ID: 433513
Sample Name: SPECIALISED SWIFT.EXE
Cookbook: default.jbs
Time: 07:55:28
Date: 12/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

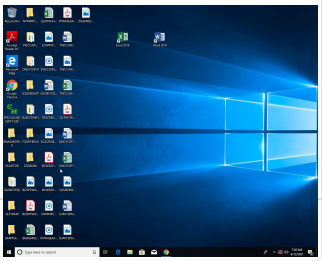
Analysis Report SPECIALISED SWIFT.EXE

Overview

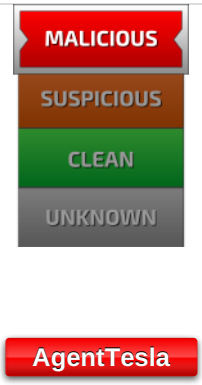
General Information

Sample Name:	SPECIALISED SWIFT.EXE
Analysis ID:	433513
MD5:	9059051337f38ff…
SHA1:	77bc68c84dac38…
SHA256:	1260c526c6bc88…
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

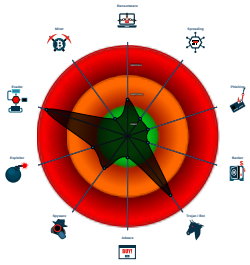


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- SPECIALISED SWIFT.EXE (PID: 6044 cmdline: 'C:\Users\user\Desktop\SPECIALISED SWIFT.EXE' MD5: 9059051337F38FF19504E7C53FA8FDF8)
  - schtasks.exe (PID: 3688 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VWIpnm' /XML 'C:\Users\user\AppData\Local\Temp\tmp551C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SPECIALISED SWIFT.EXE (PID: 5048 cmdline: {path} MD5: 9059051337F38FF19504E7C53FA8FDF8)
- pGKuRU.exe (PID: 1260 cmdline: 'C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe' MD5: 9059051337F38FF19504E7C53FA8FDF8)
  - schtasks.exe (PID: 5220 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VWIpnm' /XML 'C:\Users\user\AppData\Local\Temp\tmp74D4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - pGKuRU.exe (PID: 5252 cmdline: {path} MD5: 9059051337F38FF19504E7C53FA8FDF8)
- pGKuRU.exe (PID: 492 cmdline: 'C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe' MD5: 9059051337F38FF19504E7C53FA8FDF8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "info@aluminatiglass.co.zaP@ssword123mail.aluminatiglass.co.za"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000002.460180951.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001F.00000002.460180951.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000000.286401273.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000000.286401273.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001F.00000000.438877169.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SPECIALISED SWIFT.EXE.40296f8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SPECIALISED SWIFT.EXE.40296f8.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
22.2.pGKuRU.exe.4a79c80.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
22.2.pGKuRU.exe.4a79c80.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.0.SPECIALISED SWIFT.EXE.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Sigma Overview

No Sigma rule has matched

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 dropped file

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large array initializations

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)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Tries to delay execution (extensive OutputDebugStringW loop)

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 AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

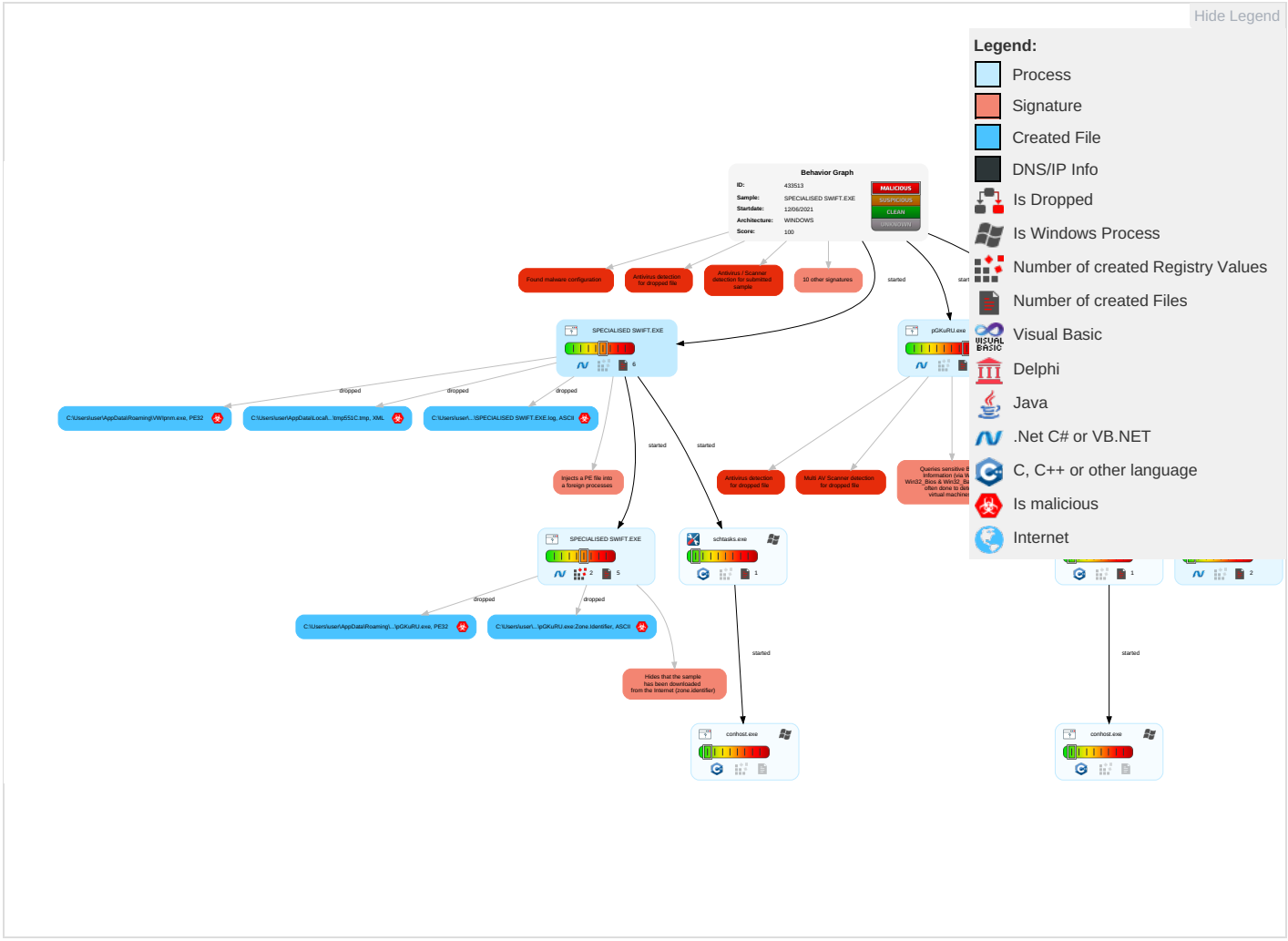
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 3 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 4 1	Security Account Manager	Virtualization/Sandbox Evasion 2 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

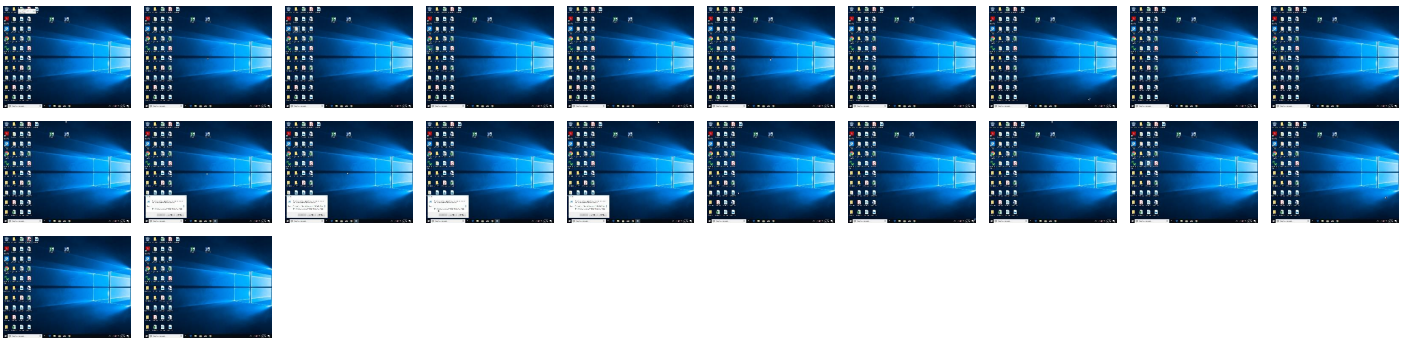
Behavior Graph



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
SPECIALISED SWIFT.EXE	55%	Virustotal		Browse
SPECIALISED SWIFT.EXE	28%	ReversingLabs	Win32.Trojan.AgentTesla	
SPECIALISED SWIFT.EXE	100%	Avira	HEUR/AGEN.1129504	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe	100%	Avira	HEUR/AGEN.1129504	
C:\Users\user\AppData\Roaming\VWIpnm.exe	100%	Avira	HEUR/AGEN.1129504	
C:\Users\user\AppData\Roaming\VWIpnm.exe	55%	Virustotal		Browse
C:\Users\user\AppData\Roaming\VWIpnm.exe	28%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe	55%	Virustotal		Browse
C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe	28%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.0.pGKuRU.exe.860000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
0.0.SPECIALISED SWIFT.EXE.b40000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
31.2.pGKuRU.exe.860000.1.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
23.2.pGKuRU.exe.5f0000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File

Source	Detection	Scanner	Label	Link	Download
14.0.SPECIALISED SWIFT.EXE.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.SPECIALISED SWIFT.EXE.b40000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
22.2.pGKuRU.exe.d80000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
14.2.SPECIALISED SWIFT.EXE.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.2.pGKuRU.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.0.pGKuRU.exe.d80000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
31.0.pGKuRU.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.0.pGKuRU.exe.860000.2.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
14.2.SPECIALISED SWIFT.EXE.e20000.1.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
14.0.SPECIALISED SWIFT.EXE.e20000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
14.0.SPECIALISED SWIFT.EXE.e20000.2.unpack	100%	Avira	HEUR/AGEN.1129504		Download File
23.0.pGKuRU.exe.5f0000.0.unpack	100%	Avira	HEUR/AGEN.1129504		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://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.tiro.com	0%	URL Reputation	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.goodfont.co.kr	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.carterandcone.coml	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.sajatypeworks.com	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.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/cn/cThe	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://fontfabrik.com	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	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%	URL Reputation	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.galapagosdesign.com/DPlease	0%	URL Reputation	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.sandoll.co.kr	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.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.zhongyicts.com.cn	0%	URL Reputation	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.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://VgqbOm.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433513
Start date:	12.06.2021
Start time:	07:55:28
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 10m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SPECIALISED SWIFT.EXE
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@13/8@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.6%) • Quality average: 41% • Quality standard deviation: 34.7%
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
07:57:09	API Interceptor	502x Sleep call for process: SPECIALISED SWIFT.EXE modified
07:57:20	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run pGKuRU C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe
07:57:29	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run pGKuRU C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SPECIALISED SWIFT.EXE.log	
Process:	C:\Users\user\Desktop\SPECIALISED SWIFT.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pGKuRU.exe.log	
Process:	C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp551C.tmp	
Process:	C:\Users\user\Desktop\SPECIALISED SWIFT.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.186021383576324
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBStn:cbh47TlNQ//rydbz9l3YODOLNdq3K
MD5:	232607EB047CBE82A2058089407BCBBF
SHA1:	6C26E0F60F679F8DB2706819B455DDDF9E93D536
SHA-256:	2056F2A86666B42B7EE11865237C3B994499515260B8071B2B38C8436E640F4A
SHA-512:	DF7872D199572A10458BBC95F5A7A547BCF67BE1C965ABF35B9A47C3EB234CDEE60EDBED8FA667E588CD4A01A3395BD3CFDD056F5E959E46751F25E20AA7140E

C:\Users\user\AppData\Local\Temp\tmp551C.tmp	
Malicious:	**true**
Reputation:	low
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\tmp74D4.tmp	
Process:	C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.186021383576324
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBStn:cbh47TlNQ//rydbz9I3YODOLNdq3K
MD5:	232607EB047CBE82A2058089407BCBBF
SHA1:	6C26E0F60F679F8DB2706819B455DDDF9E93D536
SHA-256:	2056F2A86666B42B7EE11865237C3B994499515260B8071B2B38C8436E640F4A
SHA-512:	DF7872D199572A10458BBC95F5A7A547BCF67BE1C965ABF35B9A47C3EB234CDEE60EDBED8FA667E588CD4A01A3395BD3CFDD056F5E959E46751F25E20AA714 0E
Malicious:	false
Reputation:	low
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\tmp9D5B.tmp	
Process:	C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.186021383576324
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBStn:cbh47TlNQ//rydbz9I3YODOLNdq3K
MD5:	232607EB047CBE82A2058089407BCBBF
SHA1:	6C26E0F60F679F8DB2706819B455DDDF9E93D536
SHA-256:	2056F2A86666B42B7EE11865237C3B994499515260B8071B2B38C8436E640F4A
SHA-512:	DF7872D199572A10458BBC95F5A7A547BCF67BE1C965ABF35B9A47C3EB234CDEE60EDBED8FA667E588CD4A01A3395BD3CFDD056F5E959E46751F25E20AA714 0E
Malicious:	false
Reputation:	low
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\VWIpnm.exe	
Process:	C:\Users\user\Desktop\SPECIALISED SWIFT.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	600064
Entropy (8bit):	7.569327488915576
Encrypted:	false
SSDEEP:	12288:EKl4DoplA0tnkhyMe2sol51Rt4P9b3MPl1mh6uK9T2s8qaK83PC/Oyd7sY:J4DopFnkhyMeQl5OMN1mho9T6Y
MD5:	9059051337F38FF19504E7C53FA8FDF8
SHA1:	77BC68C84DAC387CE4774E3549E2A0701AF44481
SHA-256:	1260C526C6BC88A3C92603AA3826B6581DFD134479CF4054CBC3DE3DF513D4A0
SHA-512:	62C8609083282F2961110D9CD5BFC6CCE45567DA708D62A3835E3188770456AA8C46654F0C7EF0490972D0D0F8BBBAF09D796BA369F550D4727E1660A0D3917E
Malicious:	**true**

C:\Users\user\AppData\Roaming\VWIpnm.exe	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F.`.....0.....0... ...@....@.. ..... ..@.....\0..O....@..X.....`..... ....H.....text..... ....`.rsrc...X....@.....@..@.rel oc.....`.....&.....@..B.....0.....H.....X....l.....`.....D.i.w..a.....F.x..*|.....;.j.q.>@..i....4...e.=..:.t...3.....c..fY...".u%..v"...e@V..dW..... .....dUnn.;. %%..-.-...u/5]..@.!....&.....iBu.X8..R"r.Y.....t.3..W.._.w.5.}.....R.c>.U.f.*...[9..G"..B.a..i..&|..#Oq.....W....c.0..I...6?..'..L....!.7Xr.'.....={..(x.3...x.~..2`...`7*.?@.#.}U+.. |.}.7...?i!@bJ.n-.Sl>.....?z..;9...L}...F.....5...\}O./a\.z..b..w....+...j....m..57.

C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe	
Process:	C:\Users\user\Desktop\SPECIALISED SWIFT.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	600064
Entropy (8bit):	7.569327488915576
Encrypted:	false
SSDEEP:	12288:EKl4DoplA0tnkhyMe2sol51Rt4P9b3MPl1mh6uK9T2s8qaK83PC/Oyd7sY:J4DopFnkhyMeQl5OMN1mho9T6Y
MD5:	9059051337F38FF19504E7C53FA8FDF8
SHA1:	77BC68C84DAC387CE4774E3549E2A0701AF44481
SHA-256:	1260C526C6BC88A3C92603AA3826B6581DFD134479CF4054CBC3DE3DF513D4A0
SHA-512:	62C8609083282F2961110D9CD5BFC6CCE45567DA708D62A3835E3188770456AA8C46654F0C7EF0490972D0D0F8BBBAF09D796BA369F550D4727E1660A0D3917E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F.`.....0.....0... ...@....@.. ..... ..@.....\0..O....@..X.....`..... ....H.....text..... ....`.rsrc...X....@.....@..@.rel oc.....`.....&.....@..B.....0.....H.....X....l.....`.....D.i.w..a.....F.x..*|.....;.j.q.>@..i....4...e.=..:.t...3.....c..fY...".u%..v"...e@V..dW..... .....dUnn.;. %%..-.-...u/5]..@.!....&.....iBu.X8..R"r.Y.....t.3..W.._.w.5.}.....R.c>.U.f.*...[9..G"..B.a..i..&|..#Oq.....W....c.0..I...6?..'..L....!.7Xr.'.....={..(x.3...x.~..2`...`7*.?@.#.}U+.. |.}.7...?i!@bJ.n-.Sl>.....?z..;9...L}...F.....5...\}O./a\.z..b..w....+...j....m..57.

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.569327488915576
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SPECIALISED SWIFT.EXE
File size:	600064
MD5:	9059051337f38ff19504e7c53fa8fdf8

General

SHA1:	77bc68c84dac387ce4774e3549e2a0701af44481
SHA256:	1260c526c6bc88a3c92603aa3826b6581dfd134479cf4054cbc3de3df513d4a0
SHA512:	62c8609083282f2961110d9cd5bfc6cce45567da708d62a3835e3188770456aa8c46654f0c7ef0490972d0d0f8bbbaf09d796ba369f550d4727e1660a0d3917e
SSDEEP:	12288:EKl4DoplA0tnkhyMe2sol51Rt4P9b3MPl1mh6uK9T2s8qaK83PC/Oyd7sY:J4DopFnkhyMeQl5OMN1mho9T6Y
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F.`.....0.....0... ...@....@.. .....@.....

File Icon

Icon Hash:	18da1abcb2d2d2b0

Static PE Info

General

Entrypoint:	0x4930ae
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:	0x60C34687 [Fri Jun 11 11:18:31 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x910b4	0x91200	False	0.802339039621	data	7.59382083636	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x94000	0x1058	0x1200	False	0.270182291667	data	2.84656909031	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x96000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SPECIALISED SWIFT.EXE PID: 6044 Parent PID: 5796

General

Start time:	07:56:12
Start date:	12/06/2021
Path:	C:\Users\user\Desktop\SPECIALISED SWIFT.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SPECIALISED SWIFT.EXE'
Imagebase:	0xb40000
File size:	600064 bytes
MD5 hash:	9059051337F38FF19504E7C53FA8FDF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.290470119.0000000003F61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.290470119.0000000003F61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.291001813.00000000040F6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.291001813.00000000040F6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3688 Parent PID: 6044

General

Start time:	07:56:54
Start date:	12/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VWIpnm' /XML 'C:\Users\user\AppData\Local\Temp\tmp551C.tmp'
Imagebase:	0x1090000
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: 3472 Parent PID: 3688

General

Start time:	07:56:54
Start date:	12/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: SPECIALISED SWIFT.EXE PID: 5048 Parent PID: 6044

General

Start time:	07:56:55
Start date:	12/06/2021
Path:	C:\Users\user\Desktop\SPECIALISED SWIFT.EXE
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe20000
File size:	600064 bytes
MD5 hash:	9059051337F38FF19504E7C53FA8FDF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.286401273.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.286401273.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.460242852.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.460242852.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.465914649.00000000033A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.465914649.00000000033A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: pGKuRU.exe PID: 1260 Parent PID: 3388

General

Start time:	07:57:29
Start date:	12/06/2021
Path:	C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe'
Imagebase:	0xd80000
File size:	600064 bytes
MD5 hash:	9059051337F38FF19504E7C53FA8FDF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.443548557.00000000049B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000002.443548557.00000000049B1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 55%, Virustotal, Browse • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: pGKuRU.exe PID: 492 Parent PID: 3388

General

Start time:	07:57:37
Start date:	12/06/2021
Path:	C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe'
Imagebase:	0x5f0000
File size:	600064 bytes
MD5 hash:	9059051337F38FF19504E7C53FA8FDF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.471230731.0000000004491000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.471230731.0000000004491000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: schtasks.exe PID: 5220 Parent PID: 1260

General

Start time:	07:58:05
Start date:	12/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VWIpnm' /XML 'C:\Users\user\AppData\Local\Temp\tmp74D4.tmp'
Imagebase:	0x20000
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: 5256 Parent PID: 5220

General

General

Start time:	07:58:05
Start date:	12/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: pGKuRU.exe PID: 5252 Parent PID: 1260

General

Start time:	07:58:06
Start date:	12/06/2021
Path:	C:\Users\user\AppData\Roaming\pGKuRU\pGKuRU.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x860000
File size:	600064 bytes
MD5 hash:	9059051337F38FF19504E7C53FA8FDF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.460180951.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000002.460180951.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000000.438877169.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000000.438877169.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.466469637.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001F.00000002.466469637.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis