

JOeSandbox Cloud BASIC



ID: 755961

Sample Name: PURCHASE
ORDER.exe

Cookbook: default.jbs

Time: 11:23:06

Date: 29/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report PURCHASE ORDER.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Persistence and Installation Behavior	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
System Summary	6
Boot Survival	6
Hooking and other Techniques for Hiding and Protection	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	10
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	12
Public IPs	12
General Information	13
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	14
Domains	14
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAyWOGorT.exe.log	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PURCHASE ORDER.exe.log	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yGbzOMp.exe.log	15
C:\Users\user\AppData\Local\Temp\tmp6AED.tmp	15
C:\Users\user\AppData\Local\Temp\tmpF89B.tmp	15
C:\Users\user\AppData\Roaming\PAyWOGorT.exe	16
C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe	16
\Device\ConDrv	16
Static File Info	17
General	17
File Icon	17
Static PE Info	17
General	17
Entrypoint Preview	17
Data Directories	19
Sections	19
Resources	20
Imports	20
Network Behavior	20
Network Port Distribution	20
TCP Packets	20

UDP Packets	22
DNS Queries	22
DNS Answers	22
SMTP Packets	22
Statistics	23
Behavior	23
System Behavior	23
Analysis Process: PURCHASE ORDER.exePID: 5196, Parent PID: 3528	23
General	23
File Activities	23
File Created	23
File Deleted	24
File Written	24
File Read	25
Analysis Process: schtasks.exePID: 1948, Parent PID: 5196	26
General	26
File Activities	26
File Read	26
Analysis Process: conhost.exePID: 2040, Parent PID: 1948	26
General	26
Analysis Process: RegSvc.exePID: 4212, Parent PID: 5196	26
General	26
File Activities	27
File Created	27
File Written	27
File Read	28
Registry Activities	29
Key Value Created	29
Analysis Process: PAgWOGORT.exePID: 1520, Parent PID: 1088	29
General	29
File Activities	29
File Created	29
File Deleted	29
File Written	29
File Read	30
Analysis Process: yGbzOMP.exePID: 1604, Parent PID: 3528	31
General	31
File Activities	31
File Created	31
File Written	31
File Read	32
Analysis Process: conhost.exePID: 5188, Parent PID: 1604	32
General	32
Analysis Process: yGbzOMP.exePID: 4184, Parent PID: 3528	33
General	33
File Activities	33
File Written	33
File Read	34
Analysis Process: conhost.exePID: 3720, Parent PID: 4184	34
General	34
Analysis Process: schtasks.exePID: 1240, Parent PID: 1520	34
General	34
File Activities	35
File Read	35
Analysis Process: conhost.exePID: 6096, Parent PID: 1240	35
General	35
Analysis Process: RegSvc.exePID: 5292, Parent PID: 1520	35
General	35
Analysis Process: RegSvc.exePID: 3836, Parent PID: 1520	35
General	35
File Activities	36
File Created	36
File Deleted	36
File Written	36
File Read	37
Disassembly	38

Windows Analysis Report

PURCHASE ORDER.exe

Overview

General Information

Sample Name:

PURCHASE ORDER.exe

Analysis ID:

755961

MD5:

a55b4bb0939865.

SHA1:

975f7c38780d00..

SHA256:

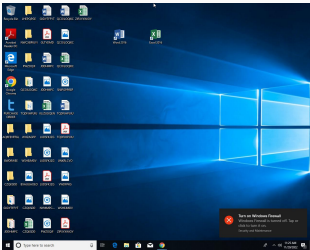
ea45a2032eebe6.

Tags:

agentteslaexe

Infos:

YARA SIGNATURE



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Malicious sample detected (through...

Yara detected AgentTesla

Yara detected AntiVM3

Sigma detected: Scheduled temp fil...

Multi AV Scanner detection for drop...

Tries to steal Mail credentials (via fi...

Initial sample is a PE file and has a...

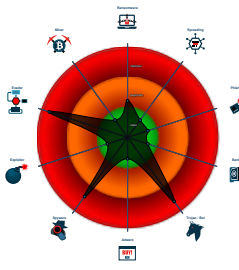
Writes to foreign memory regions

Tries to harvest and steal Putty / W...

Tries to harvest and steal ftp login c...

Tries to detect sandboxes and other...

Classification



Process Tree

System is w10x64

PURCHASE ORDER.exe

(PID: 5196 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: A55B4BB09398659D69F1B8B37541E621)

schtasks.exe

(PID: 1948 cmdline: C:\Windows\System32\schtasks.exe /Create /TN "Updates\PAyWOGorT" /XML "C:\Users\user\AppData\Local\Temp\tmpF89B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)

conhost.exe

(PID: 2040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

RegSvcs.exe

(PID: 4212 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)

PAyWOGorT.exe

(PID: 1520 cmdline: C:\Users\user\AppData\Roaming\PAyWOGorT.exe MD5: A55B4BB09398659D69F1B8B37541E621)

schtasks.exe

(PID: 1240 cmdline: C:\Windows\System32\schtasks.exe /Create /TN "Updates\PAyWOGorT" /XML "C:\Users\user\AppData\Local\Temp\tmp6AED.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)

conhost.exe

(PID: 6096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

RegSvcs.exe

(PID: 5292 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)

RegSvcs.exe

(PID: 3836 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)

yGbzMp.exe

(PID: 1604 cmdline: "C:\Users\user\AppData\Roaming\yGbzMp\yGbzMp.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)

conhost.exe

(PID: 5188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

yGbzMp.exe

(PID: 4184 cmdline: "C:\Users\user\AppData\Roaming\yGbzMp\yGbzMp.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)

conhost.exe

(PID: 3720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

cleanup

Malware Configuration

Threatname: Agenttesla

{

"Exfil Mode": "SMTP",

"Host": "mail.rogenicgroup-bd.com",

"Username": "amir.hossain@rogenicgroup-bd.com",

"Password": "Hossain\$3400"

}

Copyright Joe Security LLC 2022

Page 4 of 38

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.337559814.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.337559814.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000000.337559814.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x31d44:\$a13: get_DnsResolver 0x3043b:\$a20: get_LastAccessed 0x32772:\$a27: set_InternalServerPort 0x32aa7:\$a30: set_GuidMasterKey 0x3054d:\$a33: get_Clipboard 0x3055b:\$a34: get_Keyboard 0x31928:\$a35: get_ShiftKeyDown 0x31939:\$a36: get_AltKeyDown 0x30568:\$a37: get_Password 0x31083:\$a38: get_PasswordHash 0x321a6:\$a39: get_DefaultCredentials
00000000.00000002.341336847.0000000003297000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.412448960.00000000028F1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 15 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PURCHASE ORDER.exe.43a0ee0.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PURCHASE ORDER.exe.43a0ee0.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x34a83:\$s10: logins 0x344fd:\$s11: credential 0x3074d:\$g1: get_Clipboard 0x3075b:\$g2: get_Keyboard 0x30768:\$g3: get_Password 0x31b18:\$g4: get_CtrlKeyDown 0x31b28:\$g5: get_ShiftKeyDown 0x31b39:\$g6: get_AltKeyDown

Click to see the 7 entries

Sigma Signatures

Persistence and Installation Behavior



Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file
Multi AV Scanner detection for dropped file
Machine Learning detection for sample
Machine Learning detection for dropped file

System Summary



Malicious sample detected (through community Yara rule)
Initial sample is a PE file and has a suspicious name
.NET source code contains very large array initializations

Boot Survival



Uses schtasks.exe or at.exe to add and modify task schedules
--

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion



Yara detected AntiVM3
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



Writes to foreign memory regions
Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected AgentTesla
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Tries to harvest and steal ftp login credentials
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

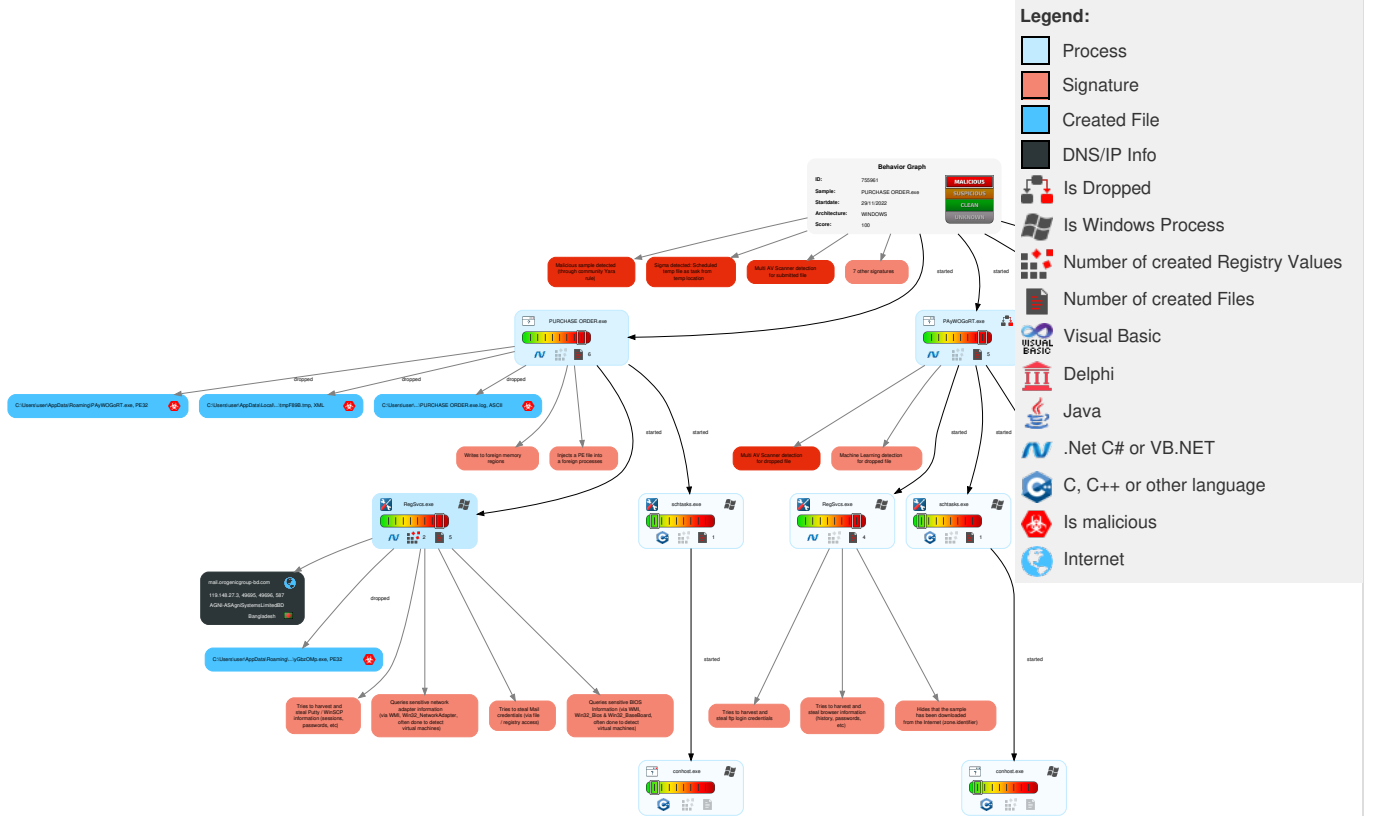


Yara detected AgentTesla

Mitre Att&ck Matrix													
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	2 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	Security Account Manager	1 1 4 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

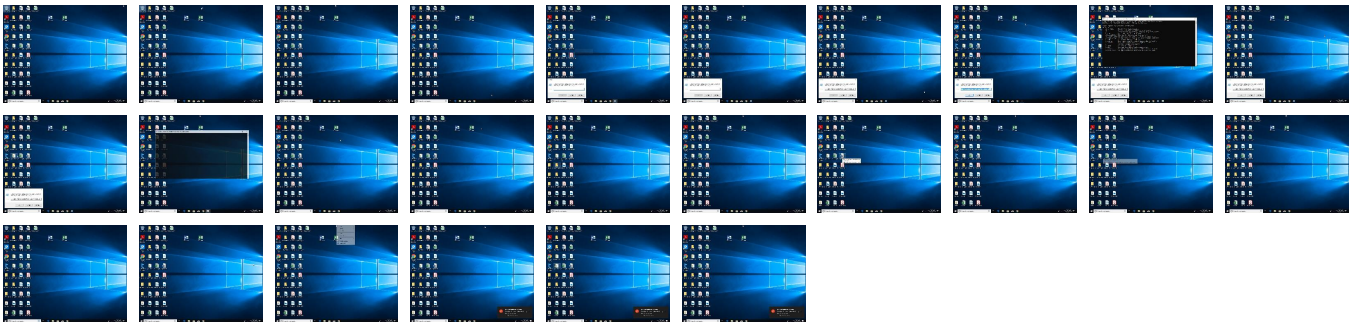
Behavior Graph



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.exe	61%	ReversingLabs	ByteCode-MSIL.Trojan.Tasku n	
PURCHASE ORDER.exe	48%	Virustotal		Browse
PURCHASE ORDER.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\PAyWOGORT.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\PAyWOGORT.exe	61%	ReversingLabs	ByteCode-MSIL.Trojan.Tasku n	
C:\Users\user\AppData\Roaming\yGbzOMPlyGbzOMP.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.RegSvc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	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/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://0boQaB1sN6dM.org	0%	Avira URL Cloud	safe	
http://mail.rogenicgroup-bd.com	0%	Avira URL Cloud	safe	
http://JXqRNJ.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.rogenicgroup-bd.com	119.148.27.3	true	false		unknown

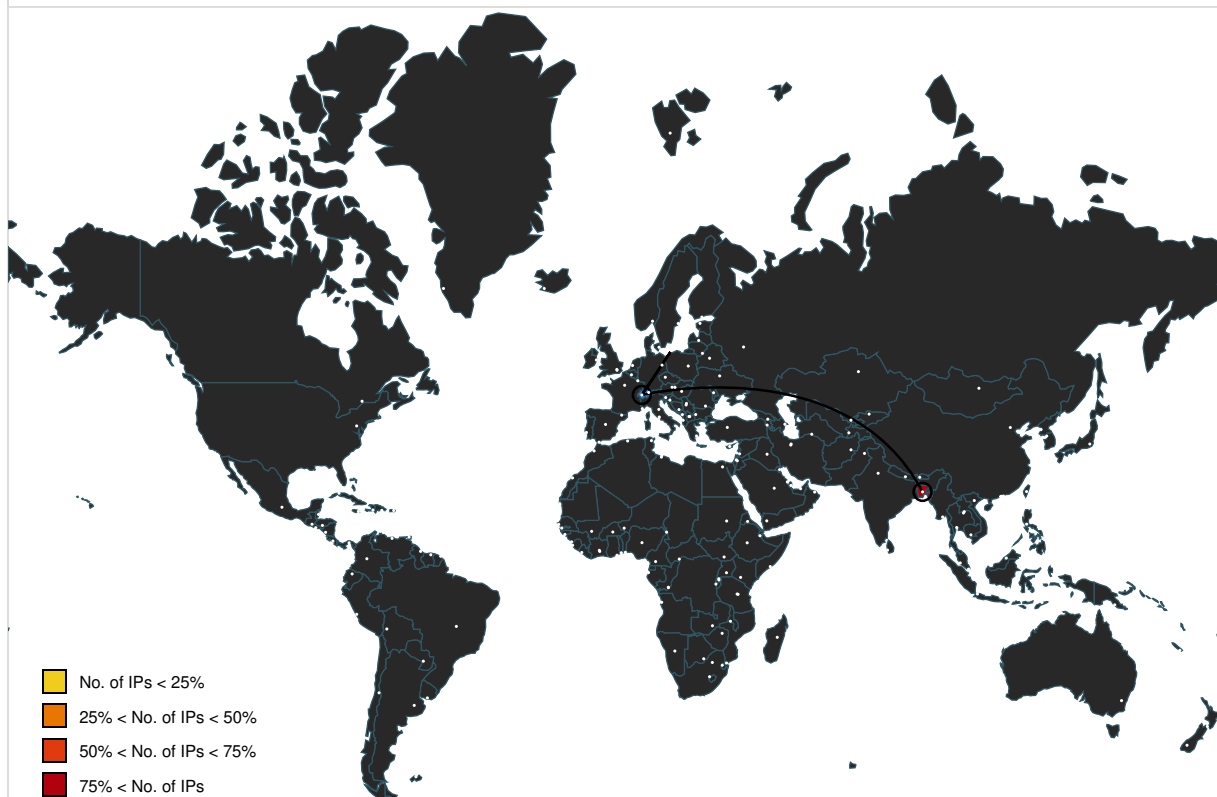
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvc.exe, 00000003.00000002.412448960.00000000028F1000.00000004.00000800.00020000.00000000.sdmp, RegSvc.exe, 0000000C.00000002.570378772.0000000002A5C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sectigo.com/CPS0	RegSvcs.exe, 00000003.00000002.417544241.0000000002C7D000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000003.00000002.422933643.0000000005D81000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000003.00000002.422762374.0000000005D62000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000C.00000002.577522128.0000000006045000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://mail.rogenicgroup-bd.com	RegSvcs.exe, 00000003.00000002.417544241.0000000002C7D000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000C.00000002.574204192.0000000002E19000.00000004.00000800.00020000.00000000.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.ziphttps://www	RegSvcs.exe, 00000003.00000002.412448960.00000000028F1000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000C.00000002.570378772.0000000002A5C000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.tiro.com	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.carterandcone.coml	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.sajatypeworks.com	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.typography.netD	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://fontfabrik.com	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	RegSvcs.exe, 0000000C.00000002.570378772.0000000002A5C000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://JXqRNJ.com	RegSvcs.exe, 0000000C.00000002.570378772.0000000002A5C000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PURCHASE ORDER.exe, 00000000.00000002.341153865.0000000003251000.00000004.00000800.00020000.00000000.sdmp, PAgWOGorT.exe, 00000004.00000002.405112701.0000000003001000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	PURCHASE ORDER.exe, 00000000.00000002.346776635.0000000007212000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://0boQaB1sN6dM.org	RegSvc.exe, 0000000C.00000002.570378772.000000002A5C000.00000004.00000800.00020000.00000000.sdmp, RegSvc.exe, 0000000C.00000002.574175039.0000000002E13000.00000004.00000800.00020000.00000000.sdmp, RegSvc.exe, 0000000C.00000002.574144305.0000000002E0F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.148.27.3	mail.rogenicgroup-bd.com	Bangladesh		23923	AGNI-ASAgniSystemsLimitedBD	false

General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755961
Start date and time:	2022-11-29 11:23:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PURCHASE ORDER.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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@18/9@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings
• Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe • Not all processes where analyzed, report is missing behavior information • 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
11:24:07	API Interceptor	1x Sleep call for process: PURCHASE ORDER.exe modified
11:24:17	Task Scheduler	Run new task: PAYWOGORT path: C:\Users\user\AppData\Roaming\PAYWOGORT.exe
11:24:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run yGbzOMP C:\Users\user\AppData\Roaming\yGbzOMP\yGbzOMP.exe
11:24:31	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run yGbzOMP C:\Users\user\AppData\Roaming\yGbzOMP\yGbzOMP.exe
11:24:35	API Interceptor	447x Sleep call for process: RegSvcs.exe modified
11:24:36	API Interceptor	1x Sleep call for process: PAYWOGORT.exe modified

Joe Sandbox View / Context

IPs
No context

Domains
No context

ASNs
No context

JA3 Fingerprints
No context

Dropped Files
No context

Created / dropped Files	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\PAyWOGORT.exe.log	
Process:	C:\Users\user\AppData\Roaming\PAyWOGORT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7FF8
Malicious:	false
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\ff1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\PURCHASE ORDER.exe.log 	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7FF8
Malicious:	true

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=b03f5f711d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f711d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\ff1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f711d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a
----------	--

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\yGbzOMP.exe.log	
Process:	C:\Users\user\AppData\Roaming\yGbzOMP\yGbzOMP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f711d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp6AED.tmp	
Process:	C:\Users\user\AppData\Roaming\PayWOGORT.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.177923914853658
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFP//rIMhEMjnPgwjplgUYODOLD9RJh7h8gKBGQBtncbhK79INQR/rydbz9I3YODOLNdq31
MD5:	80E675E5B2A240D5A633F826B64E2CF7
SHA1:	A690D2C5FB99B392615E75E68CE86972910D28AE
SHA-256:	4F6FD6CEF34AAFE00144F440C2AE385364AB808F5B9CFEF4E7EB5105066B0302
SHA-512:	3DA27B4BBD5C37247809800B67C0EE0DB05272AE56674AF3CDEE6D95226A7C22E3341CB5200021559C6AAE9240AF3B6A5581333D7A92543D56DA679C32EFF8CD
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>true

C:\Users\user\AppData\Local\Temp\tmpF89B.tmp 	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.177923914853658
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFP//rIMhEMjnPgwjplgUYODOLD9RJh7h8gKBGQBtncbhK79INQR/rydbz9I3YODOLNdq31
MD5:	80E675E5B2A240D5A633F826B64E2CF7
SHA1:	A690D2C5FB99B392615E75E68CE86972910D28AE
SHA-256:	4F6FD6CEF34AAFE00144F440C2AE385364AB808F5B9CFEF4E7EB5105066B0302
SHA-512:	3DA27B4BBD5C37247809800B67C0EE0DB05272AE56674AF3CDEE6D95226A7C22E3341CB5200021559C6AAE9240AF3B6A5581333D7A92543D56DA679C32EFF8CD
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>true

C:\Users\user\AppData\Roaming\PayWOGorT.exe 	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	600576
Entropy (8bit):	7.888370004294712
Encrypted:	false
SSDEEP:	12288:7gkzrbETCvHskFgFwlyXCD1vmAMDfJ0/legnS1onhj6W4ytrRpMf:/76CVskFgqlyXFhS/ngSWhxROf
MD5:	A55B4BB09398659D69F1B8B37541E621
SHA1:	975F7C38780D00AE497FCB6ADDF31F5AD8CDB090
SHA-256:	EA45A2032EEBE69D32B15D3EA505330EB00B5026107E8E123FB9FB9E2BF87496
SHA-512:	A5EB89B7B07AD51B747BA5C003D50AE8AA53C11ADB23034DA977E8AB25373A81C3C7216CDA025C25A0D55F9CAB989F93794D2512FB16A8998DFA8D58C5210590
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 61%
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$.PE..L.....c.....5...@...@..... ..@.....x5..W...@..4.....H.....text......H......rsrc..4....@.....@..@.rel oc.....^.....@..B.....5.....H.....T.....4.....E.....z.....(..o!..)....*.0.....{.....3.....*.....0.....{.....f.....}.....}.....s...o...}.....8.....{...o...}.....{.....}.....{.....Y}.....{...-...+H.....{.....X{...X ; {...Xa}.....}{...o...:q.....(+..{.....}.....(*.....n...}{.....{...o...}*...*.s".

C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe 	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6lq87PiU9FVlaLmf:EoOIBf0ddsYy8LujVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$.PE..L...zX.Z.....0..d.....V.....@.. .." ..^.....@.....O.....8.....r..>.....H.....text...c... ..d......rsrc...8.....f.....@..@.reloc.....p.....@..B.....8.....H.....+...S..... ...P.....r.....*2.(....(*Z.r...p(....{.....}....*...{*s.....*0.{.....Q..s.....+i~...0....{..... s.....o.....rl..p.(...Q.P.;P.....(...o...o.....(...o!...o".....o#.t.....*0..(.....s\$.....o%...X..(....-.*o&...*0.....('....&...*0.....(&...*0.....(.....{...~.....{...~....o....9]...

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F145
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /c Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.888370004294712
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.exe
File size:	600576
MD5:	a55b4bb09398659d69f1b8b37541e621
SHA1:	975f7c38780d00ae497fcb6addf31f5ad8cdb090
SHA256:	ea45a2032eebe69d32b15d3ea505330eb00b5026107e8e123fb9fb9e2bf87496
SHA512:	a5eb89b7b07ad51b747ba5c003d50ae8aa53c11adb23034da977e8ab25373a81c3c7216cda025c25a0d55f9cab989f93794d2512fb16a8998dfa8d58c5210590
SSDEEP:	12288:7gkzrbETCivHskFgFwlyXCD1vmAMDfJ0/legnS1onhj6W4ytrRpMf:/76CVskFgqlyXFhS/ngSWhxROf
TLSH:	98D4023C1B457F2BC27D88F595D24E017FF18D19A021EA1AACDE66D803C67781B90ED5
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.....PE..L.....c.....5... ..@....@..@.....

File Icon



Icon Hash:	0969696949097961
------------	------------------

Static PE Info

General

Entrypoint:	0x4935d2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63841E09 [Mon Nov 28 02:33:45 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

[illegible]

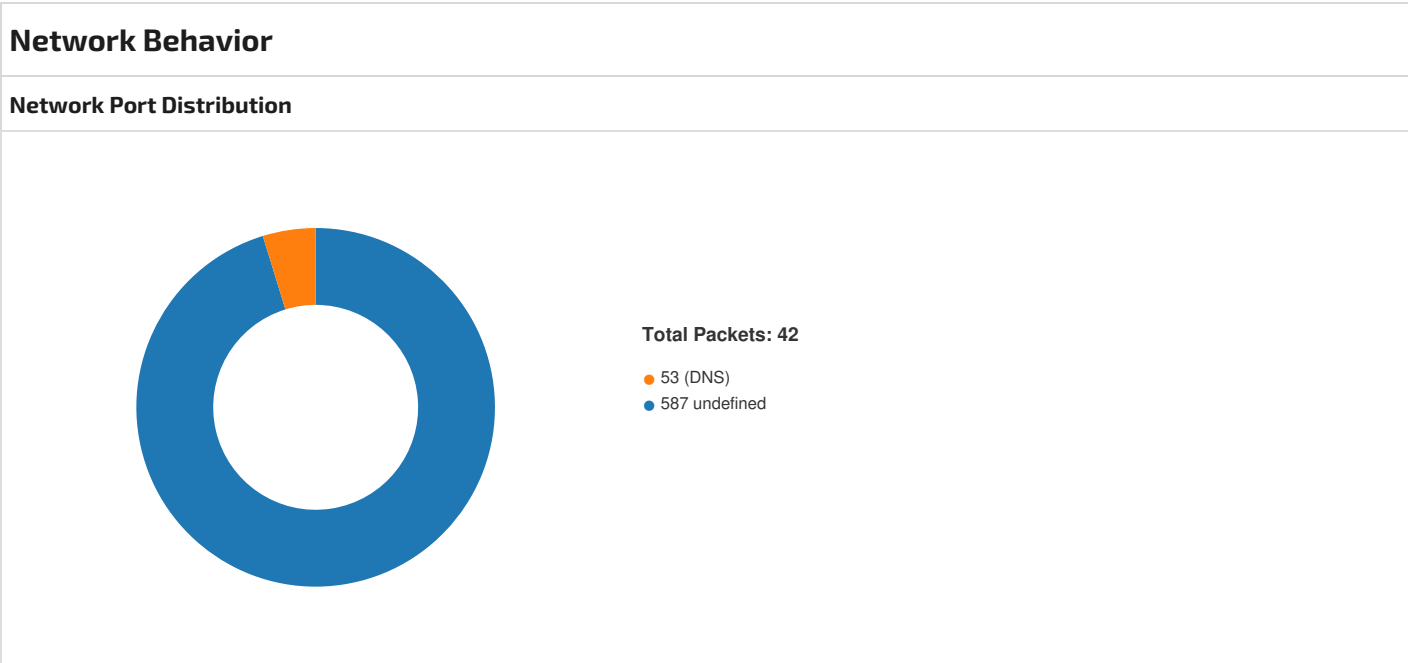
Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x93578	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x94000	0xf34	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x96000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x915d8	0x91600	False	0.8968941449914015	data	7.897447602261709	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x94000	0xf34	0x1000	False	0.674072265625	data	6.343221929180967	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x96000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDA BLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0x94118	0xa75	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x94b90	0x14	data		
RT_GROUP_ICON	0x94ba4	0x14	data		
RT_VERSION	0x94bb8	0x37c	data		

Imports	
DLL	Import
mscoree.dll	_CorExeMain



TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:24:36.287166119 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:36.589534998 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:36.589658976 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:38.225836039 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:38.226146936 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:38.523627043 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:38.523865938 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:38.826832056 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:38.889180899 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:39.213813066 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:39.213850975 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:39.213881016 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:39.213903904 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:39.213943005 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:39.213980913 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:39.217195988 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:39.264162064 CET	49695	587	192.168.2.4	119.148.27.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:24:39.562028885 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:39.623230934 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:39.920614004 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:39.944987059 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:40.242274046 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:40.251883984 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:40.587641954 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:40.821350098 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:40.822257996 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:41.119117975 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:41.119190931 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:41.119870901 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:41.424794912 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:41.425214052 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:41.724648952 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:41.726552963 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:41.730971098 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:41.731875896 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:41.731961966 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:42.029700041 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:42.035222054 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:42.035703897 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:42.035804033 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:42.120207071 CET	587	49695	119.148.27.3	192.168.2.4
Nov 29, 2022 11:24:42.164433956 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:24:57.036175013 CET	49695	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:15.563796043 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:15.861283064 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:15.861886024 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:17.602075100 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:17.602732897 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:17.901496887 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:17.902745962 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:18.200984001 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:18.215336084 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:18.529184103 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:18.529251099 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:18.529294968 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:18.529333115 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:18.529411077 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:18.529882908 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:18.531244040 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:18.541455984 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:18.841746092 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:18.886261940 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:18.943299055 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:19.239828110 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:19.242074013 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:19.538795948 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:19.540328979 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:19.875647068 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:19.899672031 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:19.900697947 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:20.196681023 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:20.196717978 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:20.197648048 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:20.502088070 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:20.502681017 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:20.798707008 CET	587	49696	119.148.27.3	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:25:20.803905010 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:20.804018974 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:20.804094076 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:20.804167986 CET	49696	587	192.168.2.4	119.148.27.3
Nov 29, 2022 11:25:21.100074053 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:21.100131035 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:21.101542950 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:21.140907049 CET	587	49696	119.148.27.3	192.168.2.4
Nov 29, 2022 11:25:21.183245897 CET	49696	587	192.168.2.4	119.148.27.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:24:36.029767036 CET	56572	53	192.168.2.4	8.8.8.8
Nov 29, 2022 11:24:36.203140020 CET	53	56572	8.8.8.8	192.168.2.4
Nov 29, 2022 11:25:15.366661072 CET	50911	53	192.168.2.4	8.8.8.8
Nov 29, 2022 11:25:15.530844927 CET	53	50911	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 11:24:36.029767036 CET	192.168.2.4	8.8.8.8	0x2672	Standard query (0)	mail.orage nicgroup-bd.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:25:15.366661072 CET	192.168.2.4	8.8.8.8	0x3968	Standard query (0)	mail.orage nicgroup-bd.com	A (IP address)	IN (0x0001)	false

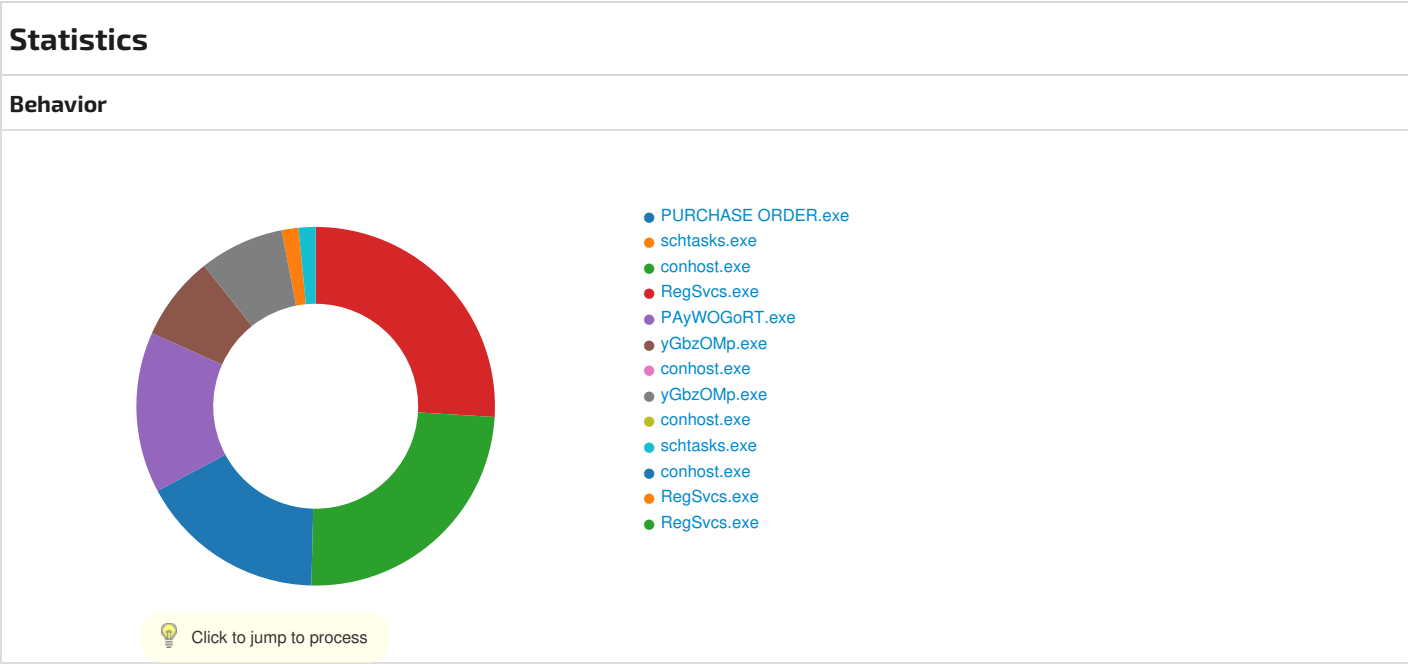
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 11:24:36.203140020 CET	8.8.8.8	192.168.2.4	0x2672	No error (0)	mail.orage nicgroup-bd.com		119.148.27.3	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:25:15.530844927 CET	8.8.8.8	192.168.2.4	0x3968	No error (0)	mail.orage nicgroup-bd.com		119.148.27.3	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 11:24:38.225836039 CET	587	49695	119.148.27.3	192.168.2.4	220-panel2.agni.com ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 16:24:38 +0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 11:24:38.226146936 CET	49695	587	192.168.2.4	119.148.27.3	EHLO 549163
Nov 29, 2022 11:24:38.523627043 CET	587	49695	119.148.27.3	192.168.2.4	250-panel2.agni.com Hello 549163 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Nov 29, 2022 11:24:38.523865938 CET	49695	587	192.168.2.4	119.148.27.3	STARTTLS
Nov 29, 2022 11:24:38.826832056 CET	587	49695	119.148.27.3	192.168.2.4	220 TLS go ahead
Nov 29, 2022 11:25:17.602075100 CET	587	49696	119.148.27.3	192.168.2.4	220-panel2.agni.com ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 16:25:17 +0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 11:25:17.602732897 CET	49696	587	192.168.2.4	119.148.27.3	EHLO 549163
Nov 29, 2022 11:25:17.901496887 CET	587	49696	119.148.27.3	192.168.2.4	250-panel2.agni.com Hello 549163 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Nov 29, 2022 11:25:17.902745962 CET	49696	587	192.168.2.4	119.148.27.3	STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 11:25:18.200984001 CET	587	49696	119.148.27.3	192.168.2.4	220 TLS go ahead



System Behavior	
Analysis Process: PURCHASE ORDER.exe PID: 5196, Parent PID: 3528	
General	
Target ID:	0
Start time:	11:23:57
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Imagebase:	0xc10000
File size:	600576 bytes
MD5 hash:	A55B4BB09398659D69F1B8B37541E621
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: 00000000.00000002.341336847.0000000003297000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.342927901.0000000004279000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.342927901.0000000004279000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.342927901.0000000004279000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities							
File Created							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D87CF06	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	6D87CF06	unknown
C:\Users\user\AppData\Roaming\PAyWOGORT.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpF89B.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C6C7038	GetTempFile NameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PURCHASE ORDER.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6DB8C78D	CreateFileW

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF89B.tmp	success or wait	1	6C6C6A95	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\PAyWOGORT.exe	0	600576	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 50 45 00 00 4c 01 03 00 09 1e fd 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 16 09 00 00 12 00 00 00 00 00 00 fd 35 09 00 00 20 00 00 00 40 09 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 fd 09 00 00 02 00 00 00 00 00 00 02 00 40 fd 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@!LThis program cannot be run in DOS mode.\$PELc5 @@ @ @	success or wait	1	6C6C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF89B.tmp	0	1642	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 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 6a 6f 6e 65 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 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo> <Date>2014-10- 25T14:27:44.8929027</ Date> <Author>computer/user </Author> </RegistrationIn	success or wait	1	6C6C1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\PURCHASE ORDER.exe.log	0	1216	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",01,"Win RT","N otApp",12,"System.Wind ows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c 56 1934e089",03,"System, Version=4.0.0.0, Culture=neutral, Publ icKeyToken=b77a5c5619 34e089", C:\Windows\assembly\Na tiveImages_v4.0.3	success or wait	1	6DB8C907	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	6D855705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D855705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebdbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Users\user\Desktop\PURCHASE ORDER.exe	unknown	600576	success or wait	1	6C6C1B4F	ReadFile

Analysis Process: schtasks.exe PID: 1948, Parent PID: 5196

General

Target ID:	1
Start time:	11:24:14
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\PayWOGORT" /XML "C:\Users\user\AppData\Local\Temp\tmpF89B.tmp
Imagebase:	0x2f0000
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\tmpF89B.tmp	unknown	2	success or wait	1	2FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF89B.tmp	unknown	1643	success or wait	1	2FABD9	ReadFile

Analysis Process: conhost.exe PID: 2040, Parent PID: 1948

General

Target ID:	2
Start time:	11:24:15
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: RegSvcs.exe PID: 4212, Parent PID: 5196

General

Target ID:	3
Start time:	11:24:15
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x610000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000003.00000000.337559814.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.337559814.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000003.00000000.337559814.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.412448960.00000000028F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.412448960.00000000028F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	6D87CF06	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	6D87CF06	unknown	
C:\Users\user\AppData\Roaming\yGbzOMP	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C6CBEFF	CreateDirectoryW	
C:\Users\user\AppData\Roaming\yGbzOMP\yGbzOMP.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	6C6CDD66	CopyFileW	
C:\Users\user\AppData\Local\Temp\tmpA606.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C6C7038	GetTempFileNameW	

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\yGbzOMp\yGbzOMp.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 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.\$PElzXZ0dV @ ""	success or wait	1	6C6CDD66	CopyFileW

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D855705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeec36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D85CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D85CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebdbbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6125b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D855705	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C6C1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ca8b3b75-86f2-4edb-b016-ef7ebe8beb9b	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\Downloader\config\database.script	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\Downloader\config\database.script	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C6C1B4F	ReadFile

Registry Activities							
Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	yGbZOMp	unicode	C:\Users\user\AppData\Roaming\yGbZOMp\yGbZOMp.exe	success or wait	1	6C6C646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	yGbZOMp	binary	02 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C6CDE2E	RegSetValueExW

Analysis Process: PAYWOGORT.exe PID: 1520, Parent PID: 1088

General	
Target ID:	4
Start time:	11:24:17
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\PAYWOGORT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\PAYWOGORT.exe
Imagebase:	0xb40000
File size:	600576 bytes
MD5 hash:	A55B4BB09398659D69F1B8B37541E621
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 61%, 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	6D87CF06	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	6D87CF06	unknown	
C:\Users\user\AppData\Local\Temp\tmp6AED.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C6C7038	GetTempFileNameW	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\PAYWOGORT.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6DB8C78D	CreateFileW	

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6AED.tmp	success or wait	1	6C6C6A95	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\Local\Temp\tmp6AED.tmp	0	1642	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 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 6a 6f 6e 65 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 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo> <Date>2014-10- 25T14:27:44.8929027</ Date> <Author>computer/user </Author> </RegistrationIn	success or wait	1	6C6C1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\PAyWOGorT.exe.log	0	1216	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",01,"Win RT","N otApp",12,"System.Wind ows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c 56 1934e089",03,"System, Version=4.0.0.0, Culture=neutral, Publ icKeyToken=b77a5c5619 34e089", C:\Windows\assembly\Na tiveImages_v4.0.3	success or wait	1	6DB8C907	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	6D855705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D855705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebd8bb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile

Analysis Process: yGbzOMp.exe PID: 1604, Parent PID: 3528

General

Target ID:	5
Start time:	11:24:31
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\yGbzOMp\yGbzOMp.exe"
Imagebase:	0x900000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR\v4.0.32\UsageLogs\yGbzOMp.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6DB8C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C6C1B4F	WriteFile
\Device\ConDrv	141	141	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67	USAGE: regsvcs.exe [options] A ssemblyNameOptions: /? or /help Display this usage message. /fc Find or create targ	success or wait	1	6C6C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\\Device\\ConDrv	397	256	20 20 20 20 20 20 20 20 45 78 70 65 63 74 20 61 6e 20 65 78 69 73 74 69 6e 67 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 74 6c 62 3a 3c 74 6c 62 66 69 6c 65 3e 20 20 46 69 6c 65 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 65 78 70 6f 72 74 65 64 20 74 79 70 65 20 6c 69 62 72 61 72 79 2e 0d 0a 20 20 20 20 2f 61 70 70 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 61 72 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 6f 72 20 69 64 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 70 61 72 74 69 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f	Expect an existing application. /tlb:<tlbfile> Filename for the exported type library. /appname: <name> Use the specified name for the target application. /parname:<name> Use the specified name or id for the target partition. /	success or wait	3	6C6C1B4F	WriteFile
\\Device\\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C6C1B4F	WriteFile
C:\\Users\\user\\AppData\\Local\\Microsoft\\CLR_v4.0_32\\UsageLogs\\yGbzOMp.exe.log	0	142	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 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","N otApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	6DB8C907	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	6D855705	unknown	
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\Config\\machine.config	unknown	6135	success or wait	1	6D855705	unknown	
C:\\Windows\\assembly\\NativeImages_v4.0.30319_32\\mscorlib.a152fe02a317a77ae36903305e8ba6\\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile	
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\Config\\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile	

Analysis Process: conhost.exe PID: 5188, Parent PID: 1604	
General	
Target ID:	6
Start time:	11:24:32
Start date:	29/11/2022
Path:	C:\\Windows\\System32\\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\\Windows\\system32\\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\\Device\\ConDrv	397	256	20 20 20 20 20 20 20 20 45 78 70 65 63 74 20 61 6e 20 65 78 69 73 74 69 6e 67 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 74 6c 62 3a 3c 74 6c 62 66 69 6c 65 3e 20 20 46 69 6c 65 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 65 78 70 6f 72 74 65 64 20 74 79 70 65 20 6c 69 62 72 61 72 79 2e 0d 0a 20 20 20 20 2f 61 70 70 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 61 72 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 6f 72 20 69 64 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 70 61 72 74 69 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f	Expect an existing application. /tlb:<tlbfile> Filename for the exported type library. /appname: <name> Use the specified name for the target application. /parname:<name> Use the specified name or id for the target partition. /	success or wait	3	6C6C1B4F	WriteFile
\\Device\\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C6C1B4F	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	6D855705	unknown	
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\Config\\machine.config	unknown	6135	success or wait	1	6D855705	unknown	
C:\\Windows\\assembly\\NativeImages_v4.0.30319_32\\mscorlib.a152fe02a317a77aeee36903305e8ba6\\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile	
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\Config\\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile	
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\Config\\machine.config	unknown	6135	success or wait	1	6D85CA54	ReadFile	
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\Config\\machine.config	unknown	7976	success or wait	1	6D85CA54	ReadFile	

Analysis Process: conhost.exe PID: 3720, Parent PID: 4184	
General	
Target ID:	8
Start time:	11:24:41
Start date:	29/11/2022
Path:	C:\\Windows\\System32\\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\\Windows\\system32\\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 1240, Parent PID: 1520	
General	
Target ID:	9
Start time:	11:24:43
Start date:	29/11/2022

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\PAyWOGorT" /XML "C:\Users\user\AppData\Local\Temp\tmp6AED.tmp
Imagebase:	0x2f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
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\tmp6AED.tmp	unknown	2	success or wait	1	2FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6AED.tmp	unknown	1643	success or wait	1	2FABD9	ReadFile

Analysis Process: conhost.exe PID: 6096, Parent PID: 1240

General

Target ID:	10
Start time:	11:24:43
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 5292, Parent PID: 1520

General

Target ID:	11
Start time:	11:24:44
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1b0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: 3836, Parent PID: 1520

General

Target ID:	12
Start time:	11:24:44
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x640000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.570378772.0000000002A5C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.570378772.0000000002A5C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

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	6D87CF06	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	6D87CF06	unknown
C:\Users\user\AppData\Roaming\yGbzOMP\yGbzOMP.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	6C6CDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4756.tmp			read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C6C7038	GetTempFile NameW
File Deleted									
File Path						Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yGbzOMP\yGbzOMP.exe						success or wait	1	6C6C6A95	DeleteFileW
File Written									
File Path		Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

 No disassembly