ID: 432424
Sample Name:
SwiftCopy.pdf.exe
Cookbook: default.jbs
Time: 10:32:54
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

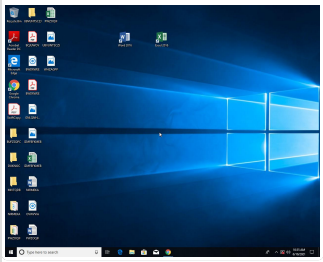
Analysis Report SwiftCopy.pdf.exe

Overview

General Information

Sample Name:	SwiftCopy.pdf.exe
Analysis ID:	432424
MD5:	5a13130ec1c425..
SHA1:	ec4a42085f6c4fd..
SHA256:	85c856fe483e3a2.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

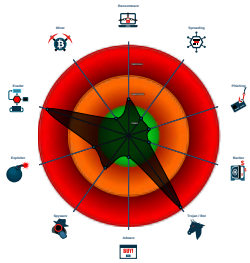
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Suspicious Double …
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- SwiftCopy.pdf.exe (PID: 6872 cmdline: 'C:\Users\user\Desktop\SwiftCopy.pdf.exe' MD5: 5A13130EC1C4259C3F63FA48167AB094)
  - schtasks.exe (PID: 6348 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xetNJdChYOitP' /XML 'C:\Users\user\AppData\Local\Temp\tmpF25B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SwiftCopy.pdf.exe (PID: 6468 cmdline: {path} MD5: 5A13130EC1C4259C3F63FA48167AB094)
  - SwiftCopy.pdf.exe (PID: 6476 cmdline: {path} MD5: 5A13130EC1C4259C3F63FA48167AB094)
    - schtasks.exe (PID: 6576 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpDE76.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6704 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpE388.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- SwiftCopy.pdf.exe (PID: 7040 cmdline: C:\Users\user\Desktop\SwiftCopy.pdf.exe 0 MD5: 5A13130EC1C4259C3F63FA48167AB094)
  - schtasks.exe (PID: 2204 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xetNJdChYOitP' /XML 'C:\Users\user\AppData\Local\Temp\tmp994A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SwiftCopy.pdf.exe (PID: 2848 cmdline: {path} MD5: 5A13130EC1C4259C3F63FA48167AB094)
- dhcpmon.exe (PID: 5848 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 5A13130EC1C4259C3F63FA48167AB094)
- dhcpmon.exe (PID: 6152 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 5A13130EC1C4259C3F63FA48167AB094)
  - schtasks.exe (PID: 2860 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xetNJdChYOitP' /XML 'C:\Users\user\AppData\Local\Temp\tmpBC24.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6892 cmdline: {path} MD5: 5A13130EC1C4259C3F63FA48167AB094)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-000c0a4c",
  "Group": "Ego come se",
  "Domain1": "sylviaoslh01.ddns.net",
  "Domain2": "194.5.98.31",
  "Port": 52943,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "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
00000020.00000000.836222469.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000020.00000000.836222469.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000020.00000000.836222469.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000001D.00000000.819759981.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001D.00000000.819759981.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 66 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
29.0.SwiftCopy.pdf.exe.400000.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
29.0.SwiftCopy.pdf.exe.400000.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
29.0.SwiftCopy.pdf.exe.400000.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
29.0.SwiftCopy.pdf.exe.400000.3.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
11.2.SwiftCopy.pdf.exe.5d70000.11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 141 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicious Double Extension

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

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

Networking:

- C2 URLs / IPs found in malware configuration
- Connects to many ports of the same IP (likely port scanning)
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

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

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

- Icon mismatch, binary includes an icon from a different legit application in order to fool users
- Hides that the sample has been downloaded from the Internet (zone.identifier)
- Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

Remote Access Functionality:

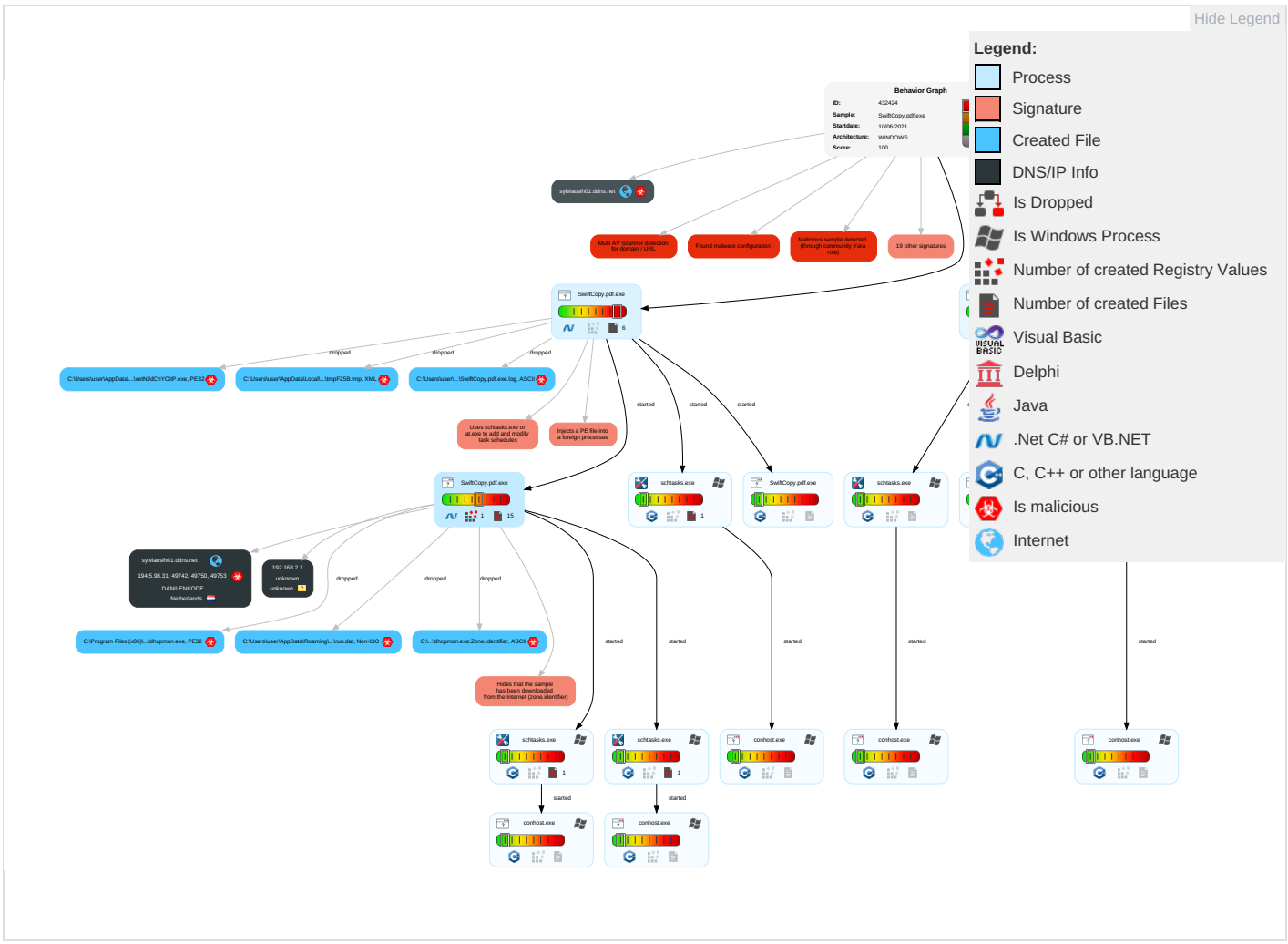
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	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	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 1 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 1	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoc
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	Rogue Base S

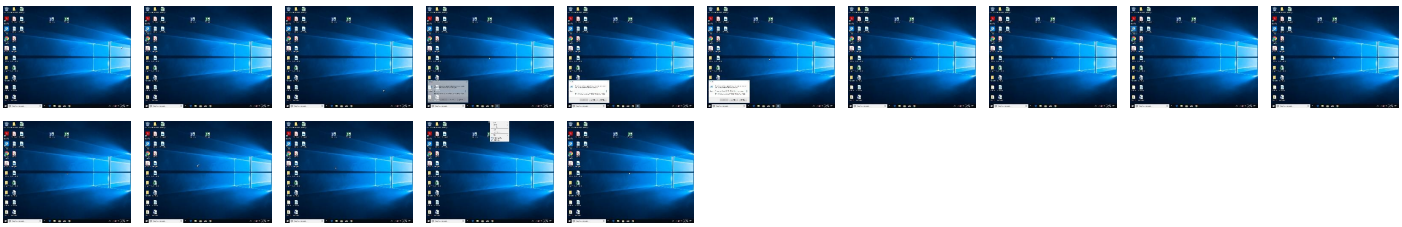
Behavior Graph



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
SwiftCopy.pdf.exe	44%	ReversingLabs		
SwiftCopy.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\xetNJdChYOitP.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	44%	ReversingLabs		
C:\Users\user\AppData\Roaming\xetNJdChYOitP.exe	44%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.SwiftCopy.pdf.exe.4332580.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
29.0.SwiftCopy.pdf.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.SwiftCopy.pdf.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.dhcpmon.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.SwiftCopy.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
29.2.SwiftCopy.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.SwiftCopy.pdf.exe.5d70000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
32.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.SwiftCopy.pdf.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
29.0.SwiftCopy.pdf.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
sylviaoslh01.ddns.net	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/D	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/L	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp//	0%	Virustotal		Browse
http://www.jiyu-kobo.co.jp/jp//	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/0	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com6	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0h	0%	Avira URL Cloud	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.fontbureau.comef	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.carterandcone.comP	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/&	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/&	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/&	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.carterandcone.comr	0%	Avira URL Cloud	safe	
194.5.98.31	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/q	0%	Avira URL Cloud	safe	
http://www.carterandcone.comv	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sylviaoslh01.ddns.net	194.5.98.31	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
194.5.98.31	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
sylviaoslh01.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.31	sylviaoslh01.ddns.net	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432424
Start date:	10.06.2021
Start time:	10:32:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SwiftCopy.pdf.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:	34
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@27/13@13/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.6%) • Quality average: 91.6% • Quality standard deviation: 10.7%
HCA Information:	• Successful, ratio: 99% • 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
10:34:15	API Interceptor	660x Sleep call for process: SwiftCopy.pdf.exe modified
10:34:22	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\SwiftCopy.pdf.exe" s>$(Arg0)
10:34:24	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
10:34:25	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
10:35:06	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.31	TPA AGREEMENT00038499530.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sylviaoslh01.ddns.net	TPA AGREEMENT00038499530.exe	Get hash	malicious	Browse	• 154.118.45.15
	0672IMP000158021.pdf.exe	Get hash	malicious	Browse	• 185.244.30.13
	C3GWn5tduT.exe	Get hash	malicious	Browse	• 197.242.98.161
	a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe	Get hash	malicious	Browse	• 194.5.97.207
	3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe	Get hash	malicious	Browse	• 194.5.97.207
	5zLV4brBQ7.exe	Get hash	malicious	Browse	• 194.5.97.207
	Bank Information.exe	Get hash	malicious	Browse	• 41.217.47.187
	0712020.exe	Get hash	malicious	Browse	• 41.217.69.179
	HSBCdoc24523820201117161551.exe	Get hash	malicious	Browse	• 194.5.98.180

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	wlCqbMRJ7p.exe	Get hash	malicious	Browse	• 194.5.98.5
	SecuriteInfo.com.Trojan.PackedNET.832.3222.exe	Get hash	malicious	Browse	• 194.5.98.144
	SecuriteInfo.com.Trojan.PackedNET.831.12541.exe	Get hash	malicious	Browse	• 194.5.98.144
	0Cg1YYs1sv.exe	Get hash	malicious	Browse	• 194.5.98.144
	Duplicated Orders.xlsx	Get hash	malicious	Browse	• 194.5.98.144
	DEPOSITAR.xlsx	Get hash	malicious	Browse	• 194.5.98.144
	InvoicePOzGlybgcIc1vHasG.exe	Get hash	malicious	Browse	• 194.5.98.87
	POInvoiceOrderIuVvcl0VWEOAmXy.exe	Get hash	malicious	Browse	• 194.5.98.87
	payment invoice.exe	Get hash	malicious	Browse	• 194.5.98.23
	#RFQ ORDER484475577797.exe	Get hash	malicious	Browse	• 194.5.98.120
	b6yzWugw8V.exe	Get hash	malicious	Browse	• 194.5.98.107
	0041#Receipt.pif.exe	Get hash	malicious	Browse	• 194.5.98.180
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.18
	SecuriteInfo.com.Trojan.PackedNET.820.24493.exe	Get hash	malicious	Browse	• 194.5.97.61
	DHL_file.exe	Get hash	malicious	Browse	• 194.5.98.145
	BBS FX.xlsx	Get hash	malicious	Browse	• 194.5.97.61
	GpnPv433gb.exe	Get hash	malicious	Browse	• 194.5.98.11
	Kj7tTd1Zimp0cil.exe	Get hash	malicious	Browse	• 194.5.97.197

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	793088
Entropy (8bit):	6.728969427122061
Encrypted:	false
SSDEEP:	12288:ipbyAsdHyDOfkigFIjGGe3OK+CwiVDkWqqLEkHqc0E:KWAiHiOMiaIyFOKHNVgjryF0E
MD5:	5A13130EC1C4259C3F63FA48167AB094
SHA1:	EC4A42085F6C4FD6FBD79705723C8D034F24EBAD
SHA-256:	85C856FE483E3A2EF7A4417693DC121C42673AC426CB8CF486FBE20B4825636A
SHA-512:	CE38522E50ADACE8D49720CD8F05183ED051ACA11C2FAE6EAB5C2D5EC830D831B041016E6B1AA9019C78803B8456A7052C1EDE99E09E8A11FB1039DFF50490 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 44%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...)2.`.....0.....p..... .....@.. ..... ..@.....O.....m.....`.....\..... ....H.....text..... ....`.rsrc....m.....n.....@..@.relo c.....`.....@..B.....H.....$...8.....^.}.....(.....(*....*.0..T.....r...ps.....o.....r...p...s.....o....&s.....s.....o....&.{.....o.. ....o.....*.0.....{....o....o....r<..p(.....{....o....o....r<..p(...._.{....o....o....r<..p(...._.{....o....o....r<..p(...._.{....o....o....r<..p(...._.{....o. ...o....r<..p(...._..9.....r...ps.....o.....{.....{....o....(....{....o....(

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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\SwiftCopy.pdf.exe.log	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.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:	**true**
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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
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_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp994A.tmp	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.183748957987971
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG/ntn:cbhK79lNQR/rydbz9I3YODOLNdq3It
MD5:	E768B7AC7BE721211F882B89152C81EC
SHA1:	0B9869E31A443D80BF82BE67C249FAC94651D881
SHA-256:	F36D60E3C11650CC66D572D7C7A6C67E0E946D0965C61D05FAB4C98EDA1F48D7
SHA-512:	052C5BBE2297993F679E942FE59A4D7E6CE32CAABF9574F081E51F3262292DDCFE3039419AF28F2FF9E92592BC6ADCC099676A7BFC8A9C555F2A721AEFBE711B
Malicious:	false
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>true

C:\Users\user\AppData\Local\Temp\tmpBC24.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.183748957987971
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG/ntn:cbhK79lNQR/rydbz9I3YODOLNdq3It
MD5:	E768B7AC7BE721211F882B89152C81EC
SHA1:	0B9869E31A443D80BF82BE67C249FAC94651D881
SHA-256:	F36D60E3C11650CC66D572D7C7A6C67E0E946D0965C61D05FAB4C98EDA1F48D7
SHA-512:	052C5BBE2297993F679E942FE59A4D7E6CE32CAABF9574F081E51F3262292DDCFE3039419AF28F2FF9E92592BC6ADCC099676A7BFC8A9C555F2A721AEFBE711B
Malicious:	false
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>true

C:\Users\user\AppData\Local\Temp\tmpDE76.tmp	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1303
Entropy (8bit):	5.101879798382705
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Ywmxtn:cbk4oL600QydbQxlYODOLedq39j
MD5:	9277324E6C97922D77E8C5B805F560BF
SHA1:	7C0F8E50ED343C7018218433E0D625D6744A5BD7
SHA-256:	76717189D5111F393F2764E76D62E105AC2DAE9EE657D177CFC2225B4FCFD93E

C:\Users\user\AppData\Local\Temp\tmpDE76.tmp	
SHA-512:	8E1264E37C72865AC0CE57FAF831B390428123BAD490A53C6738E1488733B067024D5AF76F189870BE29E239E9E58B8C3126D51787064662756191EADAD07ACE
Malicious:	false
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\tmpE388.tmp	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.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
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\tmpF25B.tmp	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.183748957987971
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG/ntn:cbhK79lNQR/rydbz9l3YODOLNdq3lt
MD5:	E768B7AC7BE721211F882B89152C81EC
SHA1:	0B9869E31A443D80BF82BE67C249FAC94651D881
SHA-256:	F36D60E3C11650CC66D572D7C7A6C67E0E946D0965C61D05FAB4C98EDA1F48D7
SHA-512:	052C5BBE2297993F679E942FE59A4D7E6CE32CAABF9574F081E51F3262292DDCFE3039419AF28F2FF9E92592BC6ADCC099676A7BFC8A9C555F2A721AEFBE711B
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
File Type:	data
Category:	modified
Size (bytes):	2728
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	48:Ik/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH87:ft3Ucrt3Ucrt3Ucrt3Ucrt3UcrN
MD5:	3F16EC9869DEDFFEC07792CA71B87AB5
SHA1:	124F3AAEB04E11DEA7361736CE472750D237D3D2
SHA-256:	1A187F3EF38284FF4EE2B20D6021C884E42FC72284F2DA858D7E389CE9C7D0E9
SHA-512:	8DDE0277C2F8CF1CEF64B1EDF120C4A239619FBE9513C833C94B9A429984ECB8AD2A346FD9E333270207951021CCB0CA08FFCDF2ADE538AAFC2B5FAAA1ADF0A2
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
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....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.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....f.Z#.|...@HkG....G..O*V.....pz...."... .r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.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....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.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....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:mPhn:4h
MD5:	1F09E9E971FDD1CF98B64E2FDF0D7BFE
SHA1:	C7FD38D5D15CA82BBAA36C61297051F0393C6800
SHA-256:	B958CDE5917C67F83AE71142141AB5E7BC489C01D2A02391DB0889D8D5DB9A2F
SHA-512:	814524AC8A197D8EF0A3430806814A43A07840AB52813278928AAC4CE98857C4AFEE7751440EB3BAD7F3A06616305FC3F85F4086D677A7F2D2E94038FA290A08
Malicious:	**true**
Preview:	.O...+.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.193942707918268
Encrypted:	false
SSDEEP:	3:oNt+WfW2SS3cT0C:oNwv2l7C
MD5:	EC4B6BB237CA5039FA75EC510514D266
SHA1:	6AFEE68877A36DA2C6FBD3282F38BD885E6FE348
SHA-256:	127CDA974A1E5B25020A36DA2727CD76DD317883513861D4AA5CB27B7E89AF0B
SHA-512:	B27F5C08E7D6BD8CF106E444C06F2789396393260F3748959E296735E2027F76FC8AB5257F969B438749287115A50A8147333928A120DDBC1242B2B1A8EEEB2B
Malicious:	false
Preview:	C:\Users\user\Desktop\SwiftCopy.pdf.exe

C:\Users\user\AppData\Roaming\xetNJdChYOitP.exe	
Process:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	793088
Entropy (8bit):	6.728969427122061
Encrypted:	false
SSDEEP:	12288:ipbyAsdHyDOfkigFIjGGe3OK+CwiVDkWqqLEkHqc0E:KWAiHiOMiaIyFOKHNVgjryF0E
MD5:	5A13130EC1C4259C3F63FA48167AB094
SHA1:	EC4A42085F6C4FD6FBD79705723C8D034F24EBAD
SHA-256:	85C856FE483E3A2EF7A4417693DC121C42673AC426CB8CF486FBE20B4825636A
SHA-512:	CE38522E50ADACE8D49720CD8F05183ED051ACA11C2FAE6EAB5C2D5EC830D831B041016E6B1AA9019C78803B8456A7052C1EDE99E09E8A11FB1039DFF504906
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 44%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...)2.`.....0.....p..... .....@.. ..... ..@.....O.....m.....`.....\..... ....H.....text..... ....`.rsrc....m.....n.....@..@.relo c.....`.....@..B.....H.....$...8.....^.}.....(.....(*....*.0..T.....r...ps.....o.....r...p...s.....o....&s.....s.....o....&.{.....o.. ....o.....*.0.....{....o....o....r<..p(....{....o....o....r<..p(...._.{....o....o....r<..p(...._.{....o....o....r<..p(...._.{....o....o....r<..p(...._.{....o. ...o....r<..p(...._..9.....r...ps.....o.....{.....{....o....(....{....o....(

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.728969427122061
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SwiftCopy.pdf.exe
File size:	793088
MD5:	5a13130ec1c4259c3f63fa48167ab094
SHA1:	ec4a42085f6c4fd6fbd79705723c8d034f24ebad
SHA256:	85c856fe483e3a2ef7a4417693dc121c42673ac426cb8cf486fbe20b4825636a
SHA512:	ce38522e50adace8d49720cd8f05183ed051aca11c2fae6eab5c2d5ec830d831b041016e6b1aa9019c78803b8456a7052c1ede99e09e8a11fb1039dff5049086
SSDEEP:	12288:ipbyAsdHyDOfkigFljGGe3OK+CwiVDkWqqLEkHqc0E:KWAiHiOMiaIyFOKHNVgjryF0E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...)2.`.....0.....p..... .....@.. .....@.....

File Icon

Icon Hash:	e28eac86b2968eb2

Static PE Info

General

Entrypoint:	0x48c6e6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C13229 [Wed Jun 9 21:27:05 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	0x8a6ec	0x8a800	False	0.789103043208	data	7.53870171772	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0x36dc8	0x36e00	False	0.0571122223804	data	2.50601914036	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 10:34:27.262192011 CEST	192.168.2.4	8.8.8.8	0x90c8	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:33.723819017 CEST	192.168.2.4	8.8.8.8	0xfd47	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:40.045242071 CEST	192.168.2.4	8.8.8.8	0x8afa	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:46.480256081 CEST	192.168.2.4	8.8.8.8	0x9319	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:52.862509012 CEST	192.168.2.4	8.8.8.8	0x7d5	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:59.221124887 CEST	192.168.2.4	8.8.8.8	0xfd24	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:06.964653015 CEST	192.168.2.4	8.8.8.8	0x325c	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:13.321352005 CEST	192.168.2.4	8.8.8.8	0xadee	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:20.150182962 CEST	192.168.2.4	8.8.8.8	0xd31f	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:26.746030092 CEST	192.168.2.4	8.8.8.8	0xa3b6	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:33.270361900 CEST	192.168.2.4	8.8.8.8	0xf1a2	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:39.698998928 CEST	192.168.2.4	8.8.8.8	0xf15b	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:45.966790915 CEST	192.168.2.4	8.8.8.8	0xd4be	Standard query (0)	sylviaoslh 01.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 10:34:27.328581095 CEST	8.8.8.8	192.168.2.4	0x90c8	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:33.785756111 CEST	8.8.8.8	192.168.2.4	0xfd47	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:40.109802961 CEST	8.8.8.8	192.168.2.4	0x8afa	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:46.540632963 CEST	8.8.8.8	192.168.2.4	0x9319	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:52.923218966 CEST	8.8.8.8	192.168.2.4	0x7d5	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:34:59.284426928 CEST	8.8.8.8	192.168.2.4	0xfd24	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 10:35:07.024833918 CEST	8.8.8.8	192.168.2.4	0x325c	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:13.380218029 CEST	8.8.8.8	192.168.2.4	0xadee	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:20.211251020 CEST	8.8.8.8	192.168.2.4	0xd31f	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:26.806623936 CEST	8.8.8.8	192.168.2.4	0xa3b6	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:33.331773043 CEST	8.8.8.8	192.168.2.4	0xf1a2	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:39.758059025 CEST	8.8.8.8	192.168.2.4	0xf15b	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)
Jun 10, 2021 10:35:46.028119087 CEST	8.8.8.8	192.168.2.4	0xd4be	No error (0)	sylviaoslh 01.ddns.net		194.5.98.31	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SwiftCopy.pdf.exe PID: 6872 Parent PID: 5940

General

Start time:	10:33:38
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SwiftCopy.pdf.exe'
Imagebase:	0x960000
File size:	793088 bytes
MD5 hash:	5A13130EC1C4259C3F63FA48167AB094
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.741715588.00000000045C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.741715588.00000000045C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.741715588.00000000045C0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.734043460.00000000041D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.734043460.00000000041D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.734043460.00000000041D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6348 Parent PID: 6872

General

Start time:	10:34:15
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xetNJdChYOitP' /XML 'C:\Users\user\AppData\Local\Temp\tmpF25B.tmp'
Imagebase:	0xb20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6344 Parent PID: 6348

General

Start time:	10:34:16
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: SwiftCopy.pdf.exe PID: 6468 Parent PID: 6872

General

Start time:	10:34:17
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x200000
File size:	793088 bytes
MD5 hash:	5A13130EC1C4259C3F63FA48167AB094
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SwiftCopy.pdf.exe PID: 6476 Parent PID: 6872

General

Start time:	10:34:17
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9d0000
File size:	793088 bytes
MD5 hash:	5A13130EC1C4259C3F63FA48167AB094
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.912587333.0000000005D60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.912587333.0000000005D60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.911932177.00000000054D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.911932177.00000000054D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.726462560.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.726462560.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.726462560.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.912619347.0000000005D70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.912619347.0000000005D70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.912619347.0000000005D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.908625280.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.908625280.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.908625280.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.911022966.0000000004319000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.726040524.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.726040524.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.726040524.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 6576 Parent PID: 6476

General

Start time:	10:34:20
Start date:	10/06/2021
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\tmpDE76.tmp'
Imagebase:	0xb20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6632 Parent PID: 6576

General

Start time:	10:34:20
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6704 Parent PID: 6476

General

Start time:	10:34:21
Start date:	10/06/2021
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\tmpE388.tmp'
Imagebase:	0xb20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6988 Parent PID: 6704

General

Start time:	10:34:22
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: SwiftCopy.pdf.exe PID: 7040 Parent PID: 968

General

Start time:	10:34:22
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SwiftCopy.pdf.exe 0
Imagebase:	0xdd0000
File size:	793088 bytes
MD5 hash:	5A13130EC1C4259C3F63FA48167AB094
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.826910629.0000000004641000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.826910629.0000000004641000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.826910629.0000000004641000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5848 Parent PID: 968

General

Start time:	10:34:25
Start date:	10/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x340000
File size:	793088 bytes
MD5 hash:	5A13130EC1C4259C3F63FA48167AB094

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.820471977.0000000003A31000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.820471977.0000000003A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.820471977.0000000003A31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 44%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 6152 Parent PID: 3424

General

Start time:	10:34:33
Start date:	10/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x6b0000
File size:	793088 bytes
MD5 hash:	5A13130EC1C4259C3F63FA48167AB094
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.841434727.0000000003D51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.841434727.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.841434727.0000000003D51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2204 Parent PID: 7040

General

Start time:	10:34:59
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xetNJdChYOitP' /XML 'C:\Users\user\AppData\Local\Temp\tmp994A.tmp'
Imagebase:	0xb20000
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: 5972 Parent PID: 2204

General

Start time:	10:35:00
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: SwiftCopy.pdf.exe PID: 2848 Parent PID: 7040

General

Start time:	10:35:01
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\SwiftCopy.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd30000
File size:	793088 bytes
MD5 hash:	5A13130EC1C4259C3F63FA48167AB094
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000000.819759981.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000000.819759981.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000000.819759981.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000002.835267863.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.835267863.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.835267863.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000000.820327781.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000000.820327781.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000000.820327781.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.836835816.0000000003391000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.836835816.0000000003391000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.836971548.0000000004391000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.836971548.0000000004391000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 2860 Parent PID: 6152

General

Start time:	10:35:07
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xetNJdChYOitP' /XML 'C:\Users\user\AppData\Local\Temp\tmpBC24.tmp'
Imagebase:	0xb20000
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: 4800 Parent PID: 2860

General

Start time:	10:35:08
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: dhcpmon.exe PID: 6892 Parent PID: 6152

General

Start time:	10:35:08
Start date:	10/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x6a0000
File size:	793088 bytes
MD5 hash:	5A13130EC1C4259C3F63FA48167AB094
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.836222469.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.836222469.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.836222469.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.857250258.0000000002F31000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.857250258.0000000002F31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000002.852127142.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.852127142.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.852127142.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.835581816.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.835581816.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.835581816.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.857349420.0000000003F31000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.857349420.0000000003F31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis