

JoeSandbox Cloud BASIC



ID: 432730

Sample Name: k6DAiaCGR7

Cookbook: default.jbs

Time: 17:51:38

Date: 10/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report k6DAiaCGR7	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Signature Overview	5
AV Detection:	5
System Summary:	5
Boot Survival:	5
Hooking and other Techniques for Hiding and Protection:	5
Malware Analysis System Evasion:	5
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
Contacted IPs	10
General Information	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	12
Static File Info	16
General	16
File Icon	16
Static PE Info	16
General	17
Entrypoint Preview	17
Data Directories	17
Sections	17
Resources	17
Imports	17
Version Infos	17
Network Behavior	17
Code Manipulations	17
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: k6DAiaCGR7.exe PID: 6348 Parent PID: 5892	18
General	18
File Activities	18
File Created	18
File Deleted	18
File Written	18
File Read	18
Analysis Process: powershell.exe PID: 6712 Parent PID: 6348	18
General	18
File Activities	18
File Created	18
File Deleted	18

File Written	18
File Read	19
Analysis Process: conhost.exe PID: 6720 Parent PID: 6712	19
General	19
Analysis Process: powershell.exe PID: 6732 Parent PID: 6348	19
General	19
File Activities	19
File Created	19
File Deleted	19
File Written	19
File Read	19
Analysis Process: conhost.exe PID: 6784 Parent PID: 6732	19
General	19
Analysis Process: schtasks.exe PID: 6816 Parent PID: 6348	20
General	20
Analysis Process: conhost.exe PID: 6836 Parent PID: 6816	20
General	20
Analysis Process: powershell.exe PID: 7052 Parent PID: 6348	20
General	20
Analysis Process: conhost.exe PID: 7064 Parent PID: 7052	21
General	21
Analysis Process: k6DAiaCGR7.exe PID: 7072 Parent PID: 6348	21
General	21
Disassembly	21
Code Analysis	21

Analysis Report k6DAiaCGR7

Overview

General Information

Sample Name:

k6DAiaCGR7 (renamed file extension from none to exe)

Analysis ID:

432730

MD5:

821f46434e52277.

SHA1:

9ada012d5399d2..

SHA256:

6b32b3f608d3e52.

Tags:

exe

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

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

Signatures

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...

Adds a directory exclusion to Windo...

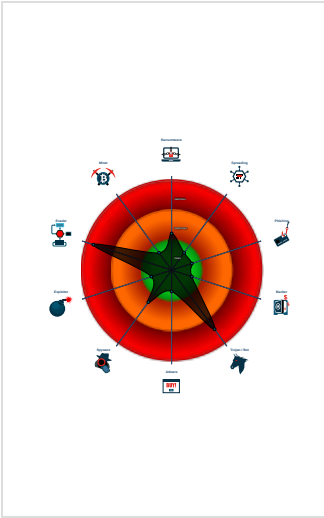
Injects a PE file into a foreign proce...

Moves itself to temp directory

Queries sensitive BIOS Information ...

Queries sensitive network adapter in...

Classification



Process Tree

System is w10x64

k6DAiaCGR7.exe (PID: 6348 cmdline: 'C:\Users\user\Desktop\k6DAiaCGR7.exe' MD5: 821F46434E52277EFB0826338C5DB60C)

powershell.exe (PID: 6712 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\k6DAiaCGR7.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)

conhost.exe (PID: 6720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

powershell.exe (PID: 6732 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\QypERSEhl.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)

conhost.exe (PID: 6784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

schtasks.exe (PID: 6816 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\QypERSEhl' /XML 'C:\Users\user\AppData\Local\Temp\tmpEEC9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)

conhost.exe (PID: 6836 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

powershell.exe (PID: 7052 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\QypERSEhl.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)

conhost.exe (PID: 7064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

k6DAiaCGR7.exe (PID: 7072 cmdline: C:\Users\user\Desktop\k6DAiaCGR7.exe MD5: 821F46434E52277EFB0826338C5DB60C)

cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "raquel.andrade@mercafar.cfdaddyhandsome@1234mail.mercafar.cfstalinperezrn@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.381685171.000000000448 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2021

Page 4 of 22

Source	Rule	Description	Author	Strings
00000001.00000002.381685171.0000000004489000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000D.00000002.597685684.0000000002FE1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.597685684.0000000002FE1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000D.00000000.368609176.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.k6DAiaCGR7.exe.4489930.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.k6DAiaCGR7.exe.4489930.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
13.0.k6DAiaCGR7.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.0.k6DAiaCGR7.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.k6DAiaCGR7.exe.4545748.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

System Summary:



Sigma detected: Non Interactive PowerShell

Signature Overview



Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

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:



Moves itself to temp directory

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

HIPS / PFW / Operating System Protection Evasion:



Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:



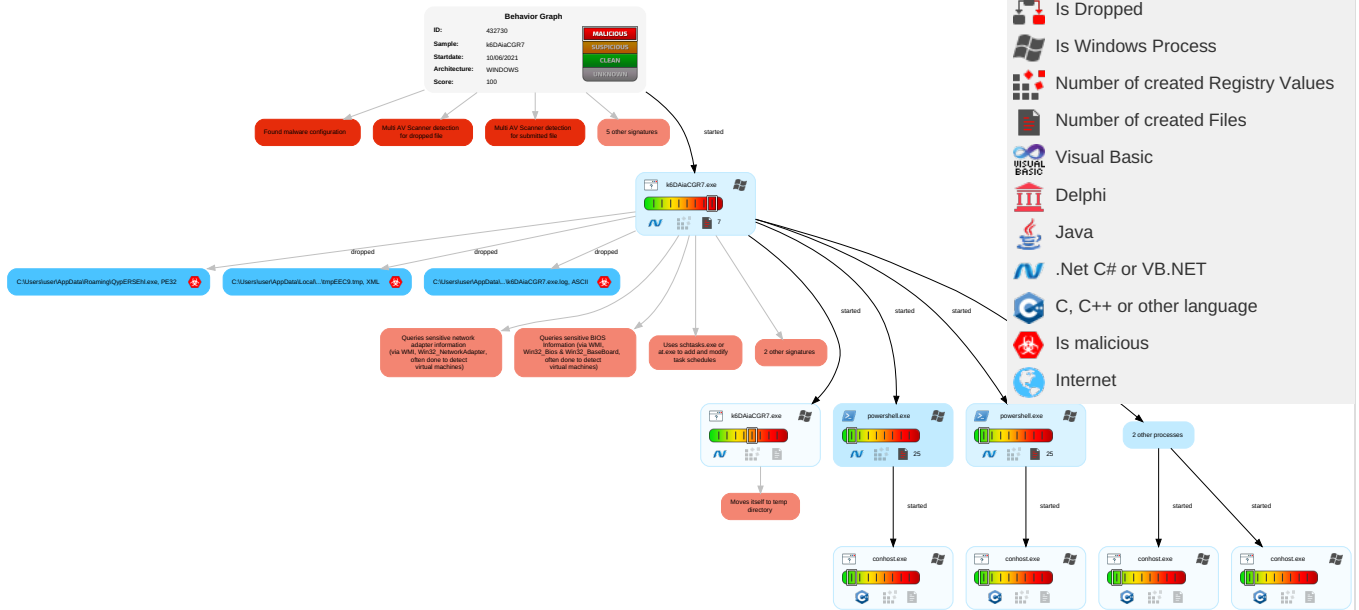
Yara detected AgentTesla

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	Impact
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Confidentiality, Integrity, Availability
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 3 2 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Junk Data	Confidentiality, Integrity, Availability
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Confidentiality, Integrity, Availability
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	Confidentiality, Integrity, Availability
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Confidentiality, Integrity, Availability
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Confidentiality, Integrity, Availability
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Confidentiality, Integrity, Availability

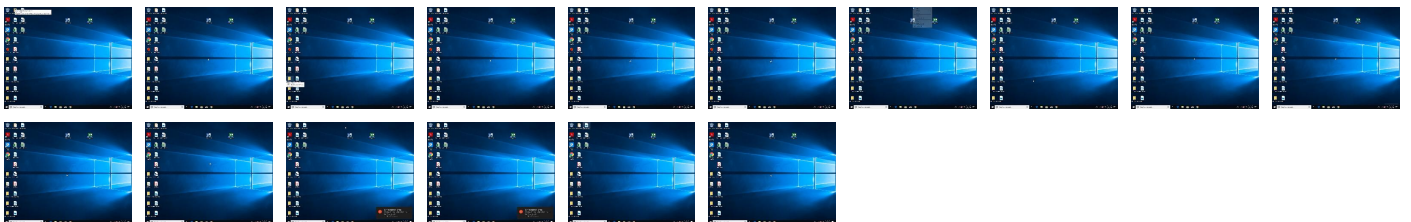
Behavior Graph



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
k6DAiaCGR7.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QypERSEhl.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.k6DAiaCGR7.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.k6DAiaCGR7.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fonts.comnl	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comn-u	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://https://go.micro\$	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.sajatypeworks.combli	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	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.comN	0%	Avira URL Cloud	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/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.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://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.typography.net	0%	URL Reputation	safe	
http://www.typography.netiefi:	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krM	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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	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.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://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	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.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://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://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.typography.netrz	0%	Avira URL Cloud	safe	
http://www.typography.netlique	0%	Avira URL Cloud	safe	
http://www.typography.netK	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comby	0%	Avira URL Cloud	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.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.sajatypeworks.comthe	0%	Avira URL Cloud	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	

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:	432730
Start date:	10.06.2021

Start time:	17:51:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	k6DAiaCGR7 (renamed file extension from none to 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:	30
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@15/18@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 73.3% • Quality standard deviation: 11.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:52:38	API Interceptor	555x Sleep call for process: k6DAiaCGR7.exe modified
17:53:32	API Interceptor	70x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\k6DAiaCGR7.exe.log	
Process:	C:\Users\user\Desktop\k6DAiaCGR7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHkoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEf
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	true
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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.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\1d8480152e0da9a60ad49c6d16a3b6d\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=b77a

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBV0GlpN6KQkj2Wkj4iUxtaKdROdBLNXp5nYoGib4J:cBV3lpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDfB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0A1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....<e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22384
Entropy (8bit):	5.351855916056427
Encrypted:	false
SSDEEP:	384:TptCD7eiwXYpCdTnQvVvgU2HYITBJNMnudTdv7gDq1dO5s5uWC:weHQvdgU2XTz6udaq8z
MD5:	1084A78EB34D6E9844AA66AFC7D4B794
SHA1:	F578B457EDB2294623B67117994E09461A015296
SHA-256:	B58D232EC220EF4E219AC7412ADB151C32219C0D9D9803ADDBA02FC64CD13A46
SHA-512:	7E1E41759F956601CB082560D4A9FB99761AE0EBD24F2FD5DA34AABA05282824CDE9EBA034C022D387F5AF21EC0D9913557A432C259D9C570319DA56A206963
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Preview:	@...e.....x.h.....@.....D.....fZve...F....x.).....System.Management.AutomationH.....<@.^L."My...:P.... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.0...A..4B.....System..4.....Zg5.:O..g..q.....System.Xml..L.....7.....J@.....~..... #.Microsoft.Management.Infrastructure.8.....'...L.}.....System.Numerics.@.....Lo..QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ..H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...\$.1.q.....System.ConfigurationP...../C..J..%..].....%Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;nt.1System.Configuration.Ins
----------	---

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ab1f0fij.1mx.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_iamy1fvf.se3.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pbikxylw.ybh.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pil3vxxv0.fqi.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pil3v xv0.fqi.ps1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_spdfylzy.10z.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ywthqgww.4ra.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpEEC9.tmp		
Process:	C:\Users\user\Desktop\k6DAiaCGR7.exe	
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators	
Category:	dropped	
Size (bytes):	1654	
Entropy (8bit):	5.158167740483007	
Encrypted:	false	
SSDEEP:	24:2dH4+SEqC/S7h2uINMfp2O/rIMhEMjnGpwjplgUYODOLD9RJh7h8gKB3V+Btr:cbha7JINQV/rydbz9I3YODOLNdq3S	
MD5:	E55EA2ED32763BE49E92DEFB1E87038B	
SHA1:	A767CEBBB84FCE628D67A7912CCC8CF4815C3F50	
SHA-256:	F003876576A310255B92533D35C1C6BF09C9BDA25B48E69CE1B071D03F543271	
SHA-512:	AF8338A9E3111F55E2A7F36E74735CE36FE2F70534D7B2BE8968D6073A2DA671D70A7DA2B259C5693CABA338561EA452FC95F625E8F1EBCDC08677B41E414671C	
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>.. <StartWhenAvail	

C:\Users\user\AppData\Roaming\QypERSEhl.exe		 
Process:	C:\Users\user\Desktop\k6DAiaCGR7.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows	
Category:	dropped	
Size (bytes):	758784	

C:\Users\luser\AppData\Roaming\Qyp\ERSEhl.exe	
Entropy (8bit):	7.528067643516331
Encrypted:	false
SSDEEP:	12288:xJGkIMV40J9EQipLYaHb+W6l65UbrZMXBpQm7lrHZ5PSWBZYzGtb/fZpJjWj6w9d:xJGkUdEYq+W265Ub2Em5f55Pl6Uz+bf//
MD5:	821F46434E52277EFB0826338C5DB60C
SHA1:	9ADA012D5399D2B0B18DB722A1AA3ED1B5759D56
SHA-256:	6B32B3F608D3E52A73BBB4AEAC21EEB401B17EDAFC1B902344D897F059D55A52
SHA-512:	371547F802D53355C1B7BD0A1BFDD0984EEFE2B3035B8BB30D23A331ACDE8332C33C857A9EE65B03B6D2C519FD079CE482887B23007C13E672937554907B2FBD
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 48%
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$.....PE..L...s`.....D..N.....Nc.....@.. ..@.....@.....b.S....xK.....H.....text...TC...D.....`.rsrc.xK.....L..F.....@..@.rel oc.....@..B.....Oc.....H.....L.....O.....*(#.....(\$.....(%.....(&.....(*N...(O.....((...*&.())...*.S.....S.....S- s.....s.*Z.....oA.....*&(B.....*j.{.....{.....+.}.....{.....+.}*j.{.....{.....+.}*j.{.....{.....+.} *{.....+.rq.psG.....z.l{.....(+*{.....+.

C:\Users\user\AppData\Roaming\Qyp\ERSEhl.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\k6DAiaCGR7.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:	false
Preview:	[ZoneTransfer].....ZoneId=0

C:\Users\user\Documents\20210610\PowerShell_transcript.878411.FwsK9FvXv.20210610175251.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5815
Entropy (8bit):	5.36876159260061
Encrypted:	false
SSDEEP:	96:BZmTLLNntqDo1Z8Z1TLLNntqDo1Zjp3hjZaTLLNntqDo1ZzVsRRMZn:a
MD5:	105A9F212C0A7FA8A9DFCD8C6C59AD3
SHA1:	4B0C7C30C28F85189633EB13E361987F2E0DFE2A
SHA-256:	76266B25774AE7D1437A96CB65CBE3E859917E13FFD88A4A19615CA9E6FC0B7D
SHA-512:	0158380B8667DC501BB1EFD2AABA266FE915DB29F31D7CE42987E976BE47BAE0BD64222F3B795F68265198A94DD852861AED910FFC7B4860A87FAF4FC4E8F1CB
Malicious:	false
Preview:	<pre> ***** ..Windows PowerShell transcript start..Start time: 20210610175326..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\AppData\Roaming\QypERSEhl.exe..Process ID: 7052..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4 .0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1 0.1..***** ***** ..Command start time: 20210610175327..***** ..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData \Roaming\QypERSEhl.exe..***** ..Windows PowerShell transcript start..Start time: 20210610175954..Username: computer\user..RunAs User: DESKTOP </pre>

C:\Users\user\Documents\20210610\PowerShell_transcript.878411.dtHbzUvE.20210610175247.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5815
Entropy (8bit):	5.3714773262683915
Encrypted:	false
SSDEEP:	96:BZETLLNvqDo1ZoZiRTLLNvqDo1Zgdp3hjZcTLLNvqDo1ZSsRRmjZ4a:sKDia
MD5:	85A5338606A8BB26AFEAF7B236A82F6A
SHA1:	607F29AFB9DAE483AAE1ECD2F5ADCF072B52B9E5
SHA-256:	EFCE4643E9E497B6C2C19EEC7B3DD2D4F3753B33563EAAFE16D9A7D0EBE6BF20
SHA-512:	F7AFE0FC6AFB7D9BE530382CAFAC7E3882787B4668D9288C4343A4F4D8271BD340BEC0D054920E26B97F302C9DFB5C214C4A003CF9275ACAE5E9428F534056
Malicious:	false

C:\Users\user\Documents\20210610\PowerShell_transcript.878411.dtHbzUvE.20210610175247.txt

Preview:	.*****.Windows PowerShell transcript start..Start time: 20210610175315..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QypERSEhl.exe..Process ID: 6732..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..*****.*****.Command start time: 20210610175316..*****.PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QypERSEhl.exe..*****.Windows PowerShell transcript start..Start time: 20210610175537..Username: computer\user..RunAs User: DESKTOP
----------	---

C:\Users\user\Documents\20210610\PowerShell_transcript.878411.m_JoOwci.20210610175242.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5787
Entropy (8bit):	5.375312745510554
Encrypted:	false
SSDEEP:	96:BZqTLLNXqDo1ZfZyTLLNXqDo1ZI6QijZ1TLLNXqDo1Zv/SS+ZJ:i
MD5:	D2D3F88110F31E66AB48A06617831425
SHA1:	4557F5610113879FE3F6AB6F4527C7AC99F2CBB3
SHA-256:	C58D7F14DC09FF75C92C76404127F424285A188081DE503B5D2C471522D654E1
SHA-512:	9978AC1ED20F3153E533ABBFA170A0A207FB66E5340B0EF0D683A89A491A96E5F1A00ACB60E0724D416D818670602BA80EDFFDD6523AB58CE352A715D7FA8D72
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20210610175313..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\k6DAiaCGR7.exe..Process ID: 6712..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..* *****.*****.Command start time: 20210610175313..*****.PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\k6DAiaCGR7.exe..*****.Windows PowerShell transcript start..Start time: 20210610175555..Username: computer\user..RunAs User: computer\engin

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.528067643516331
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.79% - 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% - Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	k6DAiaCGR7.exe
File size:	758784
MD5:	821f46434e52277efb0826338c5db60c
SHA1:	9ada012d5399d2b0b18db722a1aa3ed1b5759d56
SHA256:	6b32b3f608d3e52a73bbb4aeac21eeb401b17edafc1b902344d897f059d55a52
SHA512:	371547f802d53355c1b7bd0a1bfd0984eefe2b3035b8bb30d23a331acde8332c33c857a9ee65b03b6d2c519fd079ce482887b23007c13e672937554907b2fbd7
SSDEEP:	12288:xJGkIMV40J9EQiPLYaHb+W6l65UbrZMXBpQm7lrHZ5PSWBYUzGtb/fZpJjWj6w9d:xJGkUdEYq+W265Ub2Em5r55P6Uz+bf/
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......PE..L....s:.....D...N.....Nc..@..@.....

File Icon

	
Icon Hash:	b6f8c8dccc06110

Static PE Info

General	
Entrypoint:	0x4b634e
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:	0x60C073FA [Wed Jun 9 07:55:38 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	0xb4354	0xb4400	False	0.80430418906	data	7.58451127397	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x4b78	0x4c00	False	0.469366776316	data	4.53439461771	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	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

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: k6DAiaCGR7.exe PID: 6348 Parent PID: 5892

General

Start time:	17:52:29
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\k6DAiaCGR7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\k6DAiaCGR7.exe'
Imagebase:	0xf50000
File size:	758784 bytes
MD5 hash:	821F46434E52277EFB0826338C5DB60C
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: 00000001.00000002.381685171.0000000004489000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.381685171.0000000004489000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.378226984.00000000034C3000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

[Show Windows behavior](#)

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6712 Parent PID: 6348

General

Start time:	17:52:40
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\k6DAiaCGR7.exe'
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

[Show Windows behavior](#)

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6720 Parent PID: 6712

General

Start time:	17:52:40
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6732 Parent PID: 6348

General

Start time:	17:52:40
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\QypERSEhl.exe'
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6784 Parent PID: 6732

General

Start time:	17:52:41
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6816 Parent PID: 6348

General

Start time:	17:52:41
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\lschtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\lschtasks.exe' /Create /TN 'Updates\QypERSEh' /XML 'C:\User s\user\AppData\Local\Temp\tmpEEC9.tmp'
Imagebase:	0x940000
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: 6836 Parent PID: 6816

General

Start time:	17:52:45
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 7052 Parent PID: 6348

General

Start time:	17:52:47
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -Ex clusionPath 'C:\Users\user\AppData\Roaming\QypERSEh.exe'
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 7064 Parent PID: 7052

General

Start time:	17:52:48
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: k6DAiaCGR7.exe PID: 7072 Parent PID: 6348

General

Start time:	17:52:48
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\k6DAiaCGR7.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\k6DAiaCGR7.exe
Imagebase:	0xc80000
File size:	758784 bytes
MD5 hash:	821F46434E52277EFB0826338C5DB60C
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: 0000000D.00000002.597685684.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.597685684.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.368609176.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.368609176.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.593487085.0000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000002.593487085.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis

