF47BCEBB28486D05B
Malicious:	**true**
Preview:	.8..@..H

C:\Users\user\Documents\20210512\PowerShell_transcript.760639.0gogqNuT.20210512052206.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):	1670
Entropy (8bit):	5.409109800001059
Encrypted:	false
SSDEEP:	48:BZyvTL7oO+SWrCaqDYB1ZFWr8ZxvTL7oO+SWrCaqDYB1ZA:BZOTL7NQrNqDo1ZQr8Z9TL7NQrNqDo1m
MD5:	E721A80A2E19603A6D3D58612B752908
SHA1:	A879BA89D2D04B4495B6599F9EEBA7B1FFAFD810
SHA-256:	A9CC9D35C03DC87A11560A8C271CCB8753953073DBE34FB8C080D3B45E779EE9
SHA-512:	0FF90B271CDFEFAF5362FF2EEAE99ED3F01E4E762C5E69B5C5C37A23B0CD4033E31A66B3DB7B190886E5C30563780FB76EDC253CAEAAC8EC768EBF0AB4B5E 711
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210512052235..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe -Force..Process ID: 6884..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: 20210512052236..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe -Force..********** ..Windows PowerShell transcript star

C:\Users\user\Documents\20210512\PowerShell_transcript.760639.6iHHi+Z_.20210512052205.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):	1670
Entropy (8bit):	5.404428336497538
Encrypted:	false
SSDEEP:	48:BZ1vTL7oO+SWrCjqDYB1ZqWr8ZhvTL7oO+SWrCjqDYB1ZA:BZ5TL7NQrQqDo1Zjr8ZNTL7NQrQqDo1m
MD5:	95CF25D28B6DD66BBD65DC6981EE268C
SHA1:	DD8240ABD38443DC2D1B842A4BE75D60ADAA04F6

C:\Users\user\Documents\20210512\PowerShell_transcript.760639.6iHHi+Z_.20210512052205.txt	
SHA-256:	7DB258F10C5C48BD65DF0A3D7C796D2C79F493607A682309B8C3C50381B3FD69
SHA-512:	47C5F49146563B84CBF486828C6C78690F91DC8561C1BD45AAE272D2B1143632A0A41134096ACBB11F465D5463B80B744A40420C813BD25286644794E5729D47
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210512052230..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe -Force..Process ID: 6768..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: 20210512052231..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe -Force..**********..Windows PowerShell transcript star

C:\Users\user\Documents\20210512\PowerShell_transcript.760639.yQJTMGoZ.20210512052205.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):	5157
Entropy (8bit):	5.40281500495079
Encrypted:	false
SSDEEP:	96:BZ0TL7NT3qDo1ZQZMTL7NT3qDo1Zm4yQjZcTL7NT3qDo1ZKZA9:QXct
MD5:	C842B072D4CD14B613110323B78EEC3B
SHA1:	FD9727C0CA8A4AADA32EB9B2F8D6771A11A3C9F7
SHA-256:	4C877AB28F383BBD5FFD805D2F7108181C416BEC4592A20F5344A4789DF3B176
SHA-512:	D3C6238D1651F5E0D2DCD171E071474DB2FD88AE23B07F33A53084F7B4CF3A484F00D627589514812362ABEF3B237D232590AE5D572EEB3FB9564168416C0F3F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210512052228..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\zUEBMx2U10.exe -Force..Process ID: 6792..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: 20210512052229..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\zUEBMx2U10.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210512053304..Username: computer\user..RunAs User: DESKTOP

