ID: 483783
Sample Name: Due Invoices.exe
Cookbook: default.jbs
Time: 13:37:11
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

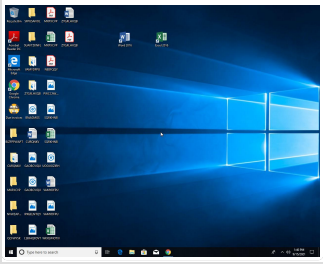
Windows Analysis Report Due Invoices.exe

Overview

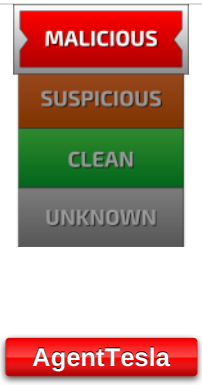
General Information

Sample Name:	Due Invoices.exe
Analysis ID:	483783
MD5:	a6b52f7798a38a5.
SHA1:	ffb626154125d6e..
SHA256:	6bb2aaf5abceeec..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection



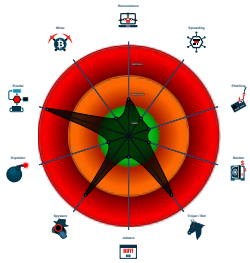
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Hides that the sample has been dow…
- Tries to steal Mail credentials (via fil…
- Queries sensitive network adapter in…
- Uses schtasks.exe or at.exe to add …
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- Due Invoices.exe (PID: 5260 cmdline: 'C:\Users\user\Desktop\Due Invoices.exe' MD5: A6B52F7798A38A5698E46C0A175A29D1)
  - schtasks.exe (PID: 5560 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CrYyKQbnVaYHC' /XML 'C:\Users\user\AppData\Local\Temp\tmpE452.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Due Invoices.exe (PID: 5556 cmdline: C:\Users\user\Desktop\Due Invoices.exe MD5: A6B52F7798A38A5698E46C0A175A29D1)
- bin2.exe (PID: 6256 cmdline: 'C:\Users\user\AppData\Roaming\bin2\bin2.exe' MD5: A6B52F7798A38A5698E46C0A175A29D1)
  - schtasks.exe (PID: 5616 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CrYyKQbnVaYHC' /XML 'C:\Users\user\AppData\Local\Temp\tmp9468.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - bin2.exe (PID: 4624 cmdline: C:\Users\user\AppData\Roaming\bin2\bin2.exe MD5: A6B52F7798A38A5698E46C0A175A29D1)
  - bin2.exe (PID: 6956 cmdline: C:\Users\user\AppData\Roaming\bin2\bin2.exe MD5: A6B52F7798A38A5698E46C0A175A29D1)
- bin2.exe (PID: 7088 cmdline: 'C:\Users\user\AppData\Roaming\bin2\bin2.exe' MD5: A6B52F7798A38A5698E46C0A175A29D1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.704241573.0000000003E19000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.704241573.0000000003E19000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000014.00000002.925882478.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000014.00000002.925882478.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000F.00000002.805743962.00000000041E 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.Due Invoices.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.Due Invoices.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
15.2.bin2.exe.42a0900.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
15.2.bin2.exe.42a0900.4.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Due Invoices.exe.3ed0900.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

System Summary:

