

# Virtual Analyzer Report



## Submission Context

Logged	2021-04-24 14:33:20
Submitter	Manual Submission
Type	WinAce archive

## Analysis Overview

Overall risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_GEN.R066C0DDH21		
Exploited vulnerabilities	-		
Analyzed objects	WinAce archive	1 - April 2021 Purchase Order_0000000000000000000000.pdf.ace	4302A778CFA4C81746EA7FAE3728BD5E96552751
	MSIL Portable executable	1.1 - April 2021 Purchase Order_0000000000000000000000.pdf.exe	69E313531A653495398DE6EDFA5F1460EF8B1E2F

## Analysis Environments

	CentOS w Docker	W7	W10
Anti-security, self-preservation		✓	✓
Autostart or other system reconfiguration			✓
Deception, social engineering			
File drop, download, sharing, or replication			✓
Hijack, redirection, or data theft		✓	✓
Malformed, defective, or with known malware traits	✓	✓	✓
Process, service, or memory object change		✓	✓
Rootkit, cloaking			
Suspicious network or messaging activity			

CentOS w Docker

Environment-specific risk level	<div>Low risk</div> The object exhibited mildly suspicious characteristics that are most likely benign.
Detections	TROJ_GEN.R066C0DDH21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - April 2021 Purchase Order\_0000000000000000000000.pdf.ace (WinAce archive)

File name	April 2021 Purchase Order_00000000000000000000000000.pdf.ace	Risk Level	Unrated
File type	WinAce archive	Detection	-
SHA-1	4302A778CFA4C81746EA7FAE3728BD5E96552751	Exploited vulnerabilities	-
SHA-256	DAD991FCBC1A0A0FA37D63C0FB6C25A69B8534065A65788122517F86C88C7C A0		
MD5	A5F5BC981FA23AA0511DE28628E8E302		
Size	659258 byte(s)		

Object 1.1 - April 2021 Purchase Order\_0000000000000000000000.pdf.exe (MSIL Portable executable)

File name	April 2021 Purchase Order_00000000000000000000000000.pdf.exe	Risk Level	Low risk
File type	MSIL Portable executable	Detection	TROJ_GEN.R066C0DDH21
SHA-1	69E313531A653495398DE6EDFA5F1460EF8B1E2F	Exploited vulnerabilities	-
SHA-256	DD4A9A91785A114C43E766FA5510586338863CFBAE280B8158483522EED40152	Threat Characteristics	Malformed, defective, or with known malware traits (1)
MD5	26194533127B81A2E6957B920C5B27F2		
Size	929280 byte(s)		

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as probable malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_GEN.R066C0DDH21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R066C0DDH21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		

Environment-specific risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.R066C0DDH21
Exploited vulnerabilities	-
Network connection	Custom

▼ Object 1 - April 2021 Purchase Order\_0000000000000000000000.pdf.ace (WinAce archive)

File name	April 2021 Purchase Order_0000000000000000000000.pdf.ace	Risk Level	Unrated
File type	WinAce archive	Detection	-
SHA-1	4302A778CFA4C81746EA7FAE3728BD5E96552751	Exploited vulnerabilities	-
SHA-256	DAD991FCBC1A0A0FA37D63C0FB6C25A69B8534065A65788122517F86C88C7CA0		
MD5	A5F5BC981FA23AA0511DE28628E8E302		
Size	659258 byte(s)		

▼ Object 1.1 - April 2021 Purchase Order\_0000000000000000000000.pdf.exe (MSIL Portable executable)

File name	April 2021 Purchase Order_0000000000000000000000.pdf.exe	Risk Level	High risk
File type	MSIL Portable executable	Detection	TROJ_GEN.R066C0DDH21
SHA-1	69E313531A653495398DE6EDFA5F1460EF8B1E2F	Exploited vulnerabilities	-
SHA-256	DD4A9A91785A114C43E766FA5510586338863CFBAE280B8158483522EED40152	Threat Characteristics	Anti-security, self-preservation (5) Hijack, redirection, or data theft (4) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (10)
MD5	26194533127B81A2E6957B920C5B27F2		
Size	929280 byte(s)		

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Windows Management Instrumentation	Characteristics: 1, 2, 3, 4
	PowerShell	Characteristics: 1
	Execution through API	Characteristics: 1
Privilege Escalation	Process Injection	Characteristics: 1, 2
		Characteristics: 1, 2
Defense Evasion	Software Packing	Characteristics: 1
	Process Injection	Characteristics: 1, 2
		Characteristics: 1, 2
	Process Hollowing	Characteristics: 1
Discovery	Process Discovery	Characteristics: 1
	System Information Discovery	Characteristics: 1, 2, 3, 4

© ATT&CK™ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (5)

Characteristic	Significance	Details
Attempts to detect sandbox application modules		Process ID: 2828 Module: SbieDll.dll
Attempts to detect sandbox characteristics		Sample attempted to detect sandbox using the following registry item: [SOFTWARE\VMware, Inc.\VMware Tools\]
Attempts to detect sandbox characteristics		Sample attempted to detect sandbox using the following registry item: [SOFTWARE\Oracle\VirtualBox Guest Additions\]
Attempts to detect active running processes		Process ID: 2828 Info: enum processes
Uses suspicious packer		File Name: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe Packer: UNKNOWN

▼ Hijack, redirection, or data theft (4)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2828 Info: Obtains Description from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2828 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2828 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 2828 Info: Obtains Win32_VideoController from API result

▼ Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Causes document reader to crash	<div><div></div><div></div><div></div></div>	Process ID: 3040 Image Path: April 2021 Purchase Order_0000000000000000000000.pdf.exe
Detected as probable malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_GEN.R066C0DDH21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

▼ Process, service, or memory object change (10)

Characteristic	Significance	Details
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 3040 Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2828 Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe Shell Command:
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2828 Injected API: WriteProcessMemory Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2828 Injected API: SetThreadContext Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe Injected Address: 0x0
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe Injected Content:
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe Injected Content: .L
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe Injected Content: MZ.
Injects memory with dropped files	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe File: MZ.
Creates process in system directory	<div><div></div><div></div><div></div></div>	Process ID: 2952 Image Path: %windir%\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
iecvlist.microsoft.com	152.199.19.161	53	-	No risk	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
ie9cvlist.ie.microsoft.com	152.199.19.161	53	-	No risk	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
iecvlist.microsoft.com	152.199.19.161	443	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
iecvlist.microsoft.com	152.199.19.161	80	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ie9cvlist.ie.microsoft.com/IE9CompatViewList.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
9Z9T61VVA4PT15L3CGA0.tmp	No risk	-	-	-	8016	8FB2E3189B0792754658DAF50E5E965E8DEF5095
d93f411851d7c929.customDestinations-ms~RF1d6343.TMP	No risk	-	-	-	8016	E8FEC2936251809B10A7D035E842FA074562114B
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	8016	8FB2E3189B0792754658DAF50E5E965E8DEF5095

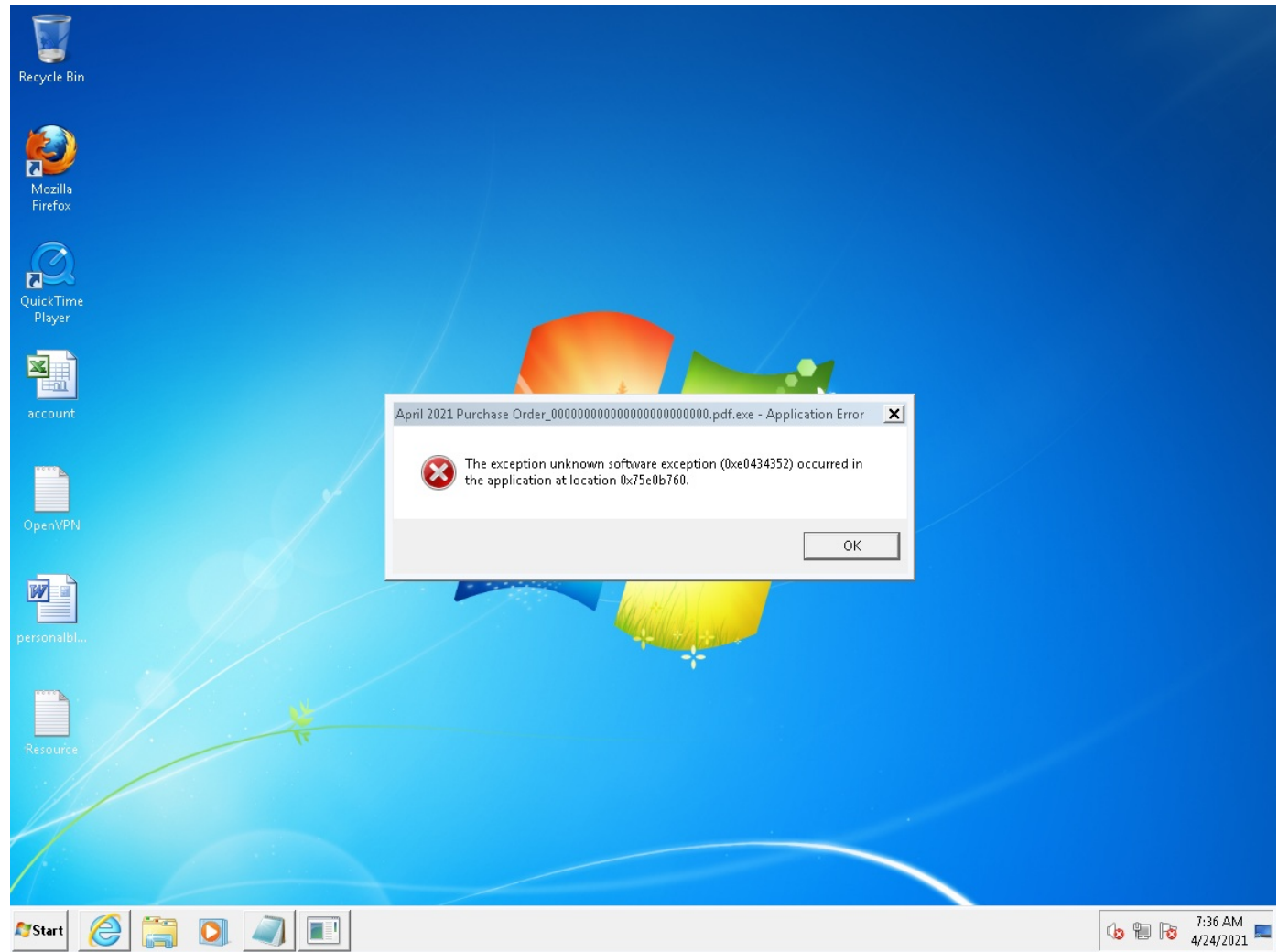
### ▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	69E313531A653495398DE6EDFA5F1460EF8B1E2F	High

### ▼ Analysis

[illegible]

Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Standard VGA Graphics Adapter, 8, 0 ) Return: 0		2828
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Standard VGA Graphics Adapter, 8, 0 ) Return: 0		2828
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Standard VGA Graphics Adapter, 8, 0 ) Return: 0		2828
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Standard VGA Graphics Adapter, 8, 0 ) Return: 0		2828
Call System API	API Name: GetModuleHandleA Args: ( SbieDll.dll ) Return: 0		2828
Detection	Threat Characteristic: Attempts to detect sandbox application modules Process ID: 2828 Module: SbieDll.dll		
Call Process API	API Name: CreateProcessW Args: ( %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe, , , , CREATE_SUSPENDED, , , Process:3040:%WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe ) Return: 1		2828
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2828 Injected API: WriteProcessMemory Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe		
Detection	Threat Characteristic: Creates process Process ID: 2828 Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:3040:%WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe, 400000, MZ, 512, 23cab4 ) Return: 1		2828
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:3040:%WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe, 402000, .t, 218624, 23cab4 ) Return: 1		2828
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Injected Content: .t.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:3040:%WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe, 438000, .1024, 23cab4 ) Return: 1		2828
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:3040:%WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe, 43a000, 512, 23cab4 ) Return: 1		2828
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Modify PEB 7ffda000 Process:3040:%WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe, 7ffda008, 4, 23cab4 ) Return: 1		2828
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2828 Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: ( Process Name:3040:%WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe ) Return: 1		2828
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2828 Injected API: SetThreadContext Target Process ID: 3040 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe		
Call Thread API	API Name: NtResumeThread Args: ( Process:3040, ) Return: ?		2828
Call System API	API Name: evtchann.SendEvent Args: ( e, pid[3040], ppid[2828 ] Return: 1		2828
Call System API	API Name: CryptExportKey Args: ( 1061f8, 0, 6, 0, 0, 8e430 ) Return: 1	2828	2952
Detection	Threat Characteristic: Creates process Process ID: 3040 Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe		
Call Filesystem API	API Name: DeleteFileW Args: ( %windir%\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.2952.1926095 ) Return: 0	2828	2952
Call Filesystem API	API Name: DeleteFileW Args: ( %windir%\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.2952.1926095 ) Return: 0	2828	2952
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2952.1926111 ) Return: 0	2828	2952
Detection	Threat Characteristic: Causes document reader to crash Process ID: 3040 Image Path: April 2021 Purchase Order_000000000000000000000000.pdf.exe		



W10

Environment-specific risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_GEN.R066C0DDH21
Exploited vulnerabilities	-
Network connection	Custom

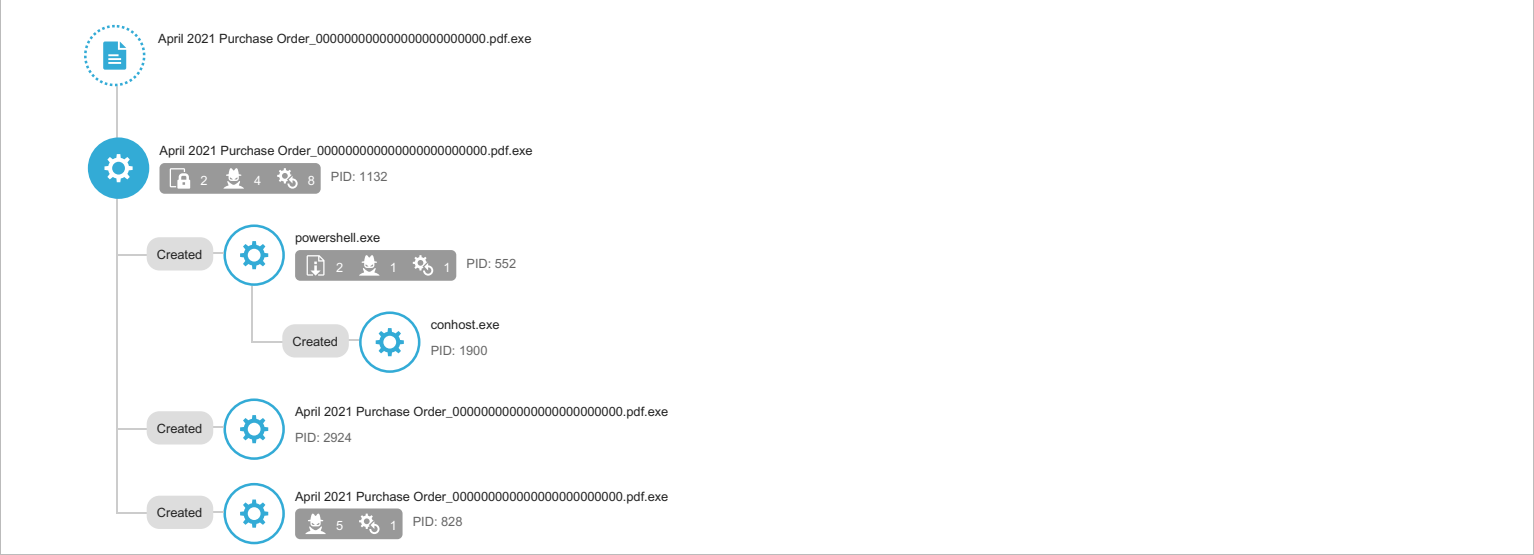
▼ Object 1 - April 2021 Purchase Order\_00000000000000000000000000000000.pdf.ace (WinAce archive)

File name	April 2021 Purchase Order_00000000000000000000000000000000.pdf.ace	Risk Level	<div>Unrated</div>
File type	WinAce archive	Detection	-
SHA-1	4302A778CFA4C81746EA7FAE3728BD5E9652751	Exploited vulnerabilities	-
SHA-256	DAD991FCBC1A0A0FA37D63C0FB6C25A69B8534065A65788122517F86C88C7CA0		
MD5	A5F5BC981FA23AA0511DE28628E8E302		
Size	659258 byte(s)		

▼ Object 1.1 - April 2021 Purchase Order\_00000000000000000000000000000000.pdf.exe (MSIL Portable executable)

File name	April 2021 Purchase Order_00000000000000000000000000000000.pdf.exe	Risk Level	<div>High risk</div>
File type	MSIL Portable executable	Detection	TROJ_GEN.R066C0DDH21
SHA-1	69E313531A653495398DE6EDFA5F1460EF8B1E2F	Exploited vulnerabilities	-
SHA-256	DD4A9A91785A114C43E766FA5510586338863CFBAE280B8158483522EED40152	Threat Characteristics	Anti-security, self-preservation (5) Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (2) Hijack, redirection, or data theft (15) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (11)
MD5	26194533127B81A2E6957B920C5B27F2		
Size	929280 byte(s)		

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Windows Management Instrumentation	Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9
	PowerShell	Characteristics: 1
	Execution through API	Characteristics: 1
Privilege Escalation	Process Injection	Characteristics: 1, 2
Defense Evasion	Software Packing	Characteristics: 1
	Process Injection	Characteristics: 1, 2
	Process Hollowing	Characteristics: 1
	File Deletion	Characteristics: 1, 2
Discovery	Process Discovery	Characteristics: 1
	System Information Discovery	Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9
Collection	Data from Local System	Characteristics: 1, 2, 3, 4, 5, 6

© ATT&CK™ is a trademark of The MITRE Corporation.

Notable Threat Characteristics

Anti-security, self-preservation (5)

Characteristic	Significance	Details
Attempts to detect active running processes		Process ID: 1132 Info: enum processes
Attempts to detect sandbox application modules		Process ID: 1132 Module: SbieDll.dll
Attempts to detect sandbox characteristics		Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware Tools\]
Attempts to detect sandbox characteristics		Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\VirtualBox Guest Additions\]
Uses suspicious packer		File Name: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe Packer: UNKNOWN

Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions		Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE

File drop, download, sharing, or replication (2)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection		Process ID: 552 File: %TEMP%\2mnjaall.0o2.psm1 Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection		Process ID: 552 File: %TEMP%\dyz2swkl.pwu.ps1 Type: VSDT_ASCII

Hijack, redirection, or data theft (15)

Characteristic	Significance	Details
Accesses decoy file	<div><div></div><div></div><div></div></div>	%LOCALAPPDATA%\Google\Chrome\User Data\Default>Login Data
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\COMODO\ICEDRAGON\PROFILES.INI
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\FILEZILLA\RECENTSERVERS.XML
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\key3.db
Accesses decoy file	<div><div></div><div></div><div></div></div>	%APPDATA%\Mozilla\Firefox\profiles.ini
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 828 Info: Obtains processorID from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 828 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 828 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 828 Info: Obtains __CLASS from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 828 Info: Obtains SerialNumber from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 1132 Info: Obtains Description from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 1132 Info: Obtains __PATH from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 1132 Info: Obtains __GENUS from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 1132 Info: Obtains Win32_VideoController from API result
Executes commands or uses API to obtain system information	<div><div></div><div></div><div></div></div>	Process ID: 552 Info: Searches files by API

▼ Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as probable malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_GEN.R066C0DDH21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

▼ Process, service, or memory object change (11)

Characteristic	Significance	Details
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 828 Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 1132 Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Shell Command:
Creates named pipe	<div><div></div><div></div><div></div></div>	\\.\pipe\PSHost.132637484426734440.552.DefaultAppDomain.powershell
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 1132 Injected API: WriteProcessMemory Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 1132 Injected API: SetThreadContext Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Injected Address: 0x0
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Injected Content:
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Injected Content: .t
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe Injected Content: MZ.
Injects memory with dropped files	<div><div></div><div></div><div></div></div>	Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_000000000000000000000000.pdf.exe File: MZ.
Creates process in system directory	<div><div></div><div></div><div></div></div>	Process ID: 552 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe"

▼ Network Destinations



Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	April 2021 Purchase Order_0000000000000000000000.pdf.exe
iecvlist.microsoft.com	152.199.19.161	53	-	No risk	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
go.microsoft.com	2.19.113.71	53	-	No risk	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
ctdl.windowsupdate.com	8.253.193.109	53	-	No risk	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
sqm.telemetry.microsoft.com	65.55.252.93	53	-	No risk	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
ieonline.microsoft.com	204.79.197.200	53	-	No risk	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
ocsp.digicert.com	93.184.220.29	80	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
go.microsoft.com	2.19.113.71	80	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
ctdl.windowsupdate.com	8.238.106.126	80	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
ctdl.windowsupdate.com	8.253.193.109	80	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
sqm.telemetry.microsoft.com	65.55.252.93	443	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
ieonline.microsoft.com	204.79.197.200	443	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe
iecvlist.microsoft.com	152.199.19.161	443	-	-	-	April 2021 Purchase Order_00000000000000000000000000.pdf.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ctdl.windowsupdate.com/msdownload/updat.../v3/static/trustedr/en/disallowedcertstl.cab?7a3cbe1cf070b39f	Computers / Internet Cloud Applications	No risk	-	April 2021 Purchase Order_000000000000000000000000.pdf.exe
http://ctdl.windowsupdate.com/msdownload/updat.../v3/static/trustedr/en/pinrulesstl.cab?0f76f2920b7851f3	Computers / Internet Cloud Applications	No risk	-	April 2021 Purchase Order_000000000000000000000000.pdf.exe
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBDuom%2FnYB4S5PUeWQU5Z12MIJHWMys%2BghUNoZ7OrUETiACEA8Ull8glGmZT9XhrHIJQel%3D	Computers / Internet Cloud Applications	No risk	-	April 2021 Purchase Order_000000000000000000000000.pdf.exe
http://ctdl.windowsupdate.com/msdownload/updat.../v3/static/trustedr/en/disallowedcertstl.cab?fe22d733ea2687c0	Computers / Internet Cloud Applications	No risk	-	April 2021 Purchase Order_000000000000000000000000.pdf.exe
http://go.microsoft.com/fwlink/?LinkID=401135	Computers / Internet	No risk	-	April 2021 Purchase Order_000000000000000000000000.pdf.exe

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
dysz2swkl.pwu.ps1	No risk	-	-	-	1	356A192B7913B04C54574D18C28D46E6395428AB
d93f411851d7c929.customDestinations-ms	No risk	-	-	-	6213	CFA52001FC0FC272BE374C1E4B4EC39AFD42DEC6
1ZU16Q59R0K2JN583CTS.temp	No risk	-	-	-	6213	CFA52001FC0FC272BE374C1E4B4EC39AFD42DEC6
d93f411851d7c929.customDestinations-ms-RF3902b.TMP	No risk	-	-	-	6213	FBC4D6995121320C454BEE7C1D6998AAD190B483
PowerShell_AnalysisCacheIndex	No risk	-	-	-	21073	6B0C1B13D48639DCA5B96D180A75222F8BAEC095
PowerShell_AnalysisCacheEntry_59996910-2bae-4b01-8439-8432fd48cc45	No risk	-	-	-	501	BC01DFE97CE498F367C39B979E42EC1798C05EF2
PowerShell_AnalysisCacheEntry_4af5a9e0-e2c2-48b5-8b10-1958ba4a717f	No risk	-	-	-	7549	28480EA3ABFA6EC15098DB0D5216FE125C841871
PowerShell_AnalysisCacheEntry_33bf3a44-1fc4-4e94-accd-a05eca95c165	No risk	-	-	-	3593	7A441E6298A953F9369B821C4DCEB0375FBA47F8
PowerShell_AnalysisCacheEntry_86a435ed-b36b-4c64-874a-968e2ab7ee47	No risk	-	-	-	7788	CCE590CB4A01E3D67FE5BDFBD930A9567CF17D80
PowerShell_AnalysisCacheEntry_623a97e5-a4a4-466d-9768-cbb2f5fe0748	No risk	-	-	-	6458	4690A032A1CC6C3CF0514873D58E67B652108F9A

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	69E313531A653495398DE6EDFA5F1460EF8B1E2F	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: TROJ_GEN.R066C0DDH21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000.pdf.exe Packer: UNKNOWN		
Call System API	API Name: System.Reflection.Assembly::Load Args: ( 4D5A9000... ) Return: 0		1132
Call System API	API Name: System.Reflection.Assembly::Load Args: ( 4D5A9000... ) Return: 0		1132
Call System API	API Name: System.Reflection.Assembly::Load Args: ( 4D5A9000... ) Return: 0		1132

Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: ( 0000000000000000, 0, 159056248, 8 ) Return: 0		1132
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: ( 0000000000000000, 0, 159056288, 8 ) Return: 0		1132
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: ( 0000000000000000, 0, 159056328, 8 ) Return: 0		1132
Call System API	API Name: EnumProcesses Args: ( ) Return: 1		1132
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 1132 Info: enum processes		
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1		1132
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1		1132
Call Process API	API Name: CreateProcessW Args: ( %windir%\System32\WindowsPowerShell\v1.0\powershell.exe, "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%WorkingDir%\April 2021 Purchase Order_00000000000000000000000000000000.pdf.exe", , , , CREATE_SUSPENDED, , %WorkingDir%, SW_HIDE, Process:552:%windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe ) Return: 1		1132
Call Thread API	API Name: NtResumeThread Args: ( Process:552, ) Return: ?		1132
Call System API	API Name: evtchann.SendEvent Args: ( e, pid[552], ppid[1132] ) Return: 1		1132
Read Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\VirtualBox Guest Additions\ Value: None		1132
Detection	Threat Characteristic: Attempts to detect sandbox characteristics Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oracle\VirtualBox Guest Additions\]		
Read Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware Tools\ Value: None		1132
Detection	Threat Characteristic: Attempts to detect sandbox characteristics Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware Tools\]		
Call WMI API	API Name: IWbemLevel1Login::NTLMLogin Args: ( \\.\ROOT\cimv2, en-US,en, 0, 6136858, ff9f038 ) Return: 0		1132
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( \\.\ROOT\cimv2, NULL, NULL, , 80, , 0, ff9f038 ) Return: 0		1132
Call WMI API	API Name: IWbemServices::ExecQuery Args: ( WQL, SELECT * FROM Win32_VideoController, 10, 0, 112d278 ) Return: 0		1132
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1132 Info: Obtains Win32_VideoController from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0		1132
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1132 Info: Obtains __GENUS from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: ( __PATH, 0, \\FIN-Adam-Serve\ROOT\cimv2:Win32_VideoController.DeviceID="VideoController1", 8, 64 ) Return: 0		1132
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1132 Info: Obtains __PATH from API result		
Detection	Threat Characteristic: Creates process in system directory Process ID: 552 Image Path: %windir%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe "%windir%\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "%WorkingDir%\April 2021 Purchase Order_00000000000000000000000000000000.pdf.exe"		
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1132 Info: Obtains Description from API result		
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	1132	552
Call System API	API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1	1132	552
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 6a4a9b90, -1, 4ae54c, 4ae548, 0 ) Return: 0	1132	552
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms ) Return: 1	1132	552
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF3902b.TMP ) Return: 1	1132	552
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\1ZU16Q59R0K2JN583CTS.temp Type: VSDT_COM_DOS	1132	552
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Write File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\1ZU16Q59R0K2JN583CTS.temp Type: VSDT_COM_DOS	1132	552
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF3902b.TMP Type: VSDT_EMPTY	1132	552
Call WMI API	API Name: Win32_VideoController::Get Args: ( Description, 0, Microsoft Basic Display Adapter, 8, 0 ) Return: 0		1132
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF3902b.TMP Type: VSDT_COM_DOS	1132	552
Call System API	API Name: GetModuleHandleA Args: ( SbieDll.dll ) Return: 0		1132
Detection	Threat Characteristic: Attempts to detect sandbox application modules Process ID: 1132 Module: SbieDll.dll		
Add File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Type: VSDT_COM_DOS	1132	552
Call Process API	API Name: CreateProcessW Args: ( %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000000000.pdf.exe, , , , , CREATE_SUSPENDED, , , , Process:2924:%WorkingDir%\April 2021 Purchase Order_00000000000000000000000000000000.pdf.exe ) Return: 1		1132
Detection	Threat Characteristic: Creates process Process ID: 1132 Image Path: %WorkingDir%\April 2021 Purchase Order_00000000000000000000000000000000.pdf.exe Shell Command:		
Delete File	Path: %APPDATA%\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF3902b.TMP Type: VSDT_COM_DOS	1132	552
Call System API	API Name: EnumProcesses Args: ( ) Return: 1		1132
Call System API	API Name: Process32Next Args: ( Parent process pid changed to: 1832 ) Return: 1		1132

Call Process API	API Name: CreateProcessW Args: ( %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe, , , , CREATE_SUSPENDED, , , , Process:828:%WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe ) Return: 1		1132
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1132 Injected API: WriteProcessMemory Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe		
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:828:%WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe, 400000, MZ,, 512, 112d6a0 ) Return: 1		1132
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:828:%WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe, 402000, .t., 2 18624, 112d6a0 ) Return: 1		1132
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe Injected Content: .t.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:828:%WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe, 438000, , 102 4, 112d6a0 ) Return: 1		1132
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:828:%WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe, 43a000, , 512 , 112d6a0 ) Return: 1		1132
Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Modify PEB 7f50d000 Process:828:%WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe, 7f50d008, , 4, 112d6a0 ) Return: 1		1132
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1132 Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: ( Process Name:828:%WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe ) Return: 1		1132
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1132 Injected API: SetThreadContext Target Process ID: 828 Target Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe		
Call Thread API	API Name: NtResumeThread Args: ( Process:828, ) Return: ?		1132
Call System API	API Name: evtchnn.SendEvent Args: ( e), pid[828], ppid[1132 ] Return: 1		1132
Call Filesystem API	API Name: CreateNamedPipeW Args: ( \\.\pipe\PSHost.132637484426734440.552.DefaultAppDomain.powershell, 1074266115, 6, 1, 32768, 32768, 0, 49054 32 ) Return: 524	1132	552
Detection	Threat Characteristic: Creates named pipe \\.\pipe\PSHost.132637484426734440.552.DefaultAppDomain.powershell		
Detection	Threat Characteristic: Creates process Process ID: 828 Image Path: %WorkingDir%\April 2021 Purchase Order_0000000000000000000000.pdf.exe		
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\April 2021 Purchase Order_0000000000000000000000.pdf.exe.log Type: VSDT_ASCII		1132
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\April 2021 Purchase Order_0000000000000000000000.pdf.exe.log Type: VSDT_ASCII		1132
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\dyz2swkl.pwu.ps1 ) Return: 1	1132	552
Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\2mnjaall.0o2.psm1 ) Return: 1	1132	552
Add File	Path: %TEMP%\dyz2swkl.pwu.ps1 Type: VSDT_ASCII	1132	552
Write File	Path: %TEMP%\dyz2swkl.pwu.ps1 Type: VSDT_ASCII	1132	552
Call Service API	API Name: OpenServiceW Args: ( 72b5a48, CryptSvc, 5 ) Return: 72b5a20	1132	552
Add File	Path: %TEMP%\2mnjaall.0o2.psm1 Type: VSDT_ASCII	1132	552
Write File	Path: %TEMP%\2mnjaall.0o2.psm1 Type: VSDT_ASCII	1132	552
Delete File	Path: %TEMP%\dyz2swkl.pwu.ps1 Type: VSDT_ASCII	1132	552
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 552 File: %TEMP%\dyz2swkl.pwu.ps1 Type: VSDT_ASCII		
Delete File	Path: %TEMP%\2mnjaall.0o2.psm1 Type: VSDT_ASCII	1132	552
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 552 File: %TEMP%\2mnjaall.0o2.psm1 Type: VSDT_ASCII		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui\Cache\7d152C64B7E\LanguageList Value: en-US\0en\0	1132	552
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\System\Certificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1132	552
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\System\Certificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1132	552
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\System\Certificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None	1132	552
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\System\Certificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_367d7386-cb1c-48bb-b1a1-a342e4e50d4c Type: VSDT_COM_DOS	1132	552

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_505d4d03-80d5-49a8-bbf5-d1da70a946da Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f2c42dea-0f9a-4e74-873c-b73e8713d7d8 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Call Filesystem API	API Name: FindFirstFileExW Args: ( %windir%\system32\WindowsPowerShell\v1.0\Modules\*, 0, a69e41c, 0, 0, 0 ) Return: 72d8648	1132	552
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 552 Info: Searches files by API		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_e116839a-2b1b-4588-be88-517689cfa536 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4d245eee-143c-43e2-ab9a-eca01a38cb58 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_c3cf3f6b-0abc-48ab-b19c-87f39e281542 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_59996910-2bae-4b01-8439-8432fd48cc45 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_37b04d57-604b-4960-afa4-a38a1594c1a7 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_d63980c8-601d-4081-80ab-dd5918e3af7a Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Call Filesystem API	API Name: GetFileAttributesW Args: ( %windir%\system32\WinMetadata\Windows.System.UserProfile.winmd ) Return: -1	1132	552
Call Filesystem API	API Name: GetFileAttributesW Args: ( %windir%\system32\WinMetadata\Windows.System.winmd ) Return: 32	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_60229287-003e-415b-8b53-4961c9d4dc01 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_1f76fb9f-ad8c-4ca8-a94e-898625bb2e86 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_72c9d763-81a0-4efc-bc24-efae2358d92 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Call WMI API	API Name: IWbemLevel1Login::NTLMLLogin Args: ( \\.root\cimv2, en-US,en,0,e399c0,a7ecac ) Return: 0	1132	828
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( \\.root\cimv2, NULL, NULL, NULL, 0, NULL, 0, a7ecac ) Return: 0	1132	828
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_ea6be6b9-079e-4a17-998a-b7bbcb6acf1b Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Call WMI API	API Name: Win32_BaseBoard::Get Args: ( SerialNumber, 0, 00IYNPXNRRJEDF, 8, 0 ) Return: 0	1132	828
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 828 Info: Obtains SerialNumber from API result		
Call WMI API	API Name: IWbemLevel1Login::NTLMLLogin Args: ( \\.root\cimv2, en-US,en,0,e39340,639f2a8 ) Return: 0	1132	828
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( \\.root\cimv2, NULL, NULL, , 80, , 0, 639f2a8 ) Return: 0	1132	828
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f95ace63-33bc-4cea-a2a4-826cd72e8851 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Call WMI API	API Name: Win32_Processor::Get Args: ( __PATH, 0, \\\FIN-Adam-Serve\ROOT\cimv2:Win32_Processor, 8, 64 ) Return: 0	1132	828
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 828 Info: Obtains __PATH from API result		
Call WMI API	API Name: Win32_Processor::Get Args: ( __CLASS, 0, Win32_Processor, 8, 64 ) Return: 0	1132	828
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 828 Info: Obtains __CLASS from API result		
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_18c9fb0c-fb68-4c86-bcd4-a92ef5adf42b Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_f904c07d-6234-4aaf-be8c-60559340f496 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_86a435ed-b36b-4c64-874a-968e2ab7ee47 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_5dec99ea-2cb6-4b5f-8ef9-a01742e42dc9 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Call WMI API	API Name: Win32_Processor::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	1132	828
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 828 Info: Obtains __GENUS from API result		
Call WMI API	API Name: Win32_Processor::Get Args: ( __PATH, 0, \\\FIN-Adam-Serve\root\cimv2:Win32_Processor.DeviceID="CPU0", 8, 64 ) Return: 0	1132	828

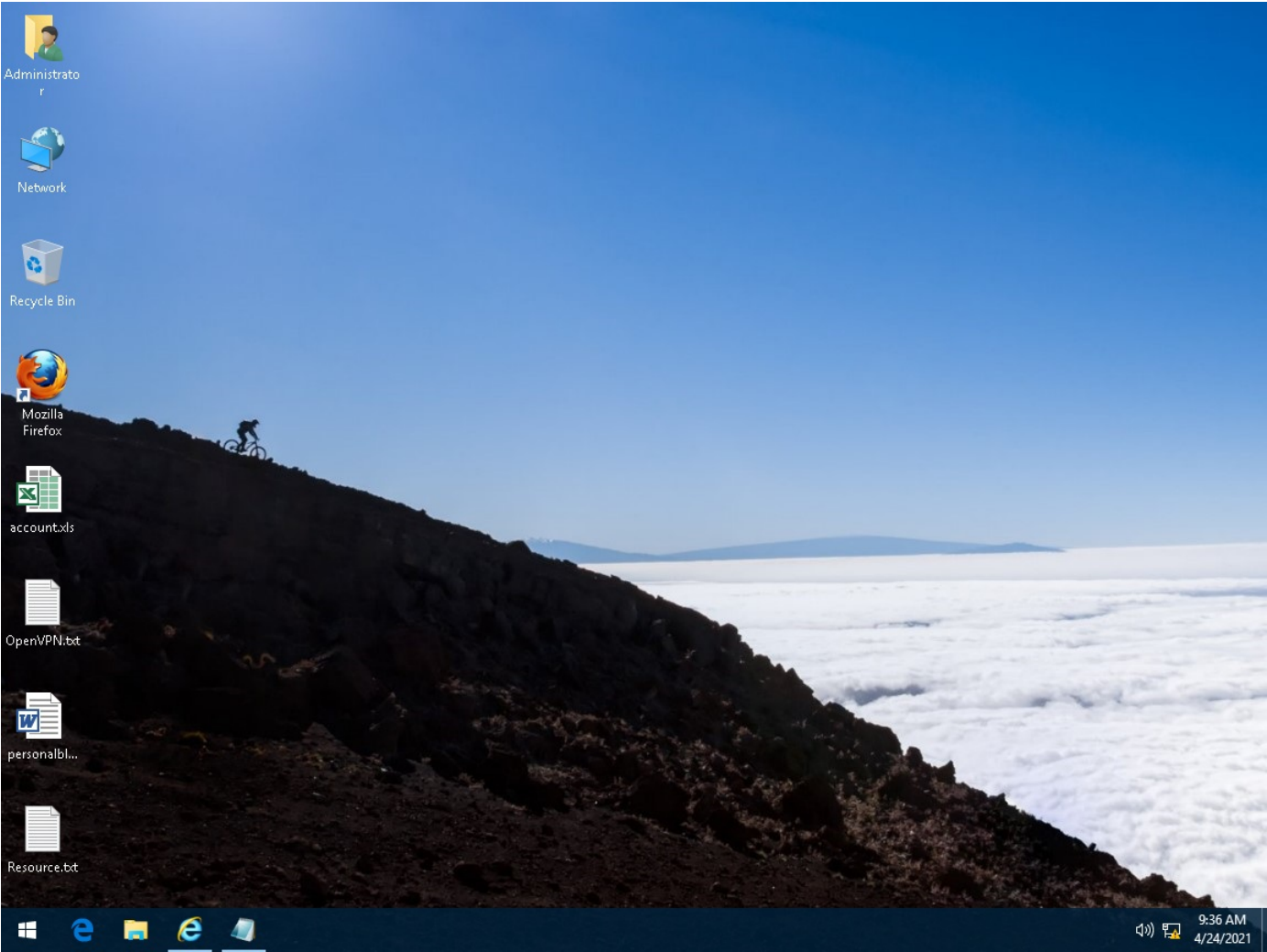
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_69dcdbbc-7545-4a92-af9e-33f77c87b07f Type: VSDT_COM_DOS	1132	552
Call WMI API	API Name: Win32_Processor::Get Args: ( processorID, 0, 1, 8, 32 ) Return: 0	1132	828
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 828 Info: Obtains processorID from API result		
Call WMI API	API Name: Win32_Processor::Get Args: ( processorID, 0, 1, 8, 32 ) Return: 0	1132	828
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Call WMI API	API Name: IWbemLevel1Login::NTLMLLogin Args: ( \\.\root\cimv2, en-US,en, 0, 5a89340, 64ef088 ) Return: 0	1132	828
Call WMI API	API Name: IWbemLocator::ConnectServer Args: ( \\.\root\cimv2, NULL, NULL, , 80, , 0, 64ef088 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\\FIN-Adam-Serve\root\cimv2:Win32_NetworkAdapterConfiguration, 8, 64 ) Return : 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __CLASS, 0, Win32_NetworkAdapterConfiguration, 8, 64 ) Return: 0	1132	828
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_a18a8c1a-12dc-421c-8600-4ee0bad81245 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\\FIN-Adam-Serve\root\cimv2:Win32_NetworkAdapterConfiguration.Index=0, 8, 64 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, 0, 11, 0 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\\FIN-Adam-Serve\root\cimv2:Win32_NetworkAdapterConfiguration.Index=1, 8, 64 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, -1, 11, 0 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( IPEnabled, 0, -1, 11, 0 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( MacAddress, 0, 00:1F:3C:8C:8D:BB, 8, 0 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( MacAddress, 0, 00:1F:3C:8C:8D:BB, 8, 0 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __GENUS, 0, 2, 3, 64 ) Return: 0	1132	828
Call WMI API	API Name: Win32_NetworkAdapterConfiguration::Get Args: ( __PATH, 0, \\\FIN-Adam-Serve\root\cimv2:Win32_NetworkAdapterConfiguration.Index=4, 8, 64 ) Return: 0	1132	828
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_6056746f-5eb1-4f3a-a8df-0ddb84cd9be7 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_057949d9-f265-4ae0-bb39-c8d4b13ac0ab Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9230a1ef-a3a0-4cb5-8f95-eb099d42b1d8 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_9a528d13-04a3-448c-b528-943230be3cac Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_35c6ed74-ae9b-4cf0-bc62-580dbdf2b29 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4af5a9e0-e2c2-48b5-bb10-1958ba4a717f Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_decaba2c-dbc5-4d8d-a112-c9522a435438 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_86d0fa65-46e2-4936-892e-13d04a74cc24 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_450102ae-6106-4c4e-a008-ec847f4ec874 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7eb349f9-d8a6-4e3d-be7d-3dbe7de3205e Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_769f96d2-2c3a-4719-b9a6-63d1aa888a67 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_7c0114f6-3a44-43d0-8833-ef686c9618ad Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_282c7b1d-8a86-4fe0-8862-782b1ea55447 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_95c6c018-1eea-4287-a70c-7d305f80a176 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_4778ef75-3dba-4959-a541-fe75d8a1069d Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheEntry_623a97e5-a4a4-466d-9768-cbb2f5fe0748 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_AnalysisCacheIndex Type: VSDT_COM_DOS	1132	552

Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_494b1a60-2944-4ad6-8ab2-f4d9be82a1c9 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_9fc74e9c-4ec2-4a28-8c76-d95b3e56c98a Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_22a63118-307f-4f05-b4a2-542141f4fb64 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_9d05625e-83a4-4a86-9f00-369a934ad822 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_4b614778-91a7-4226-a3d3-8991c69c115f Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_063b6e0a-7fdb-43f9-a8db-574e0bb22440 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_516e6127-5e24-4897-9042-e754cba0eb55 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_e2146bfe-39f2-4b5a-9190-3cbd628edc39 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_7300dbec-2865-45cc-ac58-5c32edfef1f2 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_33bf3a44-1fc4-4e94-accd-a05eca95c165 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_9c957b29-9561-45b4-9f5f-b844c5c1ce99 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_0ded4e37-020f-4c61-ab7d-a992ac43dc33 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_ea1f505a-a69a-40c3-a9cc-7b34489fd8b9 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_5ab30fef-f01b-414b-979d-49e08404589f Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_ec0b05e3-e8e6-4b86-a46d-76d9d8af06f4 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_ed9f9ad6-da58-41ab-beda-681f9c66e286 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a5318292-bdf9-41a5-b065-da2980715f5e Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_62ed1c2b-d7bc-4888-9254-487fc55c4b4b Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_2d9adf05-31af-4c86-8de0-26b3bbfdcce Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_a63c224e-fd93-4e45-bcd9-8ac0f6be3f74 Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheEntry_57a19812-ad31-47d3-b27b-900612eb602c Type: VSDT_COM_DOS	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\PowerShell\CommandAnalysis\PowerShell_Analysis\CacheIndex Type: VSDT_COM_DOS	1132	552
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	1132	552
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log Type: VSDT_ASCII	1132	552
Call System API	API Name: CLSIDFromProgIDEx Args: ( WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8} ) Return: 0	1132	828
Call System API	API Name: CLSIDFromProgIDEx Args: ( WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8} ) Return: 0	1132	828
Call System API	API Name: CLSIDFromProgIDEx Args: ( WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8} ) Return: 0	1132	828
Call System API	API Name: CLSIDFromProgIDEx Args: ( WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8} ) Return: 0	1132	828
Call System API	API Name: CLSIDFromProgIDEx Args: ( WScript.Shell, {72C24DD5-D70A-438B-8A42-98424B88AFB8} ) Return: 0	1132	828
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\key3.db		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\FILEZILLA\RECENTSERVERS.XML		
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\COMODO\ICEDRAGON\PROFILES.INI		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676 Value: None	1132	828


















Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	1132	828
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Detection	Threat Characteristic: Accesses decoy file %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data		

▼ Screenshot



Process Graph Legend

Node	Notable Threat Characteristics	
 Submitted sample	 Anti-security, self-preservation	 Malformed, defective, or with known malware traits
 Root process	 Autostart or other system reconfiguration	 Process, service, or memory object change
 Child process	 Deception, social engineering	 Rootkit, cloaking
 Direct event	 File drop, download, sharing, or replication	 Suspicious network or messaging activity
 Indirect event	 Hijack, redirection, or data theft	
 Created	Event actions	