C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe	
Process:	C:\Users\user\Desktop\zUEBMx2U10.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3858432
Entropy (8bit):	2.557351272214791
Encrypted:	false
SSDEEP:	1536:cGEBIZ5HlFuxK0Roj0whXkyiaCVS1nKT+jQdvWxdisWf52MvAsqPqMxm/wr59vEZ:cx
MD5:	9B2B7ACC05E281C17F978028722B51E9
SHA1:	9316FF35C185DCF3C80C2C3AB2FF55FF1076652A
SHA-256:	92781FA0C501E4375F625A6E8379BBE8F0D7D42FD6699981233A044222E081D4
SHA-512:	BE7BA4787433FB3FABCBC66088553FB424A65DD1C654E23458805019A2E156B4296495AE044918A49F4DFB846CC646DB26DB34704C0F3B8218CE721D0A282B24
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 38%, Browse • Antivirus: ReversingLabs, Detection: 76%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6.....".....0.....:.....:.. ....;...@.. .....@;..... ..@.....d.:.W....;..... ;..... ..H.....text....:.. ....:..... ..`.rsrc.....;.....:.....@..@.reloc..... ;.....:.....@..B.....:.....H.....8%...:.....$.....*".(.....*^..}.....(.....(.....*...s....}.....(..... ... .s....(.....r..:po!....*&.(.....*".....*".(%.... *Vs....(&...t.....*....0.....s.....+.....o.....*..0.....s.....s.....(.....+.....r...po.... ....[..(.....(.....(.....l.....,+.....+.r...po.....o.....,+....X.....+.....%.. .o.....+ l.....o.....,.+)..r..:p(.....,+....

C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\zUEBMx2U10.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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**

C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.557351272214791
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	zUEBMx2U10.exe
File size:	3858432
MD5:	9b2b7acc05e281c17f978028722b51e9
SHA1:	9316ff35c185dcf3c80c2c3ab2ff55ff1076652a
SHA256:	92781fa0c501e4375f625a6e8379bbe8f0d7d42fd6699981233a044222e081d4
SHA512:	be7ba4787433fb3fabcbc66088553fb424a65dd1c654e23458805019a2e156b4296495ae044918a49f4dfb846cc646db26db34704c0f3b8218ce721d0a282b24
SSDEEP:	1536:cGEBIZ5HlFuxK0Roj0whXkyiaCVS1nKT+jQdvWxdisWf52MvAsqPqMxm/wr59vEZ:cx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6....."...0...:.....:. ....;...@.. .....@;.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x7af4be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x8236B8BB [Fri Mar 25 00:05:15 2039 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3af464	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b0000	0x5c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3b2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x3ad4c4	0x3ad600	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x3b0000	0x5c8	0x600	False	0.416015625	data	4.10885896675	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3b2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x3b00a0	0x33c	data		
RT_MANIFEST	0x3b03dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	firstoftheday.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	firstoftheday
ProductVersion	1.0.0.0
FileDescription	firstoftheday
OriginalFilename	firstoftheday.exe

Network Behavior

Network Port Distribution

Total Packets: 90

- 53 (DNS)
- 9090 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 05:22:42.181093931 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:42.535836935 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:42.535957098 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:43.021526098 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:43.417398930 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:43.436244011 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:43.756023884 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:43.800909996 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:44.793487072 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.233567953 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.233639002 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.233707905 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.233779907 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.234361887 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.234433889 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.234456062 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.234580040 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.234647989 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.586976051 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.587085009 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.587116957 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.587173939 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.587271929 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.587327003 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.587449074 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.587498903 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.587587118 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.587635994 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.587812901 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.587866068 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.588157892 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.588201046 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.588221073 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.588315010 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.903383970 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.903712034 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.903800011 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.903809071 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.904248953 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.904311895 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.904378891 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.904501915 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.904546976 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.904601097 CEST	9090	49728	185.19.85.140	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 05:22:45.904938936 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.904989958 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.905092001 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.905220032 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.905270100 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.905327082 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.905430079 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.905477047 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.905534983 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.905827045 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.905874014 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.905886889 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:45.906181097 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:45.906239986 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.242923975 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.242954969 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.242966890 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.243083000 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.243138075 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.243163109 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.243175983 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.243225098 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.243271112 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.243534088 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.243556023 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.243621111 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.243680954 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.243798971 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.243855953 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.243957996 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.244070053 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.244124889 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.244450092 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.244504929 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.244560957 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.244638920 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.244755030 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.244810104 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.244966984 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.245413065 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.245475054 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.245563030 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.245697021 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.245743036 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.245847940 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.245954037 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.246000051 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.246074915 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.246160030 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.246201992 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.246447086 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.246548891 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.246591091 CEST	49728	9090	192.168.2.6	185.19.85.140
May 12, 2021 05:22:46.246679068 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.246911049 CEST	9090	49728	185.19.85.140	192.168.2.6
May 12, 2021 05:22:46.246929884 CEST	9090	49728	185.19.85.140	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 05:21:44.392151117 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:44.454217911 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 05:21:44.969283104 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:45.019577026 CEST	53	49448	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 05:21:46.178647995 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:46.227346897 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 05:21:47.001123905 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:47.049767017 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 05:21:49.854787111 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:49.905215979 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 05:21:50.805028915 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:50.857408047 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 05:21:51.613993883 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:51.662810087 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 05:21:52.741713047 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:52.790513992 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 05:21:53.604362011 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:53.655986071 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 05:21:55.662966013 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:55.711884022 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 05:21:56.522459984 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:56.579611063 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 05:21:57.410602093 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:57.471016884 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 05:21:59.637209892 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 05:21:59.686049938 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 05:22:00.445169926 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:00.493896961 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 05:22:01.446686983 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:01.495455980 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 05:22:02.553551912 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:02.605151892 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 05:22:03.698920012 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:03.750457048 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 05:22:04.769795895 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:04.823363066 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 05:22:21.244643927 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:21.316487074 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 05:22:39.220978975 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:39.281143904 CEST	53	49694	8.8.8.8	192.168.2.6
May 12, 2021 05:22:41.386811018 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:41.613265038 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 05:22:41.660953045 CEST	50010	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:41.719435930 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 05:22:52.175230026 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:52.397355080 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 05:22:59.768373013 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 05:22:59.830533028 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 05:23:06.820121050 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:06.891052008 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 05:23:06.963944912 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:07.023929119 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 05:23:07.732428074 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:07.837635040 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 05:23:08.897435904 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:09.001605034 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 05:23:10.012686014 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:10.069765091 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 05:23:10.889924049 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:10.947150946 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 05:23:11.772455931 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:11.829668999 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 05:23:13.295650005 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:13.358124971 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 05:23:14.012598991 CEST	54683	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:14.071949959 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 05:23:15.873629093 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:15.933146954 CEST	53	59329	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 05:23:17.469090939 CEST	64021	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:17.528901100 CEST	53	64021	8.8.8.8	192.168.2.6
May 12, 2021 05:23:17.606360912 CEST	56129	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:17.657932997 CEST	53	56129	8.8.8.8	192.168.2.6
May 12, 2021 05:23:18.770546913 CEST	58177	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:18.830600023 CEST	53	58177	8.8.8.8	192.168.2.6
May 12, 2021 05:23:19.971337080 CEST	50700	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:20.028148890 CEST	53	50700	8.8.8.8	192.168.2.6
May 12, 2021 05:23:23.621001005 CEST	54069	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:23.678153038 CEST	53	54069	8.8.8.8	192.168.2.6
May 12, 2021 05:23:25.175764084 CEST	61178	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:25.248471975 CEST	53	61178	8.8.8.8	192.168.2.6
May 12, 2021 05:23:31.218559027 CEST	57017	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:31.284054995 CEST	53	57017	8.8.8.8	192.168.2.6
May 12, 2021 05:23:32.738291025 CEST	56327	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:32.798279047 CEST	53	56327	8.8.8.8	192.168.2.6
May 12, 2021 05:23:41.981621981 CEST	50243	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:42.208885908 CEST	53	50243	8.8.8.8	192.168.2.6
May 12, 2021 05:23:45.884076118 CEST	62055	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:45.943105936 CEST	53	62055	8.8.8.8	192.168.2.6
May 12, 2021 05:23:50.228087902 CEST	61249	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:50.285227060 CEST	53	61249	8.8.8.8	192.168.2.6
May 12, 2021 05:23:57.315285921 CEST	65252	53	192.168.2.6	8.8.8.8
May 12, 2021 05:23:57.539803028 CEST	53	65252	8.8.8.8	192.168.2.6
May 12, 2021 05:24:04.391263008 CEST	64367	53	192.168.2.6	8.8.8.8
May 12, 2021 05:24:04.439948082 CEST	53	64367	8.8.8.8	192.168.2.6
May 12, 2021 05:24:06.723969936 CEST	55066	53	192.168.2.6	8.8.8.8
May 12, 2021 05:24:06.800782919 CEST	53	55066	8.8.8.8	192.168.2.6
May 12, 2021 05:24:07.639086962 CEST	60211	53	192.168.2.6	8.8.8.8
May 12, 2021 05:24:07.707125902 CEST	53	60211	8.8.8.8	192.168.2.6
May 12, 2021 05:24:24.540781021 CEST	56570	53	192.168.2.6	8.8.8.8
May 12, 2021 05:24:24.598411083 CEST	53	56570	8.8.8.8	192.168.2.6
May 12, 2021 05:24:30.486408949 CEST	58454	53	192.168.2.6	8.8.8.8
May 12, 2021 05:24:30.535231113 CEST	53	58454	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 05:22:41.386811018 CEST	192.168.2.6	8.8.8.8	0x30b2	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:22:52.175230026 CEST	192.168.2.6	8.8.8.8	0xaef8	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:22:59.768373013 CEST	192.168.2.6	8.8.8.8	0x64d8	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:23:06.963944912 CEST	192.168.2.6	8.8.8.8	0xc4ed	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:23:17.469090939 CEST	192.168.2.6	8.8.8.8	0xdaf4	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:23:23.621001005 CEST	192.168.2.6	8.8.8.8	0x7abb	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:23:32.738291025 CEST	192.168.2.6	8.8.8.8	0xb97d	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:23:41.981621981 CEST	192.168.2.6	8.8.8.8	0x7ad	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:23:50.228087902 CEST	192.168.2.6	8.8.8.8	0x6bd9	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:23:57.315285921 CEST	192.168.2.6	8.8.8.8	0x1a0d	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)
May 12, 2021 05:24:24.540781021 CEST	192.168.2.6	8.8.8.8	0xf295	Standard query (0)	backupjuly .duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

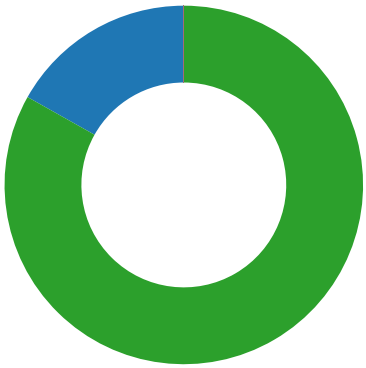
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 05:22:41.613265038 CEST	8.8.8.8	192.168.2.6	0x30b2	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 05:22:52.397355080 CEST	8.8.8.8	192.168.2.6	0xaef8	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:22:59.830533028 CEST	8.8.8.8	192.168.2.6	0x64d8	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:23:07.023929119 CEST	8.8.8.8	192.168.2.6	0xc4ed	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:23:17.528901100 CEST	8.8.8.8	192.168.2.6	0xdaf4	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:23:23.678153038 CEST	8.8.8.8	192.168.2.6	0x7abb	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:23:32.798279047 CEST	8.8.8.8	192.168.2.6	0xb97d	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:23:42.208885908 CEST	8.8.8.8	192.168.2.6	0x7ad	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:23:50.285227060 CEST	8.8.8.8	192.168.2.6	0x6bd9	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:23:57.539803028 CEST	8.8.8.8	192.168.2.6	0x1a0d	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)
May 12, 2021 05:24:24.598411083 CEST	8.8.8.8	192.168.2.6	0xf295	No error (0)	backupjuly .duckdns.org		185.19.85.140	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



- zUEBMx2U10.exe
- svchost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- zUEBMx2U10.exe
- svchost.exe
- zUEBMx2U10.exe
- svchost.exe
- zUEBMx2U10.exe
- svchost.exe
- svchost.exe
- WerFault.exe
- WerFault.exe
- svchost.exe
- svchost.exe
- svchost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: zUEBMx2U10.exe PID: 6540 Parent PID: 5980

General

Start time:	05:21:52
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\zUEBMx2U10.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zUEBMx2U10.exe'
Imagebase:	0xbc0000
File size:	3858432 bytes
MD5 hash:	9B2B7ACC05E281C17F978028722B51E9
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: 00000001.00000002.680956480.0000000006E35000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.680956480.0000000006E35000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.680956480.0000000006E35000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.651427825.00000000042A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.651427825.00000000042A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.651427825.00000000042A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD0BEFF	CreateDirectoryW
C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD0DD66	CopyFileW
C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD0DD66	CopyFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Resources\Themes\n2 4d78b7bgh77OZ2K111tT4aUZ16c1FC 8fLd3d31Nr6\svchost.exe	0	524288	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 bb b8 36 82 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 d6 3a 00 00 08 00 00 00 00 00 00 be f4 3a 00 00 20 00 00 00 00 3b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 3b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....6........... "...0...:............:.. ....;...@.. ....@ ;...........@................	success or wait	8	6CD0DD66	CopyFileW
C:\Windows\Resources\Themes\n2 4d78b7bgh77OZ2K111tT4aUZ16c1FC 8fLd3d31Nr6\svchost.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD0DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DE7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DE7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DE7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DE7D72F	unknown
C:\Users\user\Desktop\zUEBMx2U10.exe	unknown	4096	success or wait	1	6DE7D72F	unknown
C:\Users\user\Desktop\zUEBMx2U10.exe	unknown	512	success or wait	1	6DE7D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CD05F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CD05F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CD05F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe	dword	0	success or wait	1	6CD0C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\zUEBMx2U10.exe	dword	0	success or wait	1	6CD0C075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	9EO342rLb92o62	unicode	C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe	success or wait	1	6CD0646A	RegSetValueExW

Analysis Process: svchost.exe PID: 6644 Parent PID: 560

General

Start time:	05:21:56
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 6768 Parent PID: 6540

General

Start time:	05:22:01
Start date:	12/05/2021
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:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' -Force
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CC65B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CC65B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uludn5pk.srf.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jxa21zr3.o5a.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW
C:\Users\user\Documents\20210512\PowerShell_transcript.760639.6iHHi+Z_.20210512052205.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD01E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uludn5pk.srf.ps1	success or wait	1	6CD06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jxa21zr3.o5a.psm1	success or wait	1	6CD06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uludn5pk.srf.ps1	unknown	1	31	1	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jxa21zr3.o5a.psm1	unknown	1	31	1	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\Documents\20210512\PowerShell_transcript.760639.6iHHi+Z_.20210512052205.txt	unknown	3	ef bb bf	...	success or wait	1	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210512\PowerShell_transcript.760639.6iHHi+Z_.20210512052205.txt	unknown	728	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 35 31 32 30 35 32 32 33 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 36 30 36 33 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********..Windows PowerShell transcript start..Start time: 20210512052230..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	6	6CD01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....w.e....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	2	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module..... .inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6CD01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CD01B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DEA1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21356	success or wait	1	6DEA203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	135	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4\9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DE95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CD01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CD01B4F	ReadFile

Analysis Process: conhost.exe PID: 6776 Parent PID: 6768

General

Start time:	05:22:02
Start date:	12/05/2021
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: powershell.exe PID: 6792 Parent PID: 6540

General

Start time:	05:22:02
Start date:	12/05/2021
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\zUEBMx2U10.exe' -Force
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

Analysis Process: conhost.exe PID: 6844 Parent PID: 6792

General

Start time:	05:22:02
Start date:	12/05/2021
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: powershell.exe PID: 6884 Parent PID: 6540

General

Start time:	05:22:02
Start date:	12/05/2021
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:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' -Force
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

Analysis Process: conhost.exe PID: 6940 Parent PID: 6884

General

Start time:	05:22:03
Start date:	12/05/2021
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: cmd.exe PID: 7112 Parent PID: 6540

General

Start time:	05:22:06
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 7148 Parent PID: 7112

General

Start time:	05:22:07
Start date:	12/05/2021
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: timeout.exe PID: 5784 Parent PID: 7112

General

Start time:	05:22:08
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xc00000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: zUEBMx2U10.exe PID: 2940 Parent PID: 6540

General

Start time:	05:22:14
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\zUEBMx2U10.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\zUEBMx2U10.exe
Imagebase:	0x330000
File size:	3858432 bytes
MD5 hash:	9B2B7ACC05E281C17F978028722B51E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: svchost.exe PID: 6276 Parent PID: 3440

General

Start time:	05:22:16
Start date:	12/05/2021

Path:	C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe'
Imagebase:	0xa60000
File size:	3858432 bytes
MD5 hash:	9B2B7ACC05E281C17F978028722B51E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, Metadefender, Browse • Detection: 76%, ReversingLabs
Reputation:	low

Analysis Process: zUEBMx2U10.exe PID: 3800 Parent PID: 6540

General

Start time:	05:22:18
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\zUEBMx2U10.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\zUEBMx2U10.exe
Imagebase:	0x1e0000
File size:	3858432 bytes
MD5 hash:	9B2B7ACC05E281C17F978028722B51E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: svchost.exe PID: 6384 Parent PID: 560

General

Start time:	05:22:21
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: zUEBMx2U10.exe PID: 6516 Parent PID: 6540

General

Start time:	05:22:22
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\zUEBMx2U10.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\zUEBMx2U10.exe

Imagebase:	0xed0000
File size:	3858432 bytes
MD5 hash:	9B2B7ACC05E281C17F978028722B51E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: svchost.exe PID: 6480 Parent PID: 3440

General

Start time:	05:22:24
Start date:	12/05/2021
Path:	C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe'
Imagebase:	0xb30000
File size:	3858432 bytes
MD5 hash:	9B2B7ACC05E281C17F978028722B51E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: svchost.exe PID: 6728 Parent PID: 560

General

Start time:	05:22:28
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6680 Parent PID: 6728

General

Start time:	05:22:29
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 6540 -ip 6540
Imagebase:	0xea0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6876 Parent PID: 6540

General

Start time:	05:22:30
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6540 -s 1760
Imagebase:	0xea0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 6256 Parent PID: 560

General

Start time:	05:22:43
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 3224 Parent PID: 560

General

Start time:	05:23:04
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2276 Parent PID: 560

General

Start time:	05:23:19
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3624 Parent PID: 6276

General

Start time:	05:23:36
Start date:	12/05/2021
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:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' -Force
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 7044 Parent PID: 3624

General

Start time:	05:23:37
Start date:	12/05/2021
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

Analysis Process: powershell.exe PID: 1768 Parent PID: 6276

General

Start time:	05:23:37
Start date:	12/05/2021
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:\Windows\Resources\Themes\n24d78b7bgh77OZ2K111tT4aUZ16c1FC8fLd3d31Nr6\svchost.exe' -Force
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 4264 Parent PID: 1768

General

Start time:	05:23:38
Start date:	12/05/2021
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

Disassembly

Code Analysis