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

Copyright Joe Security LLC 2021

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

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

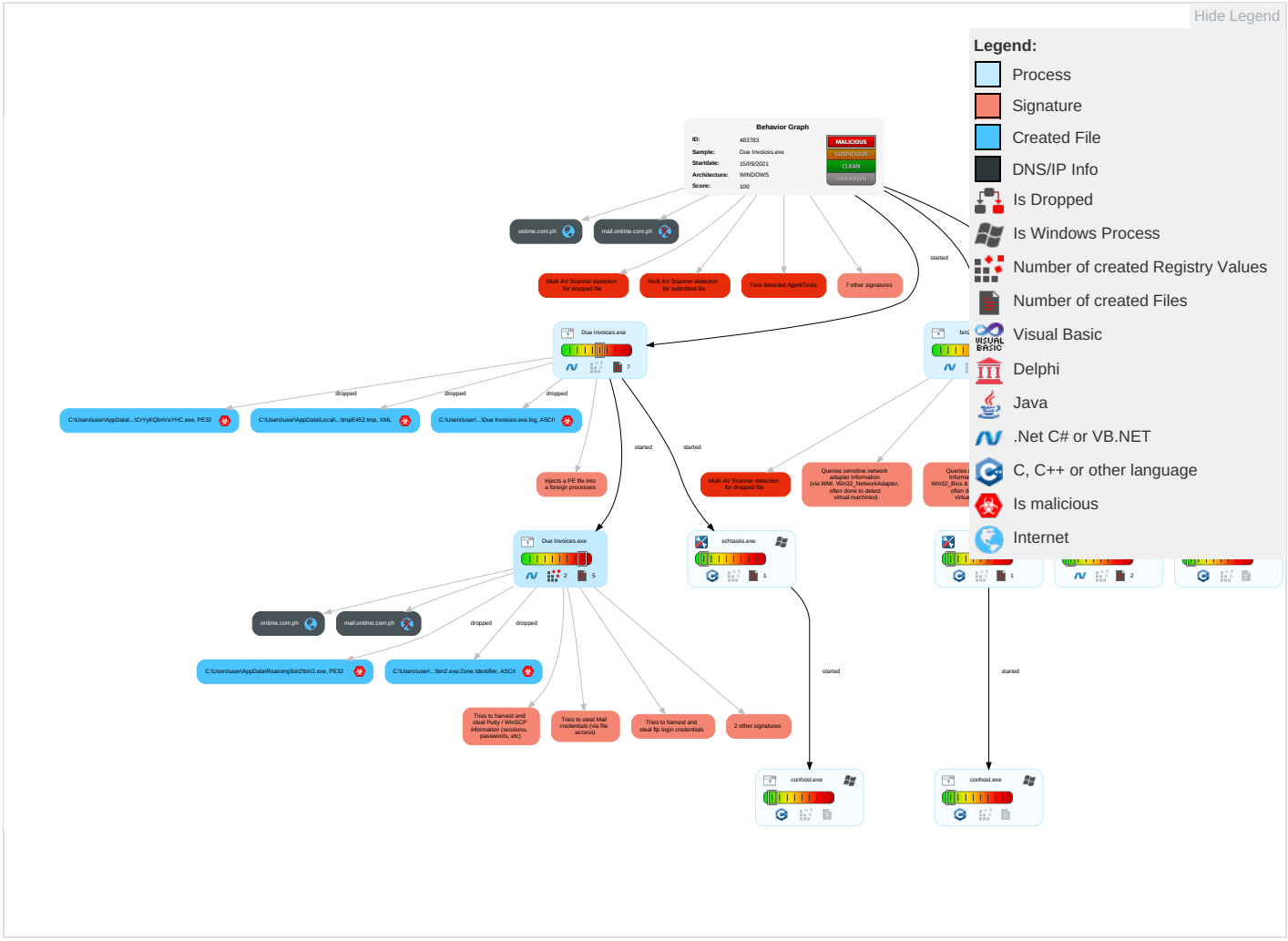
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

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
Due Invoices.exe	27%	Virustotal		Browse
Due Invoices.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\CrYyKQbnVaYHC.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\bin2\bin2.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.Due Invoices.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
20.2.bin2.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2021

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://mail.ontime.com.ph	0%	Avira URL Cloud	safe	
http://www.urwpp.de;S	0%	Avira URL Cloud	safe	
http://www.urwpp.deXS9	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.commicolY	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	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://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.dewa	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://FzDyJtWTr6Up41DQo.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	0%	URL Reputation	safe	
http://www.urwpp.de.rWS0	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.tiro.comslnt	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://ontime.com.ph	0%	Avira URL Cloud	safe	
http://www.tiro.com;S	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.comES	0%	Avira URL Cloud	safe	
http://www.tiro.comNorm	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.ht2	0%	Avira URL Cloud	safe	
http://www.carterandcone.comhU(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ontime.com.ph	23.111.189.130	true	false		high
mail.ontime.com.ph	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483783
Start date:	15.09.2021
Start time:	13:37:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Due Invoices.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:	24
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.spyw.evad.winEXE@15/9@2/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 64.8% • Quality standard deviation: 37.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:38:17	API Interceptor	640x Sleep call for process: Due Invoices.exe modified
13:38:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run bin2 C:\Users\user\AppData\Roaming\bin2\bin2.exe
13:38:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run bin2 C:\Users\user\AppData\Roaming\bin2\bin2.exe
13:39:03	API Interceptor	391x Sleep call for process: bin2.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Due Invoices.exe.log	
Process:	C:\Users\user\Desktop\Due Invoices.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	unknown
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\bin2.exe.log	
Process:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	unknown
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\tmp88FF.tmp	
Process:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646

C:\Users\user\AppData\Local\Temp\tmp88FF.tmp	
Entropy (8bit):	5.193277854469177
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGGtn:cbhK79lNQR/rydbz9I3YODOLNdq3F
MD5:	AABA067EC120D0659B9B19990DB36981
SHA1:	572D98E2DFAEECDFAB55C26EF489A81C19E701A0
SHA-256:	8400A5E7338ABE481A56F0D275A4B82C58764802AB75768DB217A5544A5226B5
SHA-512:	42C273C37778BA2BEC9CDB4AA8EF6F742AD9E4C20482F591A4419617DD763CA0ED8EE9EF4C7B94C8C73FBE63CEDA326B7EF28A9036C867196C2C532BF2180E2
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp9468.tmp	
Process:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.193277854469177
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGGtn:cbhK79lNQR/rydbz9I3YODOLNdq3F
MD5:	AABA067EC120D0659B9B19990DB36981
SHA1:	572D98E2DFAEECDFAB55C26EF489A81C19E701A0
SHA-256:	8400A5E7338ABE481A56F0D275A4B82C58764802AB75768DB217A5544A5226B5
SHA-512:	42C273C37778BA2BEC9CDB4AA8EF6F742AD9E4C20482F591A4419617DD763CA0ED8EE9EF4C7B94C8C73FBE63CEDA326B7EF28A9036C867196C2C532BF2180E2
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpE452.tmp	
Process:	C:\Users\user\Desktop\Due Invoices.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.193277854469177
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGGtn:cbhK79lNQR/rydbz9I3YODOLNdq3F
MD5:	AABA067EC120D0659B9B19990DB36981
SHA1:	572D98E2DFAEECDFAB55C26EF489A81C19E701A0
SHA-256:	8400A5E7338ABE481A56F0D275A4B82C58764802AB75768DB217A5544A5226B5
SHA-512:	42C273C37778BA2BEC9CDB4AA8EF6F742AD9E4C20482F591A4419617DD763CA0ED8EE9EF4C7B94C8C73FBE63CEDA326B7EF28A9036C867196C2C532BF2180E2
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\CrYyKQbnVaYHC.exe	
Process:	C:\Users\user\Desktop\Due Invoices.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	632320
Entropy (8bit):	7.696124068841204

C:\Users\user\AppData\Roaming\CrYyKQbnVaYHC.exe	
Encrypted:	false
SSDEEP:	12288:62l/yzQs2TaIpIY3wyGy4omFaD4Sir7eON/+bwTV45lD:GMIpIVyPmM4Sz2PVuID
MD5:	A6B52F7798A38A5698E46C0A175A29D1
SHA1:	FFB626154125D6E7842069475AF74C87A0472A1E
SHA-256:	6BB2AAF5ABCEEEC0BA17D3A4A857DE168176FF58C688D931D6B4CA71295B3FA7
SHA-512:	D0FCB16022E85C4B735C0FFB32D804608D5A4DB2D5962D47B6366F3DB314FBBD97DD99100F98955708F7430C5AD95A36806718A97F24BC2866BA618C2A06C08
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 18%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Aa.....6...n.....ZT... ...`....@.. ..... .@.....T..W.....dk.....`..... ....H.....text...`4... ...6..... ..`.reloc.....`.....8.....@..B.rsrc ...dk.....l...:.....@..@.....<T.....H.....XW.....H...l..<F.....z.(.....}.....(....o....}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S} .....}....*..}..... ..Q.}.....}....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}....*..}..... "G.R}.....}....*..}.....*...{....*.s....z.2.{.....+...*....0..<..... {.....3..{....(....o....3...}.....+..s.....{....}..

C:\Users\user\AppData\Roaming\CrYyKQbnVaYHC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Due Invoices.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
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\bin2\bin2.exe	
Process:	C:\Users\user\Desktop\Due Invoices.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	632320
Entropy (8bit):	7.696124068841204
Encrypted:	false
SSDEEP:	12288:62l/yzQs2TaIpIY3wyGy4omFaD4Sir7eON/+bwTV45lD:GMIpIVyPmM4Sz2PVuID
MD5:	A6B52F7798A38A5698E46C0A175A29D1
SHA1:	FFB626154125D6E7842069475AF74C87A0472A1E
SHA-256:	6BB2AAF5ABCEEEC0BA17D3A4A857DE168176FF58C688D931D6B4CA71295B3FA7
SHA-512:	D0FCB16022E85C4B735C0FFB32D804608D5A4DB2D5962D47B6366F3DB314FBBD97DD99100F98955708F7430C5AD95A36806718A97F24BC2866BA618C2A06C08
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 18%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Aa.....6...n.....ZT... ...`....@.. ..... .@.....T..W.....dk.....`..... ....H.....text...`4... ...6..... ..`.reloc.....`.....8.....@..B.rsrc ...dk.....l...:.....@..@.....<T.....H.....XW.....H...l..<F.....z.(.....}.....(....o....}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S} .....}....*..}..... ..Q.}.....}....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}....*..}..... "G.R}.....}....*..}.....*...{....*.s....z.2.{.....+...*....0..<..... {.....3..{....(....o....3...}.....+..s.....{....}..

C:\Users\user\AppData\Roaming\bin2\bin2.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Due Invoices.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64

C:\Users\user\AppData\Roaming\bin2\bin2.exe:Zone.Identifier	
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.696124068841204
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Due Invoices.exe
File size:	632320
MD5:	a6b52f7798a38a5698e46c0a175a29d1
SHA1:	ffb626154125d6e7842069475af74c87a0472a1e
SHA256:	6bb2aaf5abceeec0ba17d3a4a857de168176ff58c688d931d6b4ca71295b3fa7
SHA512:	d0fcb16022e85c4b735c0ffb32d804608d5a4db2d5962d47b6366f3db314fbbd97dd99100f98955708f7430c5ad95a36806718a97f24bc2866ba618c2a06c088
SSDEEP:	12288:62l/yzQs2TaIpIY3wyGy4omFaD4Sir7eON/+bwTV45ID:GMIpIVyPmM4Sz2PVuID
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Aa.....6...n.....ZT... ...`....@.. .....@.....

File Icon

Icon Hash:	f1f0f4d0eecccc71

Static PE Info

General

Entrypoint:	0x49545a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6141A2CC [Wed Sep 15 07:37:48 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	0x93460	0x93600	False	0.862807463953	data	7.77383122415	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x96000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x98000	0x6b64	0x6c00	False	0.441767939815	data	5.12984328991	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 13:40:10.011022091 CEST	192.168.2.4	8.8.8.8	0xf8bf	Standard query (0)	mail.ontime.com.ph	A (IP address)	IN (0x0001)
Sep 15, 2021 13:40:10.391025066 CEST	192.168.2.4	8.8.8.8	0xfa88	Standard query (0)	mail.ontime.com.ph	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 13:40:10.161604881 CEST	8.8.8.8	192.168.2.4	0xf8bf	No error (0)	mail.ontime.com.ph	ontime.com.ph		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 13:40:10.161604881 CEST	8.8.8.8	192.168.2.4	0xf8bf	No error (0)	ontime.com.ph		23.111.189.130	A (IP address)	IN (0x0001)
Sep 15, 2021 13:40:10.657954931 CEST	8.8.8.8	192.168.2.4	0xfa88	No error (0)	mail.ontime.com.ph	ontime.com.ph		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 13:40:10.657954931 CEST	8.8.8.8	192.168.2.4	0xfa88	No error (0)	ontime.com.ph		23.111.189.130	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

Copyright Joe Security LLC 2021

System Behavior

Analysis Process: Due Invoices.exe PID: 5260 Parent PID: 6580

General

Start time:	13:38:05
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\Due Invoices.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Due Invoices.exe'
Imagebase:	0xa50000
File size:	632320 bytes
MD5 hash:	A6B52F7798A38A5698E46C0A175A29D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.704241573.0000000003E19000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.704241573.0000000003E19000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.706451004.0000000004040000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.706451004.0000000004040000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.703233657.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5560 Parent PID: 5260

General

Start time:	13:38:24
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CrYyKQbnVaYHC' /XML 'C:\Users\user\AppData\Local\Temp\tmpE452.tmp'
Imagebase:	0x9c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5652 Parent PID: 5560

General

Start time:	13:38:25
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Due Invoices.exe PID: 5556 Parent PID: 5260

General

Start time:	13:38:25
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\Due Invoices.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Due Invoices.exe
Imagebase:	0xd20000
File size:	632320 bytes
MD5 hash:	A6B52F7798A38A5698E46C0A175A29D1
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: 00000007.00000002.929167866.00000000030D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.929167866.00000000030D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.925882279.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.925882279.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Copyright Joe Security LLC 2021

Key Value Created

Analysis Process: bin2.exe PID: 6256 Parent PID: 3424

General

Start time:	13:38:57
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\bin2\bin2.exe'
Imagebase:	0xec0000
File size:	632320 bytes
MD5 hash:	A6B52F7798A38A5698E46C0A175A29D1
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: 0000000E.00000002.799250736.0000000003341000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.803495883.000000000456F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.803495883.000000000456F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.802138840.0000000004349000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.802138840.0000000004349000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 18%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: bin2.exe PID: 7088 Parent PID: 3424

General

Start time:	13:39:05
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\bin2\bin2.exe'
Imagebase:	0xe60000
File size:	632320 bytes
MD5 hash:	A6B52F7798A38A5698E46C0A175A29D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.805743962.00000000041E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.805743962.00000000041E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.804132861.00000000031E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: schtasks.exe PID: 5616 Parent PID: 6256

General

Start time:	13:39:07
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CrYyKQbnVaYHC' /XML 'C:\Users\user\AppData\Local\Temp\tmp9468.tmp'
Imagebase:	0x9c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1688 Parent PID: 5616

General

Start time:	13:39:07
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: bin2.exe PID: 4624 Parent PID: 6256

General

Start time:	13:39:07
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
Imagebase:	0x1e0000
File size:	632320 bytes
MD5 hash:	A6B52F7798A38A5698E46C0A175A29D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: bin2.exe PID: 6956 Parent PID: 6256

General

Start time:	13:39:08
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\bin2\bin2.exe
Imagebase:	0xfc0000
File size:	632320 bytes
MD5 hash:	A6B52F7798A38A5698E46C0A175A29D1
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: 00000014.00000002.925882478.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.925882478.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.929081705.00000000034E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.929081705.00000000034E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021