ID: 457985
Sample Name: Swift Payment-3134101002.exe
Cookbook: default.jbs
Time: 16:40:23
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

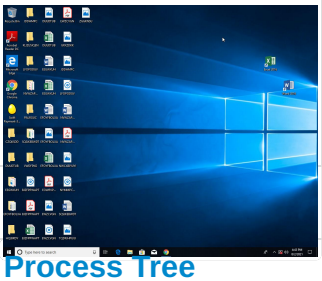
Windows Analysis Report Swift Payment-3134101002.exe

Overview

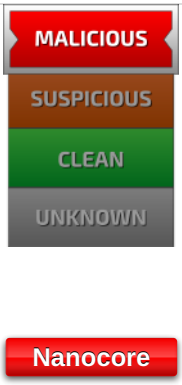
General Information

Sample Name:	Swift Payment-3134101002.exe
Analysis ID:	457985
MD5:	3221d82b7169d5..
SHA1:	96326c074c61d3..
SHA256:	41a5f782da40bea.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



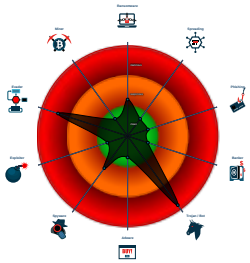
Nanocore

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains method …
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- Swift Payment-3134101002.exe (PID: 896 cmdline: 'C:\Users\user\Desktop\Swift Payment-3134101002.exe' MD5: 3221D82B7169D545F01F2E2BA94ADE25)
  - powershell.exe (PID: 2896 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Swift Payment-3134101002.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5908 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5452 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TPiUrUItCGsY' /XML 'C:\Users\user\AppData\Local\Temp\tmpD9EC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3888 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4500 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Swift Payment-3134101002.exe (PID: 5848 cmdline: C:\Users\user\Desktop\Swift Payment-3134101002.exe MD5: 3221D82B7169D545F01F2E2BA94ADE25)
  - Swift Payment-3134101002.exe (PID: 5260 cmdline: C:\Users\user\Desktop\Swift Payment-3134101002.exe MD5: 3221D82B7169D545F01F2E2BA94ADE25)
    - schtasks.exe (PID: 5872 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp54AF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6172 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp5992.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Swift Payment-3134101002.exe (PID: 6208 cmdline: 'C:\Users\user\Desktop\Swift Payment-3134101002.exe' 0 MD5: 3221D82B7169D545F01F2E2BA94ADE25)
  - powershell.exe (PID: 1692 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Swift Payment-3134101002.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1332 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TPiUrUItCGsY' /XML 'C:\Users\user\AppData\Local\Temp\tmpF33C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5492 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Swift Payment-3134101002.exe (PID: 5436 cmdline: C:\Users\user\Desktop\Swift Payment-3134101002.exe MD5: 3221D82B7169D545F01F2E2BA94ADE25)
- dhcpmon.exe (PID: 6580 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 3221D82B7169D545F01F2E2BA94ADE25)
- dhcpmon.exe (PID: 6812 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 3221D82B7169D545F01F2E2BA94ADE25)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "533a35a8-575b-4ab4-8925-c191b861",
  "Group": "Yota",
  "Domain1": "yota890.hopto.org",
  "Domain2": "127.0.0.1",
  "Port": 23890,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 50,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "yota890.hopto.org",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000002A.00000002.453841025.0000000002D0 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000002A.00000002.453841025.0000000002D0 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2380b:$a: NanoCore • 0x23864:$a: NanoCore • 0x238a1:$a: NanoCore • 0x2391a:$a: NanoCore • 0x2386d:$b: ClientPlugin • 0x238aa:$b: ClientPlugin • 0x241a8:$b: ClientPlugin • 0x241b5:$b: ClientPlugin • 0x1b57a:$e: KeepAlive • 0x23cf5:$g: LogClientMessage • 0x23c75:$i: get_Connected • 0x1583d:$j: #=q • 0x1586d:$j: #=q • 0x158a9:$j: #=q • 0x158d1:$j: #=q • 0x15901:$j: #=q • 0x15931:$j: #=q • 0x15961:$j: #=q • 0x15991:$j: #=q • 0x159ad:$j: #=q • 0x159dd:$j: #=q
0000002A.00000002.446482666.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000002A.00000002.446482666.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000002A.00000002.446482666.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.Swift Payment-3134101002.exe.3d47ab8.8.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
13.2.Swift Payment-3134101002.exe.3d47ab8.8.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
13.2.Swift Payment-3134101002.exe.3d47ab8.8.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
13.2.Swift Payment-3134101002.exe.3d4c0e1.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
13.2.Swift Payment-3134101002.exe.3d4c0e1.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
Click to see the 52 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Connects to many ports of the same IP (likely port scanning)

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- .NET source code contains method to dynamically call methods (often used by packers)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

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

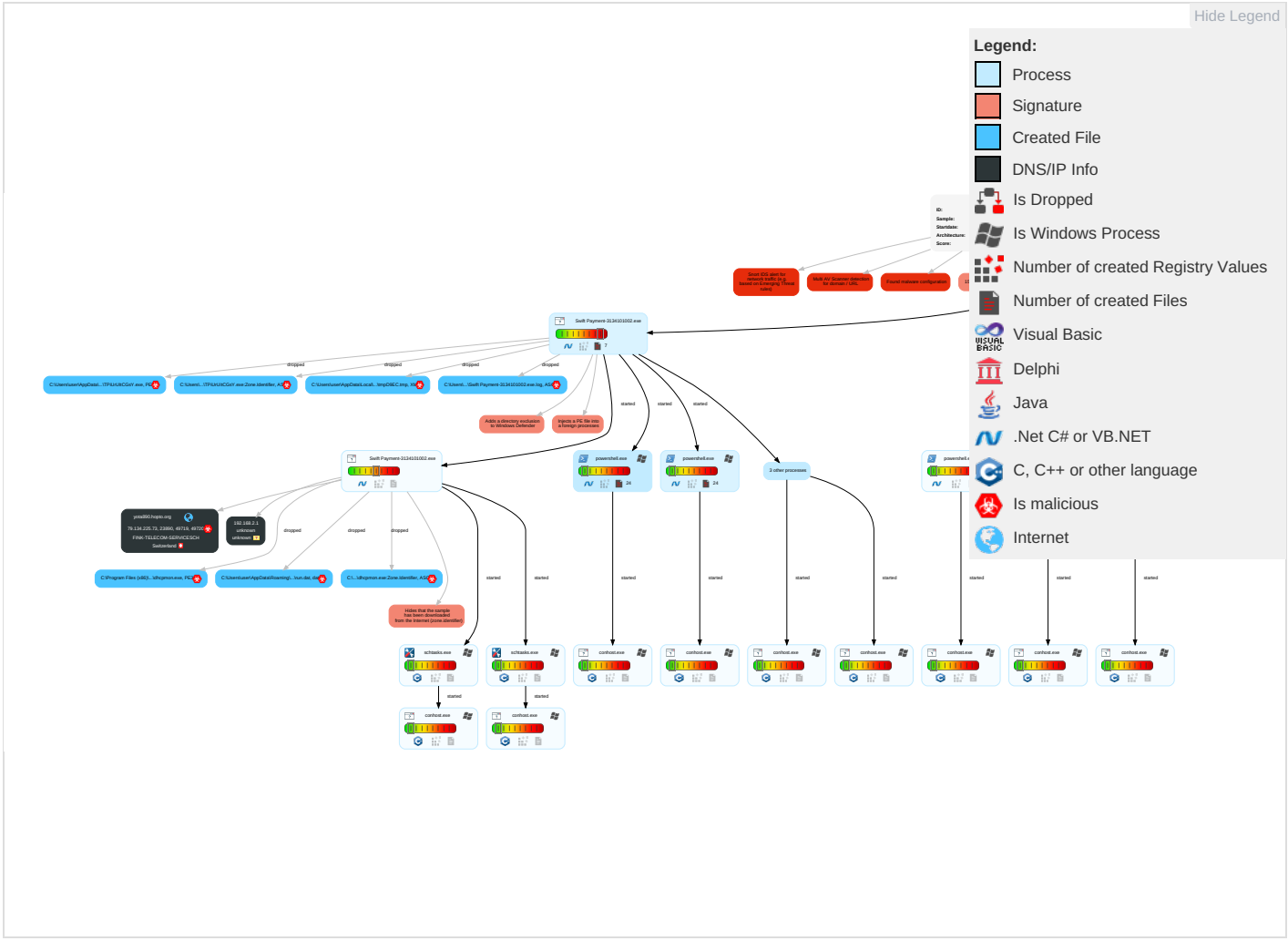
Remote Access Functionality:

- 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	N E
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E I N C
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 1	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D I F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	F E

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
Swift Payment-3134101002.exe	100%	Avira	HEUR/AGEN.1105323	
Swift Payment-3134101002.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe	100%	Avira	HEUR/AGEN.1105323	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	HEUR/AGEN.1105323	
C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.0.dhcpmon.exe.d00000.0.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
42.0.Swift Payment-3134101002.exe.5a0000.0.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
10.2.Swift Payment-3134101002.exe.a0000.0.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
13.0.Swift Payment-3134101002.exe.4d0000.0.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
13.2.Swift Payment-3134101002.exe.4d0000.1.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
42.2.Swift Payment-3134101002.exe.5a0000.1.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
42.2.Swift Payment-3134101002.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
13.2.Swift Payment-3134101002.exe.3d47ab8.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
13.2.Swift Payment-3134101002.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.Swift Payment-3134101002.exe.c90000.0.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
28.0.dhcpmon.exe.840000.0.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
18.0.Swift Payment-3134101002.exe.860000.0.unpack	100%	Avira	HEUR/AGEN.1105323		Download File
10.0.Swift Payment-3134101002.exe.a0000.0.unpack	100%	Avira	HEUR/AGEN.1105323		Download File

Domains

Source	Detection	Scanner	Label	Link
yota890.hopto.org	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
yota890.hopto.org	7%	Virustotal		Browse
yota890.hopto.org	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
yota890.hopto.org	79.134.225.73	true	true	• 7%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
yota890.hopto.org	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.73	yota890.hopto.org	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457985
Start date:	02.08.2021

Start time:	16:40:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Swift Payment-3134101002.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:	47
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@37/38@16/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.8% (good quality ratio 12.4%) • Quality average: 41.6% • Quality standard deviation: 39%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:41:26	API Interceptor	667x Sleep call for process: Swift Payment-3134101002.exe modified
16:41:33	API Interceptor	152x Sleep call for process: powershell.exe modified
16:41:36	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Swift Payment-3134101002.exe" s>$(Arg0)
16:41:36	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:41:40	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
16:42:42	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.73	POS AUTO REJECT TRANSACTIONSxlsx.vbs	Get hash	malicious	Browse	• subsnet.duckdns.org:35500/is-ready
	50Passagem 2.js	Get hash	malicious	Browse	• accer.syt es.net:7974/Vre
	50Passagem 2.js	Get hash	malicious	Browse	• accer.syt es.net:7974/Vre

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
yota890.hopto.org	Faktura-835382925.exe	Get hash	malicious	Browse	• 79.134.225.73
	New Order.exe	Get hash	malicious	Browse	• 79.134.225.73
	New Order July.exe	Get hash	malicious	Browse	• 79.134.225.73
	jtH33Uljkz.exe	Get hash	malicious	Browse	• 79.134.225.73
	JUBnIETj2h.exe	Get hash	malicious	Browse	• 79.134.225.73

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	NEW INQUIRY.exe	Get hash	malicious	Browse	• 79.134.225.95
	Order List.exe	Get hash	malicious	Browse	• 79.134.225.115
	RFQ 217563.exe	Get hash	malicious	Browse	• 79.134.225.116
	ORDER CONFIRMATION - 5309,pdf.exe	Get hash	malicious	Browse	• 79.134.225.76
	y7DZJshX9j.exe	Get hash	malicious	Browse	• 79.134.225.44
	SQycD6hL4Y.exe	Get hash	malicious	Browse	• 79.134.225.12
	TENDER INQUIRY REQUIREMENTS.exe	Get hash	malicious	Browse	• 79.134.225.95
	xwcTd7Kh9O.exe	Get hash	malicious	Browse	• 79.134.225.16
	RA1_20210729.exe	Get hash	malicious	Browse	• 79.134.225.98
	spworks.msi	Get hash	malicious	Browse	• 79.134.225.73
	spworks.msi	Get hash	malicious	Browse	• 79.134.225.73
	Request For Quotation.xlsx	Get hash	malicious	Browse	• 79.134.225.16
	Faktura-835382925.exe	Get hash	malicious	Browse	• 79.134.225.73
	Order List.gz.exe	Get hash	malicious	Browse	• 79.134.225.100
	doc_18000476456499946534.exe	Get hash	malicious	Browse	• 79.134.225.44
	Bh8aCXgJx4.exe	Get hash	malicious	Browse	• 79.134.225.22
	Resumen detallado del proveedor de 1302640 de solicitud de presupuesto.exe	Get hash	malicious	Browse	• 79.134.225.8
	Investment1FZELtd.exe	Get hash	malicious	Browse	• 79.134.225.35
	KRooWcCysc.exe	Get hash	malicious	Browse	• 79.134.225.25
	Request price for partsDP35212202122000.exe	Get hash	malicious	Browse	• 79.134.225.44

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1495040
Entropy (8bit):	7.453387490513826
Encrypted:	false
SSDEEP:	24576:J1oxcVmGXEzFfx8Dgkfx8DgT+rw8ojngl1F4aw1jhzxSbj5mZUYLL:cxQ+F58Dgk58DgJbIFYdxQj4ZUA
MD5:	3221D82B7169D545F01F2E2BA94ADE25
SHA1:	96326C074C61D3D176F4C6760CE5027B565FAD03
SHA-256:	41A5F782DA40BEA08F41A9510A299BFA071C7F84547085F65006C25002802449
SHA-512:	C3699599F6649AF0919906EA4CC40039C11C22D16A4FAE4CDAF23779A1811F405317B9058C3F7CBAA17340E0DAD261A3251700C2658F5E10F7AA76242FFD4B10
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....~.... ... .@.. .....@..... ..@.....0...K....@.. ....H.....text..... ....`.sdata..... .....@....rsr c...,....@.....@..@.reloc..... .....@..B..... ....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Swift Payment-3134101002.exe.log	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21692
Entropy (8bit):	5.3617502255191
Encrypted:	false
SSDEEP:	384:btL6sk2nTnOgRdEeexXn3YTxQ1pghV0J/3eSJMC3at:lkE9Rdr2P1pgT0pFMCg
MD5:	F26BD29FDBE62ADF1B27226C0BCA0F76
SHA1:	575CD4E74CADE25362041CD1D39D97D7FFA4B103
SHA-256:	5C6E29CAB2238370A0312DF7305EE77D37AD73208D5AA9CCE32847A240A24AE0
SHA-512:	7AE0DFAB07A0A0D9B809ECB2E9E2A9A0DDCC18948F3DF1F23D552A7792EB63BF9B8DC4609314006F46EB779446CCD32D1EB7B966A93E1F644D0473E28175C2 4
Malicious:	false
Reputation:	unknown
Preview:	@...e.....3.d.[.....Q.{...v.....@.....D.....fZve...F.....x.)].....System.Management.AutomationH.....<@.^.L."My...:U..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,j.....(.Microsoft.PowerShell.Commands.ManagementT.....7.,.fiD..... .....*.Microsoft.Management.Inf

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2gdksdx4.dbh.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eh3vh0vl.a5b.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eh3vh0vl.a5b.psm1	
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fgq2ow1k.yiq.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ft3s03ih.awi.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hikacsuv.u45.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jjgrjvom.1cc.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kj1llfos.ssx.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q2i2gyxt.uiy.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qtoebvt2.pqv.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

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

C:\Users\user\AppData\Local\Temp\tmp54AF.tmp	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1315
Entropy (8bit):	5.118105243297081
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0PpgqxtnCbk4oL600QydbQxIYODOLedq3Sdj
MD5:	AED85AE1D81D0B7B27DC4BA30626540C
SHA1:	2D401295A809F8ED7669D7DB7D9B5D6EEB20BCD1
SHA-256:	F5EC002D41D0481CEE02B0205CE033460D998755D6B8E9FA9E60D5BE1636EBFA
SHA-512:	012F34354AC0A09E707A65B4F1AEC2D272F01BA81DFBFEFE6B5B8FD4E7EE373A006D7FF518E1C0A35EDE7792230C2B9C3102D8F65701053DFDD562CF3C1FC4 1
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp5992.tmp	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpD9EC.tmp	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1649

C:\Users\user\AppData\Local\Temp\tmpD9EC.tmp	
Entropy (8bit):	5.171845576133123
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB9tn:cbhC7ZlNQF/rydbz9I3YODOLNdq31
MD5:	ABA8A7EB8FC293B45B8926B254C8545D
SHA1:	C265284659BCC0F1CA9EF728D93F050E6A0DB2FA
SHA-256:	46E944053EFBC4554B10F9C8187AEA3FD48BF87C4466E3F463ED803C55005F24
SHA-512:	8045D1CFE3CD98513A68C7698FA981CB6A3FA8161659FBEEA416FC923B01BB6AAABBEB9CA0F9F343C78371FE233D5D1333CA44D6A6FDD968AED8500C429160 3B
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpF33C.tmp	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1649
Entropy (8bit):	5.171845576133123
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB9tn:cbhC7ZlNQF/rydbz9I3YODOLNdq31
MD5:	ABA8A7EB8FC293B45B8926B254C8545D
SHA1:	C265284659BCC0F1CA9EF728D93F050E6A0DB2FA
SHA-256:	46E944053EFBC4554B10F9C8187AEA3FD48BF87C4466E3F463ED803C55005F24
SHA-512:	8045D1CFE3CD98513A68C7698FA981CB6A3FA8161659FBEEA416FC923B01BB6AAABBEB9CA0F9F343C78371FE233D5D1333CA44D6A6FDD968AED8500C429160 3B
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6 B5
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.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\Swift Payment-3134101002.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SSDEEP:	3:zgQt:UQt
MD5:	A4BBCDC296399DF2D741B81AC1F23823
SHA1:	DC25F6B400FFC462E07B540A9EF2AE0DDC65A244
SHA-256:	427760C35EEFFED1C016FAA83871E56BE306DF8AB2CF038969DBE4E5409550F9
SHA-512:	660A3A98791BDA9CC850E7233B4409CCC994749CE56EE780DEB491618850362A14A20A74371E9A072F3C2A54D847267CB2F19992ED86EA3049E0442047502DBE
Malicious:	**true**
Reputation:	unknown
Preview:	x$...V.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVnXygY6oRDT6P2bfVn1:RzWDT62DWDT621
MD5:	4315325323A62DE913E5CCD153817BCE
SHA1:	8B38155CD8ACB20BBA0C2A8AF02BFD35B15221A8
SHA-256:	E0C2085D878FDF53CD7D8F0AA9F07490802C51FC3C14A52B6FEA96AD0743C838
SHA-512:	B5036A6CD4852CEBCA86F588D94B9D58B63EB07B2F4DEBD38D5E1BE68B0BB62F82FA239673B6C08F432A28DD50E1D15773DC3738251BD2F9959F1255D72745E B
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Reputation:	unknown
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:....L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..).(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!.;.^9"H.....*...OkF....v.m_.e.v..f...."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	4.702856968507876
Encrypted:	false
SSDEEP:	3:oNUWJRW2SSxPyuUA:oNNJA2lxPytA
MD5:	4597423D7779AE7F4FA8A6B862260DD2
SHA1:	745488A3ABF6049DE33048A5EDE992FE4270EFEB
SHA-256:	C7E01DA4600D50612BBDAB98A956011520318AD65E0450663E192B798B47CEE6
SHA-512:	A7CB95E50AEEA29743EE77230265EBA8B32391048CC445C717CA757A664B31710BA04A7C0F5A0FC85DA642149418380052DE9F90AC8FEF44BAE289F8F772AC7(
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\Swift Payment-3134101002.exe

C:\Users\user\AppData\Roaming\TPiUrUltCGsY.exe	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1495040
Entropy (8bit):	7.453387490513826
Encrypted:	false
SSDEEP:	24576:J1oxcVmGXEzFfx8Dgkfx8DgT+rw8ojngl1F4aw1jhzxSbj5mZUYLL:cxQ+F58Dgk58DgJbIFYdxQj4ZUA
MD5:	3221D82B7169D545F01F2E2BA94ADE25
SHA1:	96326C074C61D3D176F4C6760CE5027B565FAD03
SHA-256:	41A5F782DA40BEA08F41A9510A299BFA071C7F84547085F65006C25002802449
SHA-512:	C3699599F6649AF0919906EA4CC40039C11C22D16A4FAE4CDAF23779A1811F405317B9058C3F7CBAA17340E0DAD261A3251700C2658F5E10F7AA76242FFD4B10
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....~.... ... .@.. .....@..... ..@.....0...K....@.,..... ....H.....text..... ....`.sdata..... .....@....rsr c...,....@.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\Roaming\TPiUrUltCGsY.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210802\PowerShell_transcript.536720.lwZ5ajft.20210802164132.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):	5807
Entropy (8bit):	5.388031589896704
Encrypted:	false
SSDEEP:	96:BZu/ZN1qDo1Z2Zm/ZN1qDo1ZV71zjZM/ZN1qDo1ZFFCDDbjZJa:f
MD5:	508D96D6BBC567F1C717F2DC6C005DB3
SHA1:	F79EE77B4EC7C0B70A2094A8011D8A934300B1EA

C:\Users\user\Documents\20210802\PowerShell_transcript.536720.lwZ5ajft.20210802164132.txt	
SHA-256:	0228A771C8540238E866460D2A862F1BB611AEB315367227A4E46BD840EC919B
SHA-512:	71EF8C48192D588BB85865D36491068D031213767EF63F32902925CD43FDBD23123361B66920A1605B6AC97B3D98DC7F4CB7A1F2F621355F41D3C9BE9ECD8814
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210802164132..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 536720 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe..Process ID: 4500..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: 20210802164132..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe..**********..Windows PowerShell transcript start..Start time: 20210802164626..Username: computer\user..RunAs User: DESKTOP-716

C:\Users\user\Documents\20210802\PowerShell_transcript.536720.JVTY2eBe.20210802164130.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):	3605
Entropy (8bit):	5.318356877927142
Encrypted:	false
SSDEEP:	96:BZe/ZN0vqDo1Z1w7Z0/ZN0vqDo1ZCqp8K0c8K0c8K08ZY:2ddy
MD5:	24FDE701767F202DCB517D8B148FC598
SHA1:	033DF7DE0AB2F439B2F5D6F4A30BDC67FEC8C3BA
SHA-256:	FBF84A2C356AA29CD560FA38DE81D50CC33F8CE3A6985F8A6E46C76FEB44A133
SHA-512:	2119D12A0E863F65DBE80184792E54019062676F8C9270F3514020B97B129F081BA27CA251E743B3A1AE274105F26C2C4AC4621173A4CD426492EF9312F3B5B5
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210802164147..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 536720 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Swift Payment-3134101002.exe..Process ID: 2896..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: 20210802164147..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Swift Payment-3134101002.exe..**********..Command start time: 20210802164426..**********..PS>TerminatingError(Add-MpPreference): "A positional p

C:\Users\user\Documents\20210802\PowerShell_transcript.536720.K3SQstla.20210802164132.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):	5807
Entropy (8bit):	5.392081511020278
Encrypted:	false
SSDEEP:	96:BZK/ZNOqDo1ZqZO/ZNOqDo1ZI71zjZ4/ZNOqDo1ZuCDD8ZL:0
MD5:	E00626F25F13D0C679ED820A84502AAE
SHA1:	79CF9942DB9C3A8EE6045622FA61DC1604EE6752
SHA-256:	9FD4C75E09295A278067F27BEB5C1D0A05A9E5506A7B2BBB7424D69E2F26E157
SHA-512:	3E71632F297843C3C17A5EAEE03F3FC5628AE08A66C2FF20D1D2FDB3DFEF93F7D1C907D2C8B4FB4D18A6D5FD2FF9806261EEF3C7AA80C4C50AF25CA79D1A63C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210802164150..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 536720 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe..Process ID: 5908..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: 20210802164150..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe..**********..Windows PowerShell transcript start..Start time: 20210802164543..Username: computer\user..RunAs User: DESKTOP-716

C:\Users\user\Documents\20210802\PowerShell_transcript.536720.b2b1JaRZ.20210802164247.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):	5807
Entropy (8bit):	5.392856142812632
Encrypted:	false
SSDEEP:	96:BZ6/ZNaqDo1ZGZ4/ZNaqDo1Z171zjZH/ZNaqDo1ZpCDDVZG:N
MD5:	B6101E7BB87EBD02C2932CDB18FF5DCD
SHA1:	BF3CE5A808786047C51D083A58E4DE817BC18886
SHA-256:	4C68AAE17234B6882FE9E870B581C54A467CDB459B4CF22C48BA2FAEB044BDFF

C:\Users\user\Documents\20210802\PowerShell_transcript.536720.b2b1JaRZ.20210802164247.txt	
SHA-512:	5AAB833A179E998926C9EED67588977D4E8C50A1D1C702C797778A35F6515E9D6006C82EA7CE8F6CECB50BB2B337C6DB8DFBCB222643DAD888CA234F03707EA
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210802164248..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 536720 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe..Process ID: 5492..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: 20210802164248..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe..**********..Windows PowerShell transcript start..Start time: 20210802164530..Username: computer\user..RunAs User: DESKTOP-716

C:\Users\user\Documents\20210802\PowerShell_transcript.536720.lMSIrPJI.20210802164243.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):	3605
Entropy (8bit):	5.319640725470849
Encrypted:	false
SSDEEP:	96:BZF/ZN0UqDo1ZCD7Za/ZN0UqDo1Zsqp8K0c8K0c8K0DZ8:HddZ
MD5:	0A5AB307A3F607F622B35D20BCE8D51D
SHA1:	54009D83A2E9FF991180BCBE72ED29A98FCFA66D
SHA-256:	8E7F0999A9C7E9E677B5F6517AC9C5A3FBE6D89FE7AACFD34E9A819D34A2A20E
SHA-512:	6E11A6DC2A6F1BA3295BC5E01734AAA10A936F65437E913AC8D718486E220B960A64D1C3D38CF0A0728D87D586AAA7B916CD8BDCC8BED10BE4CD4C22E9AF9F6
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210802164245..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 536720 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Swift Payment-3134101002.exe..Process ID: 1692..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: 20210802164245..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Swift Payment-3134101002.exe..**********..Command start time: 20210802164517..**********..PS>TerminatingError(Add-MpPreference): "A positional p

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.453387490513826
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Swift Payment-3134101002.exe
File size:	1495040
MD5:	3221d82b7169d545f01f2e2ba94ade25
SHA1:	96326c074c61d3d176f4c6760ce5027b565fad03
SHA256:	41a5f782da40bea08f41a9510a299bfa071c7f84547085f65006c25002802449
SHA512:	c3699599f6649af0919906ea4cc40039c11c22d16a4fae4cdaf23779a1811f405317b9058c3f7cbaa17340e0dad261a3251700c2658f5e10f7aa76242ffd4b10
SSDEEP:	24576:J1oxcVmGXEzFfx8Dgkfx8DgT+rw8ojngl1F4aw1jhzxSbj5mZUYLL:cxQ+F58Dgk58DgJbIFYdxQj4ZUA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....~... ... .@.. .....@.....@.....

File Icon

Icon Hash:	b07968fcd4ec7090

Static PE Info

General

Entrypoint:	0x560c7e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6107C205 [Mon Aug 2 09:59:33 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x15ec84	0x15ee00	False	0.71893856319	data	7.48327692436	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0x162000	0x2e8	0x400	False	0.6943359375	data	5.88739726342	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x164000	0xd62c	0xd800	False	0.708206741898	data	6.59783939226	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x172000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/02/21-16:41:47.058768	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	23890	192.168.2.5	79.134.225.73
08/02/21-16:41:51.890582	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	23890	192.168.2.5	79.134.225.73
08/02/21-16:41:56.612791	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	23890	192.168.2.5	79.134.225.73
08/02/21-16:42:03.499938	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	23890	192.168.2.5	79.134.225.73

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/02/21-16:42:10.415467	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	23890	192.168.2.5	79.134.225.73
08/02/21-16:42:17.750707	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	23890	192.168.2.5	79.134.225.73
08/02/21-16:42:24.307217	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	23890	192.168.2.5	79.134.225.73
08/02/21-16:42:31.204864	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	23890	192.168.2.5	79.134.225.73
08/02/21-16:42:37.998295	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	23890	192.168.2.5	79.134.225.73
08/02/21-16:42:42.962502	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	23890	192.168.2.5	79.134.225.73
08/02/21-16:42:50.403222	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	23890	192.168.2.5	79.134.225.73
08/02/21-16:42:56.846613	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	23890	192.168.2.5	79.134.225.73
08/02/21-16:43:04.763657	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	23890	192.168.2.5	79.134.225.73
08/02/21-16:43:11.242964	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	23890	192.168.2.5	79.134.225.73
08/02/21-16:43:17.840281	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	23890	192.168.2.5	79.134.225.73

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 2, 2021 16:41:41.054807901 CEST	192.168.2.5	8.8.4.4	0xa7b8	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:41:46.771965981 CEST	192.168.2.5	8.8.4.4	0xdd89	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:41:51.733905077 CEST	192.168.2.5	8.8.4.4	0x7e1b	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:41:56.451141119 CEST	192.168.2.5	8.8.4.4	0xc259	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:01.961852074 CEST	192.168.2.5	8.8.4.4	0xfffe	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:10.186383009 CEST	192.168.2.5	8.8.4.4	0x1fe7	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:17.589596033 CEST	192.168.2.5	8.8.4.4	0x73ef	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:24.055679083 CEST	192.168.2.5	8.8.4.4	0x85d3	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:30.967924118 CEST	192.168.2.5	8.8.4.4	0xe93	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:37.348054886 CEST	192.168.2.5	8.8.4.4	0x1933	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:42.710858107 CEST	192.168.2.5	8.8.4.4	0x8906	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:49.929044962 CEST	192.168.2.5	8.8.4.4	0x57c	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:56.599541903 CEST	192.168.2.5	8.8.4.4	0x5926	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:43:04.450381994 CEST	192.168.2.5	8.8.4.4	0x430b	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:43:10.854367971 CEST	192.168.2.5	8.8.4.4	0xdf09	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)
Aug 2, 2021 16:43:17.681235075 CEST	192.168.2.5	8.8.4.4	0xced8	Standard query (0)	yota890.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 2, 2021 16:41:41.091090918 CEST	8.8.4.4	192.168.2.5	0xa7b8	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:41:46.809206009 CEST	8.8.4.4	192.168.2.5	0xdd89	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:41:51.766741991 CEST	8.8.4.4	192.168.2.5	0x7e1b	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:41:56.488117933 CEST	8.8.4.4	192.168.2.5	0xc259	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:01.994751930 CEST	8.8.4.4	192.168.2.5	0xfffe	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:10.218887091 CEST	8.8.4.4	192.168.2.5	0x1fe7	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:17.618062019 CEST	8.8.4.4	192.168.2.5	0x73ef	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:24.091873884 CEST	8.8.4.4	192.168.2.5	0x85d3	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:31.002733946 CEST	8.8.4.4	192.168.2.5	0xe93	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:37.381407976 CEST	8.8.4.4	192.168.2.5	0x1933	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:42.748768091 CEST	8.8.4.4	192.168.2.5	0x8906	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:49.962647915 CEST	8.8.4.4	192.168.2.5	0x57c	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:42:56.631890059 CEST	8.8.4.4	192.168.2.5	0x5926	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:43:04.485606909 CEST	8.8.4.4	192.168.2.5	0x430b	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:43:10.892431021 CEST	8.8.4.4	192.168.2.5	0xdf09	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)
Aug 2, 2021 16:43:17.716440916 CEST	8.8.4.4	192.168.2.5	0xced8	No error (0)	yota890.hopto.org		79.134.225.73	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Swift Payment-3134101002.exe PID: 896 Parent PID: 5768

General

Start time:	16:41:11
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Swift Payment-3134101002.exe'
Imagebase:	0xc90000
File size:	1495040 bytes
MD5 hash:	3221D82B7169D545F01F2E2BA94ADE25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2896 Parent PID: 896

General

Start time:	16:41:27
Start date:	02/08/2021
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\Swift Payment-3134101002.exe'
Imagebase:	0xf50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 3228 Parent PID: 2896

General

Start time:	16:41:28
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 5908 Parent PID: 896

General

Start time:	16:41:28
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe'
Imagebase:	0xf50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 2952 Parent PID: 5908

General

Start time:	16:41:29
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5452 Parent PID: 896

General

Start time:	16:41:29
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TPiUrUItCGsY' /XML 'C:\Users\user\AppData\Local\Temp\tmpD9EC.tmp'
Imagebase:	0x12b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 3888 Parent PID: 5452

General

Start time:	16:41:29
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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: 4500 Parent PID: 896

General

Start time:	16:41:30
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe'
Imagebase:	0xf50000
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: Swift Payment-3134101002.exe PID: 5848 Parent PID: 896

General

Start time:	16:41:31
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
Imagebase:	0xa0000
File size:	1495040 bytes
MD5 hash:	3221D82B7169D545F01F2E2BA94ADE25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 980 Parent PID: 4500

General

Start time:	16:41:30
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: Swift Payment-3134101002.exe PID: 5260 Parent PID: 896

General

Start time:	16:41:32
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
Imagebase:	0x4d0000
File size:	1495040 bytes
MD5 hash:	3221D82B7169D545F01F2E2BA94ADE25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.504645095.0000000003D3A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.492657764.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.492657764.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.492657764.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.502833366.0000000002D3D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 5872 Parent PID: 5260

General

Start time:	16:41:35
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp54AF.tmp'
Imagebase:	0x12b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 1188 Parent PID: 5872

General

Start time:	16:41:36
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6172 Parent PID: 5260

General

Start time:	16:41:36
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp5992.tmp'
Imagebase:	0x12b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Swift Payment-3134101002.exe PID: 6208 Parent PID: 904

General

Start time:	16:41:37
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Swift Payment-3134101002.exe' 0
Imagebase:	0x860000
File size:	1495040 bytes

MD5 hash:	3221D82B7169D545F01F2E2BA94ADE25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6236 Parent PID: 6172

General

Start time:	16:41:37
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 6580 Parent PID: 904

General

Start time:	16:41:41
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xd00000
File size:	1495040 bytes
MD5 hash:	3221D82B7169D545F01F2E2BA94ADE25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: dhcpmon.exe PID: 6812 Parent PID: 3472

General

Start time:	16:41:45
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x840000
File size:	1495040 bytes
MD5 hash:	3221D82B7169D545F01F2E2BA94ADE25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 1692 Parent PID: 6208

General

Start time:	16:42:41
Start date:	02/08/2021
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\Swift Payment-3134101002.exe'
Imagebase:	0xf50000
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: 2248 Parent PID: 1692

General

Start time:	16:42:42
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 1332 Parent PID: 6208

General

Start time:	16:42:42
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TPiUrUItCGsY' /XML 'C:\Users\user\AppData\Local\Temp\tmpF33C.tmp'
Imagebase:	0x12b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6740 Parent PID: 1332

General

Start time:	16:42:43
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 5492 Parent PID: 6208

General

Start time:	16:42:44
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\TPiUrUItCGsY.exe'
Imagebase:	0xf50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: Swift Payment-3134101002.exe PID: 5436 Parent PID: 6208

General

Start time:	16:42:46
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Swift Payment-3134101002.exe
Imagebase:	0x5a0000
File size:	1495040 bytes
MD5 hash:	3221D82B7169D545F01F2E2BA94ADE25
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000002A.00000002.453841025.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000002A.00000002.453841025.0000000002D01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000002A.00000002.446482666.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000002A.00000002.446482666.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000002A.00000002.446482666.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000002A.00000002.453923165.0000000003D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000002A.00000002.453923165.0000000003D01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: conhost.exe PID: 5076 Parent PID: 5492

General

Start time:	16:42:45
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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