ID: 458886
Sample Name: Purchase Order-568149.exe
Cookbook: default.jbs
Time: 20:40:28
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

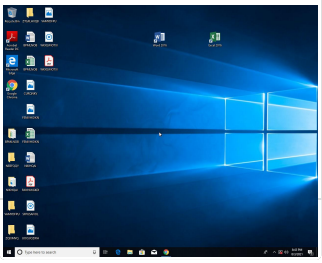
Windows Analysis Report Purchase Order-568149.exe

Overview

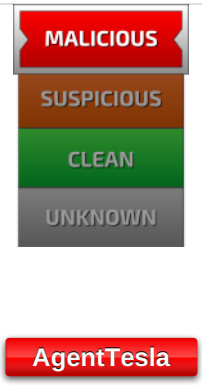
General Information

Sample Name:	Purchase Order-568149.exe
Analysis ID:	458886
MD5:	83f1afd58bf104c…
SHA1:	4d57ea68149da8..
SHA256:	f0a5918de0509be.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

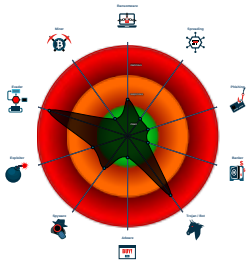


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Purchase Order-568149.exe (PID: 3452 cmdline: 'C:\Users\user\Desktop\Purchase Order-568149.exe' MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
  - schtasks.exe (PID: 2520 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RQqbzWGR' /XML 'C:\Users\user\AppData\Local\Temp\tmp5CCB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase Order-568149.exe (PID: 2796 cmdline: C:\Users\user\Desktop\Purchase Order-568149.exe MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
    - schtasks.exe (PID: 5012 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TxWUEITvoDwYs' /XML 'C:\Users\user\AppData\Local\Temp\tmp8013.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Purchase Order-568149.exe (PID: 3916 cmdline: C:\Users\user\Desktop\Purchase Order-568149.exe MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
    - Purchase Order-568149.exe (PID: 3728 cmdline: C:\Users\user\Desktop\Purchase Order-568149.exe MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
- YYtJku.exe (PID: 5800 cmdline: 'C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe' MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
  - schtasks.exe (PID: 5788 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RQqbzWGR' /XML 'C:\Users\user\AppData\Local\Temp\tmp31EE.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - YYtJku.exe (PID: 4788 cmdline: C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
    - schtasks.exe (PID: 4700 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TxWUEITvoDwYs' /XML 'C:\Users\user\AppData\Local\Temp\tmp51AB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - YYtJku.exe (PID: 4752 cmdline: C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
- YYtJku.exe (PID: 5964 cmdline: 'C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe' MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
  - schtasks.exe (PID: 2944 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RQqbzWGR' /XML 'C:\Users\user\AppData\Local\Temp\tmp5526.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - YYtJku.exe (PID: 3120 cmdline: C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
    - schtasks.exe (PID: 4872 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TxWUEITvoDwYs' /XML 'C:\Users\user\AppData\Local\Temp\tmp75EC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - YYtJku.exe (PID: 5864 cmdline: C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe MD5: 83F1AFD58BF104CB33FACC556D7BAE89)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000026.00000002.598185480.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000026.00000002.598185480.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000019.00000002.509309042.000000000318000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000007.00000002.390113039.0000000003B49000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.390113039.0000000003B49000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.Purchase Order-568149.exe.4097118.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.Purchase Order-568149.exe.4097118.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.2.Purchase Order-568149.exe.4097118.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.Purchase Order-568149.exe.4097118.4.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
11.2.Purchase Order-568149.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

Initial sample is a PE file and has a suspicious name

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)

Moves itself to temp directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

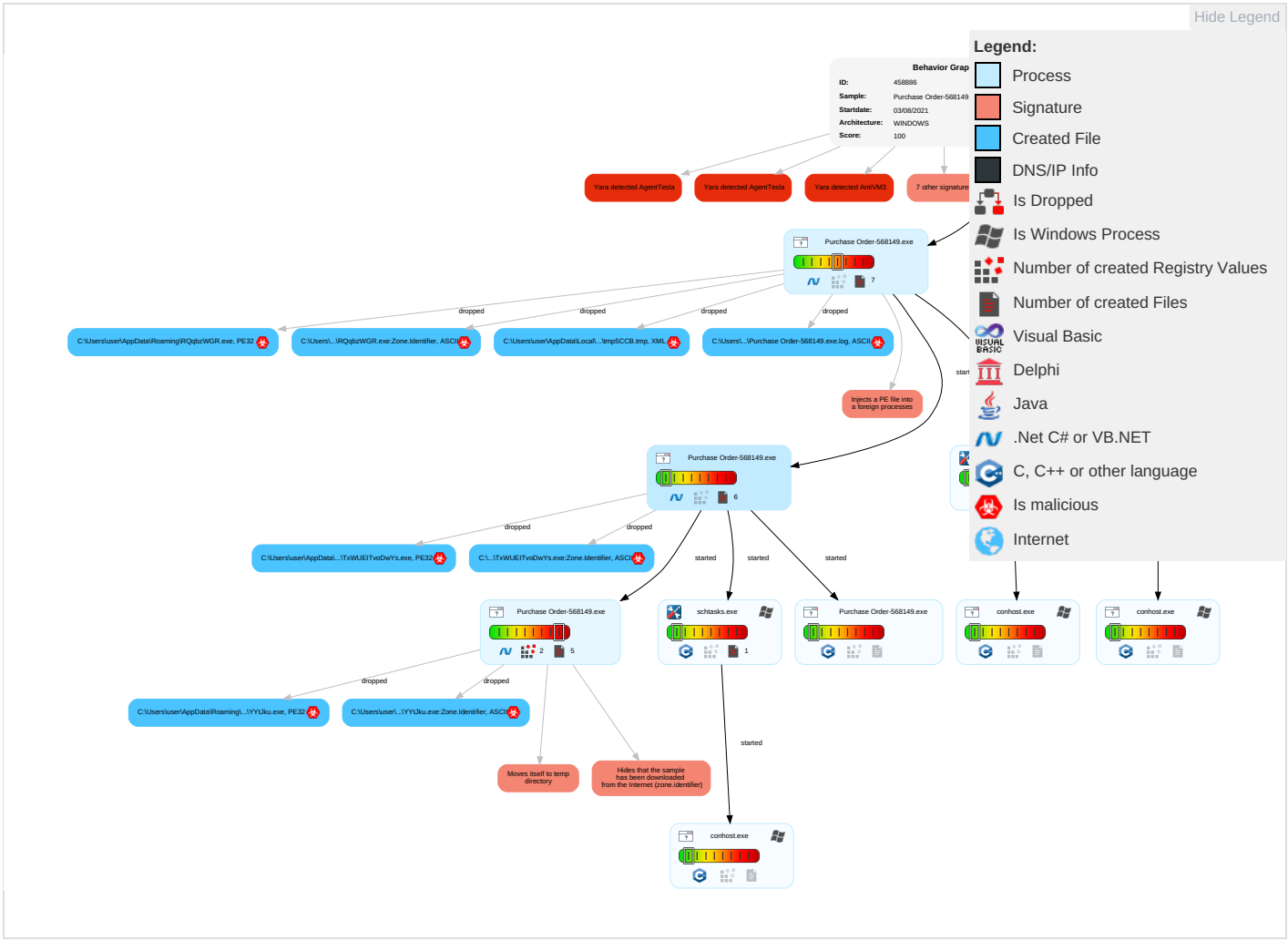
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

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

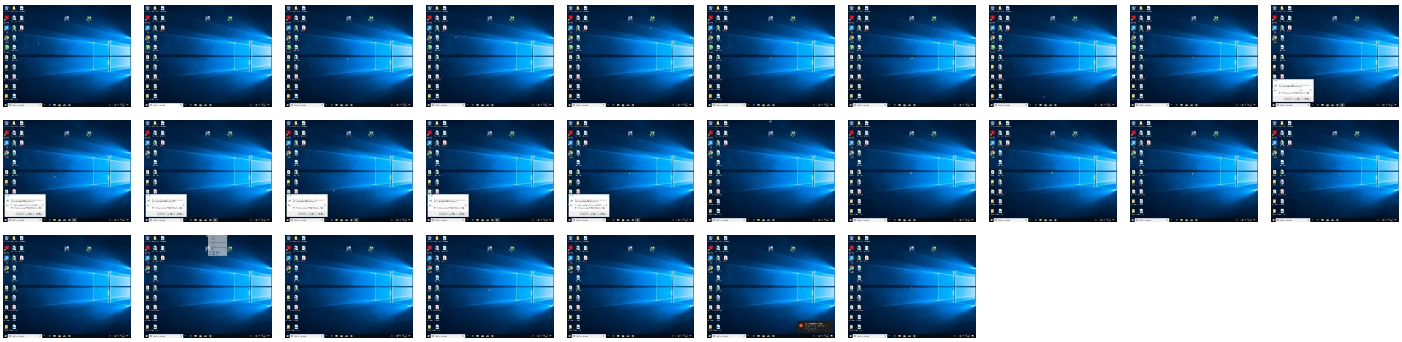
Behavior Graph



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
Purchase Order-568149.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RQqbzWGR.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\TxWUEITvoDwYs.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.Purchase Order-568149.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.tiro.com:	0%	Virustotal		Browse
http://www.tiro.com:	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnarkp9	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnC	0%	Avira URL Cloud	safe	
http://www.urwpp.deld	0%	Avira URL Cloud	safe	
http://www.tiro.coms89k3	0%	Avira URL Cloud	safe	
http://www.carterandcone.com-s(9	0%	Avira URL Cloud	safe	
http://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.founder.com.cn/cna-d	0%	URL Reputation	safe	
http://www.sandoll.co.krn-un(	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comceta	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com(	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-g	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/ef1H	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/a	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://flUPyp.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.carterandcone.comuct	0%	Avira URL Cloud	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.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.carterandcone.comncyI)	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	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://www.carterandcone.comX	0%	URL Reputation	safe	
http://www.tiro.comb3	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueto	0%	Avira URL Cloud	safe	
http://www.carterandcone.comg	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/cnl9	0%	Avira URL Cloud	safe	
http://www.carterandcone.comint	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.sakkal.com(	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krn-usur-(	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comau	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnadeB8	0%	Avira URL Cloud	safe	
http://www.carterandcone.comkf	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.com-g	0%	Avira URL Cloud	safe	
http://www.carterandcone.comopsz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458886
Start date:	03.08.2021
Start time:	20:40:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order-568149.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:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@31/11@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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
20:41:29	API Interceptor	578x Sleep call for process: Purchase Order-568149.exe modified
20:42:09	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run YYtJku C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
20:42:17	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run YYtJku C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
20:42:22	API Interceptor	133x Sleep call for process: YYtJku.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\Purchase Order-568149.exe.log	
Process:	C:\Users\user\Desktop\Purchase Order-568149.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\YYtJku.exe.log	
Process:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\YYtJku.exe.log	
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\tmp31EE.tmp	
Process:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1653
Entropy (8bit):	5.167460387336423
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Fbtn:cbha7JlNQV/rydbz9I3YODOLNdq3n5
MD5:	0F0234C5E88A75551290F5AE18781C63
SHA1:	95BCC8204FBBB833D17A76D18F5966A1BDBD0B49
SHA-256:	5444BB2D5C248215AD57A7519EA1CD1726B2809A3BFC6C4394833834l6EC0B9A
SHA-512:	B6BB6CF7DA41783FC9FC96AF57D846403EE4A4AB4CB4B2ACD1FD75E81CC008988B3C1D3A2B29A57ABF3EA38488AF4A47CC6C70DFD12A0F8B9F69BB029A447 E33
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>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp5526.tmp	
Process:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Fbtn:cbha7JlNQV/rydbz9I3YODOLNdq3n5
MD5:	0F0234C5E88A75551290F5AE18781C63
SHA1:	95BCC8204FBBB833D17A76D18F5966A1BDBD0B49
SHA-256:	5444BB2D5C248215AD57A7519EA1CD1726B2809A3BFC6C4394833834l6EC0B9A
SHA-512:	B6BB6CF7DA41783FC9FC96AF57D846403EE4A4AB4CB4B2ACD1FD75E81CC008988B3C1D3A2B29A57ABF3EA38488AF4A47CC6C70DFD12A0F8B9F69BB029A447 E33
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>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp5CCB.tmp	
Process:	C:\Users\user\Desktop\Purchase Order-568149.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1653

C:\Users\user\AppData\Local\Temp\tmp5CCB.tmp	
Entropy (8bit):	5.167460387336423
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Fbtn:cbha7JlNQV/rydbz9I3YODOLNdq3n5
MD5:	0F0234C5E88A75551290F5AE18781C63
SHA1:	95BCC8204FBBB833D17A76D18F5966A1BDBD0B49
SHA-256:	5444BB2D5C248215AD57A7519EA1CD1726B2809A3BFC6C439483383416EC0B9A
SHA-512:	B6BB6CF7DA41783FC9FC96AF57D846403EE4A4AB4CB4B2ACD1FD75E81CC008988B3C1D3A2B29A57ABF3EA38488AF4A47CC6C70DFD12A0F8B9F69BB029A447E33
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>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp8013.tmp	
Process:	C:\Users\user\Desktop\Purchase Order-568149.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1658
Entropy (8bit):	5.162387295213227
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Jtn:cbha7JlNQV/rydbz9I3YODOLNdq3Z
MD5:	C273A4C55231177FD5797CC6408B118D
SHA1:	E2150489D6EA72A4F8C5EC4BAA4A74B9AA26511F
SHA-256:	AA5C261A8B2AF9FAF44C0687688AE84534BC157B116A2AC52D46A51108A29D21
SHA-512:	D42A6703F685714EA6D057AAC239A82A45B9FB185AAC5B424F063149F5599FFA89DFB4AE72C0725B0175A9AD6D0E6E8A0FEA78391418CF222DE887B8E10EDF24
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>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\RQqbzWGR.exe	
Process:	C:\Users\user\Desktop\Purchase Order-568149.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1958400
Entropy (8bit):	7.426284873219883
Encrypted:	false
SSDEEP:	49152:kMJyo1U3GlbQA1obnz3Mc7Dcd/k7AK1j:l9qSov3Mc7DX
MD5:	83F1AFD58BF104CB33FACC556D7BAE89
SHA1:	4D57EA68149DA873D3DA6DE49241D1CD33F1B3F3
SHA-256:	F0A5918DE0509BE93FFA64BE5E74942989FA8ACD94B34B6659F479D22ABAB0CA
SHA-512:	54DC3D6AAE0401EBE1DEE9F98FAA653127D93F5C0BFE2C86C68D4F97E468F344FDBE92F2BB0040A74CF486D1476AACE27974DA3C37507A85CA7F00DA76C187E0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....\|.a.....P..... ... .@.. .....@.....@..X...O.... ....H.....text..... .....`.rsrc..... .....@..@.reloc..... .....@..B.....H.....L....8.....M...X..../.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*"....*.0..&.....(....r%..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

C:\Users\user\AppData\Roaming\RQqbzWGR.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase Order-568149.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

C:\Users\user\AppData\Roaming\RQqbzWGR.exe:Zone.Identifier	
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\TxWUElTvoDwYs.exe	
Process:	C:\Users\user\Desktop\Purchase Order-568149.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1958400
Entropy (8bit):	7.426284873219883
Encrypted:	false
SSDEEP:	49152:kMJyo1U3GlbQA1obnz3Mc7Dcd/k7AK1j:l9qSov3Mc7DX
MD5:	83F1AFD58BF104CB33FACC556D7BAE89
SHA1:	4D57EA68149DA873D3DA6DE49241D1CD33F1B3F3
SHA-256:	F0A5918DE0509BE93FFA64BE5E74942989FA8ACD94B34B6659F479D22ABAB0CA
SHA-512:	54DC3D6AAE0401EBE1DEE9F98FAA653127D93F5C0BFE2C86C68D4F97E468F344FDBE92F2BB0040A74CF486D1476AACE27974DA3C37507A85CA7F00DA76C187E0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....\|.a.....P..... ... .@.. .....@..... ..@.....X...O.... ....H.....text..... ....`.rsrc..... .....@..@.reloc..... .....@..B.....H.....L....8.....M...X.../.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,lr...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r%..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

C:\Users\user\AppData\Roaming\TxWUElTvoDwYs.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase Order-568149.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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	
Process:	C:\Users\user\Desktop\Purchase Order-568149.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1958400
Entropy (8bit):	7.426284873219883
Encrypted:	false
SSDEEP:	49152:kMJyo1U3GlbQA1obnz3Mc7Dcd/k7AK1j:l9qSov3Mc7DX
MD5:	83F1AFD58BF104CB33FACC556D7BAE89
SHA1:	4D57EA68149DA873D3DA6DE49241D1CD33F1B3F3
SHA-256:	F0A5918DE0509BE93FFA64BE5E74942989FA8ACD94B34B6659F479D22ABAB0CA
SHA-512:	54DC3D6AAE0401EBE1DEE9F98FAA653127D93F5C0BFE2C86C68D4F97E468F344FDBE92F2BB0040A74CF486D1476AACE27974DA3C37507A85CA7F00DA76C187E0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....\|.a.....P..... ... .@.. .....@..... ..@.....X...O.... ....H.....text..... ....`.rsrc..... .....@..@.reloc..... .....@..B.....H.....L....8.....M...X.../.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~.... o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r%..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase Order-568149.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
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):	7.426284873219883
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:	Purchase Order-568149.exe
File size:	1958400
MD5:	83f1afd58bf104cb33facc556d7bae89
SHA1:	4d57ea68149da873d3da6de49241d1cd33f1b3f3
SHA256:	f0a5918de0509be93ffa64be5e74942989fa8acd94b34b6659f479d22abab0ca
SHA512:	54dc3d6aae0401ebe1dee9f98faa653127d93f5c0bfe2c86c68d4f97e468f344fdbe92f2bb0040a74cf486d1476aace27974da3c37507a85ca7f00da76c187e0
SSDEEP:	49152:kMJyo1U3GlbQA1obnz3Mc7Dcd/k7AK1j:l9qSov3Mc7DX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....|.a.....P..... ... .@.. .....@..... ..@.....

File Icon

Icon Hash:	f0c2a07179b396e8

Static PE Info

General

Entrypoint:	0x5a0aaa
Entrypoint Section:	.text

General

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:	0x61097C8D [Tue Aug 3 17:27:41 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	0x19eab0	0x19ec00	False	0.747485896059	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.43251327113	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1a2000	0x3f098	0x3f200	False	0.744009127475	data	7.06543166408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1e2000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase Order-568149.exe PID: 3452 Parent PID: 5732

General

Start time:	20:41:18
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Order-568149.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order-568149.exe'
Imagebase:	0xca0000
File size:	1958400 bytes
MD5 hash:	83F1AFD58BF104CB33FACC556D7BAE89
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: 00000000.00000002.368950363.0000000003568000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2520 Parent PID: 3452

General

Start time:	20:41:31
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RQqbzWGR' /XML 'C:\Users\user\AppData\Local\Temp\tmp5CCB.tmp'
Imagebase:	0xa50000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5668 Parent PID: 2520

General

Start time:	20:41:32
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Purchase Order-568149.exe PID: 2796 Parent PID: 3452

General

Start time:	20:41:33
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Order-568149.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order-568149.exe
Imagebase:	0x650000
File size:	1958400 bytes
MD5 hash:	83F1AFD58BF104CB33FACC556D7BAE89
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: 00000007.00000002.390113039.0000000003B49000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.390113039.0000000003B49000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000007.00000002.389374922.0000000002CCB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5012 Parent PID: 2796

General

Start time:	20:41:41
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\TxWUEITvoDwYs' /XML 'C:\Users\user\AppData\Local\Temp\tmp8013.tmp'
Imagebase:	0xa50000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5824 Parent PID: 5012

General

Start time:	20:41:42
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Purchase Order-568149.exe PID: 3916 Parent PID: 2796

General

Start time:	20:41:43
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Order-568149.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Purchase Order-568149.exe
Imagebase:	0x3a0000
File size:	1958400 bytes
MD5 hash:	83F1AFD58BF104CB33FACC556D7BAE89
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Purchase Order-568149.exe PID: 3728 Parent PID: 2796

General

Start time:	20:41:44
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Purchase Order-568149.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order-568149.exe
Imagebase:	0x790000
File size:	1958400 bytes
MD5 hash:	83F1AFD58BF104CB33FACC556D7BAE89
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: 0000000B.00000002.596505185.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.596505185.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.604354638.0000000002D81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.604354638.0000000002D81000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: YYtJku.exe PID: 5800 Parent PID: 3440

General

Start time:	20:42:18
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe'
Imagebase:	0xf70000
File size:	1958400 bytes
MD5 hash:	83F1AFD58BF104CB33FACC556D7BAE89
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: 00000014.00000002.485090142.00000000039F8000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5788 Parent PID: 5800

General

Start time:	20:42:25
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RQqbzWGR' /XML 'C:\Users\user\AppData\Local\Temp\tmp31EE.tmp'
Imagebase:	0xa50000
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: 1676 Parent PID: 5788

General

Start time:	20:42:25
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: YYtJku.exe PID: 5964 Parent PID: 3440

General

Start time:	20:42:26
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\YYtJku\YYtJku.exe'
Imagebase:	0x990000
File size:	1958400 bytes
MD5 hash:	83F1AFD58BF104CB33FACC556D7BAE89
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: 00000019.00000002.509309042.0000000003188000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis