JoeSandbox Cloud BASIC

Windows Analysis Report ADJUSTED PO3917NOV.exe

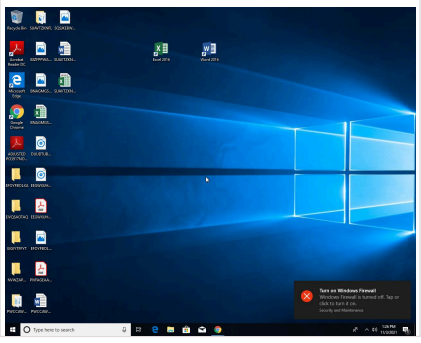
Create Interactive Tour

Overview

General Information

Sample Name:	ADJUSTED PO3917NOV.exe
Analysis ID:	514608
MD5:	ec46f95f234b89325…
SHA1:	d0600cdb17f86f31ef…
SHA256:	01bbef21bea94b6ec…
Tags:	exe, warzonerat
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

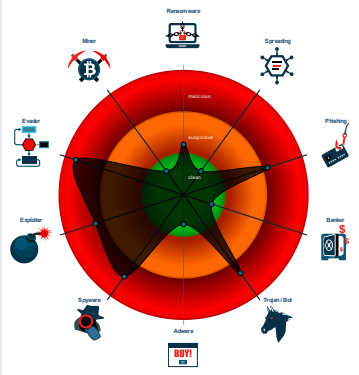
AveMaria UACMe

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

Signatures

- Yara detected AntiVM3
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Malicious sample detected (through commu…
- Yara detected UACMe UAC Bypass tool
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dropped file
- Tries to steal Mail credentials (via file / regis…
- Tries to detect sandboxes and other dynami…
- .NET source code contains potential unpacker
- Hides that the sample has been downloade…
- Uses schtasks.exe or at.exe to add and mo…
- Tries to harvest and steal browser informatio…
- Increases the number of concurrent connect…
- Contains functionality to hide user accounts

Classification



Process Tree

- **System is w10x64**
- ADJUSTED PO3917NOV.exe (PID: 5404 cmdline: "C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe" MD5: EC46F95F234B89325E198104D1887B1C)
  - schtasks.exe (PID: 3244 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QUQovKcaZRcNZ" /XML "C:\Users\user\AppData\Local\Temp\tmpD7D5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ADJUSTED PO3917NOV.exe (PID: 1328 cmdline: C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe MD5: EC46F95F234B89325E198104D1887B1C)
- **cleanup**

Malware Configuration

Threatname: AveMaria


```
{
  "C2 url": "185.222.57.253",
  "port": 4782
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.327703338.00000000015C4000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000003.327703338.00000000015C4000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000004.00000000.319379461.0000000000400000.00000040.00000001.sdmp	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x150e8:$a1: \Opera Software\Opera Stable\Login Data • 0x15410:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x14d58:$a3: \Google\Chrome\User Data\Default\Login Data
00000004.00000000.319379461.0000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000000.319379461.0000000000400000.00000040.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	

Click to see the 63 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.ADJUSTED PO3917NOV.exe.15a0220.2.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2318:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
4.3.ADJUSTED PO3917NOV.exe.15a0220.2.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2318:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x2318:$c1: Elevation:Administrator!new:
4.3.ADJUSTED PO3917NOV.exe.15a0220.2.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
4.3.ADJUSTED PO3917NOV.exe.15a0220.5.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xb18:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
4.3.ADJUSTED PO3917NOV.exe.15a0220.5.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xb18:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xb18:$c1: Elevation:Administrator!new:

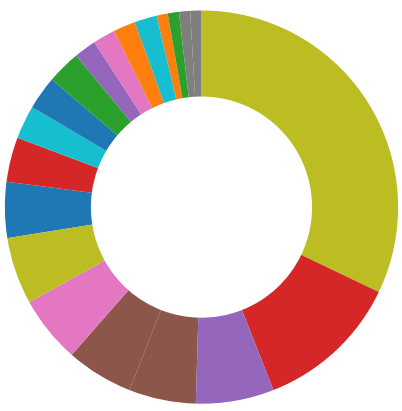
Click to see the 131 entries

JoeSandbox Cloud BASIC

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview



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

Click to jump to signature section

Show All Signature Results

AV Detection:

Found malware configuration — Show sources
Multi AV Scanner detection for submitted file — Show sources
Yara detected AveMaria stealer — Show sources
Multi AV Scanner detection for dropped file — Show sources

Exploits:

Yara detected UACMe UAC Bypass tool — Show sources

Networking:

C2 URLs / IPs found in malware configuration — Show sources

E-Banking Fraud:

Yara detected AveMaria stealer — Show sources

System Summary:

Malicious sample detected (through community Yara rule) — Show sources

Data Obfuscation:

.NET source code contains potential unpacker — Show sources

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules — Show sources

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier) — Show sources
Contains functionality to hide user accounts — Show sources

Malware Analysis System Evasion:

Yara detected AntiVM3 — Show sources
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function) — Show sources

HIPS / PFW / Operating System Protection Evasion:

Contains functionality to inject threads in other processes — Show sources

Increases the number of concurrent connection per server for Internet Explorer — Show sources

Stealing of Sensitive Information:

Yara detected AveMaria stealer — Show sources
Tries to steal Mail credentials (via file / registry access) — Show sources
Tries to harvest and steal browser information (history, passwords, etc) — Show sources
Contains functionality to steal e-mail passwords — Show sources
Contains functionality to steal Chrome passwords or cookies — Show sources

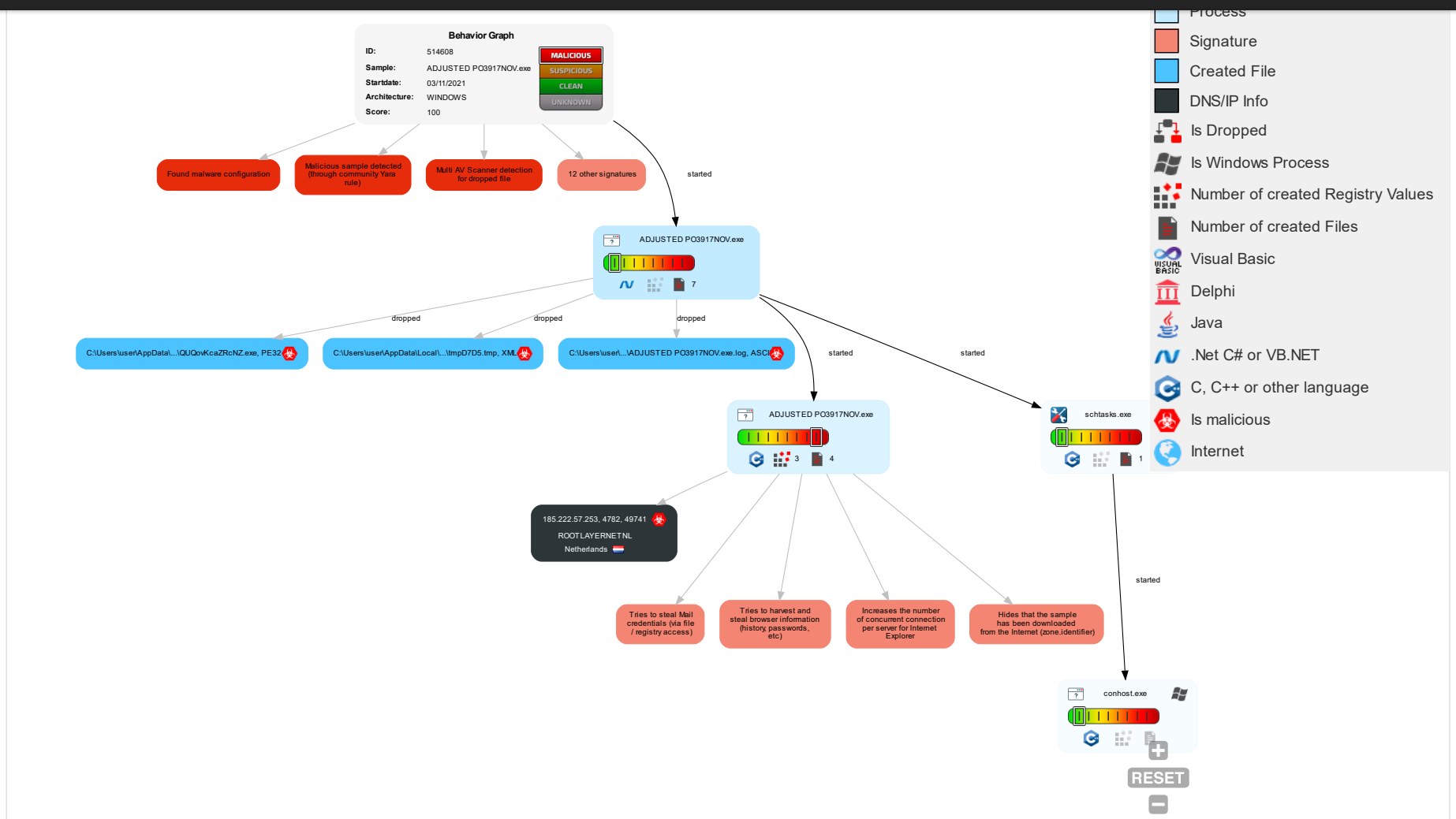
Remote Access Functionality:

Yara detected AveMaria stealer — Show sources

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	Native API 1	Create Account 1	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 3	System Time Discovery 1 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Endpoint Denial of Service 1
Default Accounts	Scheduled Task/Job 1	Windows Service 1	Windows Service 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	System Service Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	Service Execution 2	Scheduled Task/Job 1	Process Injection 1 2 2	Obfuscated Files or Information 2	Credentials In Files 1	File and Directory Discovery 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 1	NTDS	System Information Discovery 2 7	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Application Layer Protocol 1	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 3	LSA Secrets	Security Software Discovery 2 2 1	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	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	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	Access Token Manipulation 1	DCSync	Process Discovery 3	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	Process Injection 1 2 2	Proc Filesystem	Network Service Scanning	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)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Users 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

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
ADJUSTED PO3917NOV.exe	31%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QUQovKcaZRcNZ.exe	29%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.ADJUSTED PO3917NOV.exe.400000.8.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.ADJUSTED PO3917NOV.exe.400000.15.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.2.ADJUSTED PO3917NOV.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.ADJUSTED PO3917NOV.exe.400000.21.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.ADJUSTED PO3917NOV.exe.400000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.ADJUSTED PO3917NOV.exe.400000.18.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.ADJUSTED PO3917NOV.exe.400000.12.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.ADJUSTED PO3917NOV.exe.400000.6.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
4.0.ADJUSTED PO3917NOV.exe.400000.10.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/dz	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comB	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
185.222.57.253	4%	Virustotal		Browse
185.222.57.253	0%	Avira URL Cloud	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.sajatypeworks.comeL	0%	Avira URL Cloud	safe	

http://www.fontbureau.com;	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnpor	0%	Avira URL Cloud	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://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Stan	0%	Avira URL Cloud	safe	
http://www.fontbureau.comde	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/l	0%	URL Reputation	safe	
http://www.fontbureau.comceva	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnr(	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdl	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/l	0%	URL Reputation	safe	
http://www.fontbureau.comM.TTF	0%	URL Reputation	safe	
http://www.sajatypeworks.com#	0%	Avira URL Cloud	safe	
http://www.fontbureau.comival	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn#	0%	URL Reputation	safe	

Domains and IPs

Download Network PCAP: filtered – full

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.222.57.253	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.222.57.253	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	514608
Start date:	03.11.2021
Start time:	13:23:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 14s
Hypervisor based Inspection enabled:	false
Report type:	full
Sample file name:	ADJUSTED PO3917NOV.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:	19
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.phis.troj.spyw.expl.evad.winEXE@6/6@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.1% (good quality ratio 26.6%) • Quality average: 84.6% • Quality standard deviation: 21%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 101 • Number of non-executed functions: 122
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:24:17	API Interceptor	2x Sleep call for process: ADJUSTED PO3917NOV.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.222.57.253	Kyodo International Corp - Products Lists.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	RJH56789098704321234067876543056 70.exe	Get hash	malicious	Browse	• 185.222.57.217
	Q4EtLThkYIEkFwu.exe	Get hash	malicious	Browse	• 45.137.22.146
	CORMATEX - INQUIRY LIST.exe	Get hash	malicious	Browse	• 45.137.22.70
	Purchase Order# 210145.exe	Get hash	malicious	Browse	• 185.222.57.71
	PO_Contract_ANR07152112_20210715181907__110.exe	Get hash	malicious	Browse	• 185.222.57.71
	PO_Contract_ANR07152112_20210715181907__110.exe	Get hash	malicious	Browse	• 185.222.57.71
	PO.90764535.slip.scan.xls...exe	Get hash	malicious	Browse	• 185.222.57.242
	ENC MARKETING - INQUIRY AND SAMPLE REQUEST.exe	Get hash	malicious	Browse	• 45.137.22.70
	NAC0098765434567890-09876.exe	Get hash	malicious	Browse	• 185.222.57.90
	Order#7631298.slip..xls...exe	Get hash	malicious	Browse	• 185.222.57.242
	RHK0987600456780090 00.exe	Get hash	malicious	Browse	• 185.222.57.90
	FHKPO098765432345.exe	Get hash	malicious	Browse	• 185.222.57.90
	SecuriteInfo.com.Suspicious.Win32.Save.a.4240.exe	Get hash	malicious	Browse	• 185.222.58.151
	SecuriteInfo.com.Artemis3008D0721A6C.1070.exe	Get hash	malicious	Browse	• 185.222.58.151
	AWB #3099657260.xlsx	Get hash	malicious	Browse	• 185.222.57.190
	HIC INTERNATIONAL - REQUEST FOR QUOTATION DOCUMENTS.exe	Get hash	malicious	Browse	• 45.137.22.70
	AWB #30996572600.xlsx	Get hash	malicious	Browse	• 185.222.57.190
	BL. NO. ANSMUNDAR3621.exe	Get hash	malicious	Browse	• 185.222.57.71

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ADJUSTED PO3917NOV.exe.log Download File

Process:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.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:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmpD7D5.tmp Download File

Process:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.2021349858666435
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBgAPtn:cbh47TlNQ//rydbz9l3YODOLNdq3yy
MD5:	1C1A65CA91C09759C032BDB8A9D63E5D
SHA1:	99404B26FCF77D27761690D71EEDB2C2B41B8755
SHA-256:	14C38D65AA4C38350AD298E9742BC7982B635FF0D82C1B973710D84BAFB53C2E
SHA-512:	9ACF01FDBC35568D22E53C21723C1B4EFB488EEC84E17B8444823A628F5D09EDEA04EEFF76A3A524C0C8C050D2CE819FABB6DA845767B531F260614C72B165B8
Malicious:	**true**
Reputation:	low
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\AHuvEkw.tmp Download File

Process:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+lIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Roaming\Knptwsn.tmp Download File

Process:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXaflB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647

Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAA AAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7IkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXlE4R7l0AAAABIt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166079 96"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Roaming\QUQovKcaZRcNZ.exe Download File

Process:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	963072
Entropy (8bit):	6.000080999689837
Encrypted:	false
SSDEEP:	6144:KMs+2EfXXT4uWtf5YTZkUPTUTsTlNOsk4F8d5JF4Nydla+4dZN0lTwl:Kk/DeV5YTZHPTesTW5JF4MN4dU1wl
MD5:	EC46F95F234B89325E198104D1887B1C
SHA1:	D0600CDB17F86F31EFF130D029A87717FDE2CC7A
SHA-256:	01BBEF21BEA94B6EC60C739DF3E40E887CF0EA1DF7BA2F1678CE708BA10A6203
SHA-512:	C3207A8C9C4639A40AD72308C7AA6710C78C4AC014704CF6675AD7D724CFDBA9D7A0AFD292E7B133EEB964342A1B0988A6CFC8C24D0EB84A43787405227968EB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...p.a.....0.....+... ...@....@.. ....H.....text..... ....`.rsrc... ....@.....@..@.reloc.....@..B..... .x+.....H.....T...R.....}.....P.....{....*.0..-.....6...%..~.o.....%.r...p.%.r?..p.%...*J.rU..p}.....(....*.0.....rU..p}.....(.....}.....}.....9.....o.....3V..+...o....~e.....3...}.... +...X.~e....i2...+...o....~f.....3...}....+...X.~f....i2..{....-..rU..p(...,...}.....+..~g.....(...,...}....*..X.~g....i2.*..{....*...0..x.....rU..p..{.....YE.....,...+8.rW..p(.....+6.rg..p(.....+(.r}..p(.....+..r...p(

C:\Users\user\AppData\Roaming\QUQovKcaZRcNZ.exe:Zone.Identifier Download File

Process:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.000080999689837
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:	ADJUSTED PO3917NOV.exe
File size:	963072
MD5:	ec46f95f234b89325e198104d1887b1c
SHA1:	d0600cdb17f86f31eff130d029a87717fde2cc7a
SHA256:	01bbef21bea94b6ec60c739df3e40e887cf0ea1df7ba2f1678ce708ba10a6203
SHA512:	c3207a8c9c4639a40ad72308c7aa6710c78c4ac014704cf6675ad7d724cfdba9d7a0afd292e7b133eeb964342a1b0988a6cfc8c24d0eb84a43787405227968eb
SSDEEP:	6144:KMs+2EfXXT4uWtf5YTZkUPTUTsTlNOsk4F8d5JF4Nydla+4dZN0lTwl:Kk/DeV5YTZHPTesTW5JF4MN4dU1wl
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...p..a.....0.....+... ...@....@.. ....@.....

File Icon

Icon Hash:	f0f0faf2e8ccb48a

Static PE Info

General

Entrypoint:	0x482b96
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

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	0x80bcc	0x80c00	False	0.561988015777	data	6.21831911022	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x6a120	0x6a200	False	0.121188070524	data	5.17746746332	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

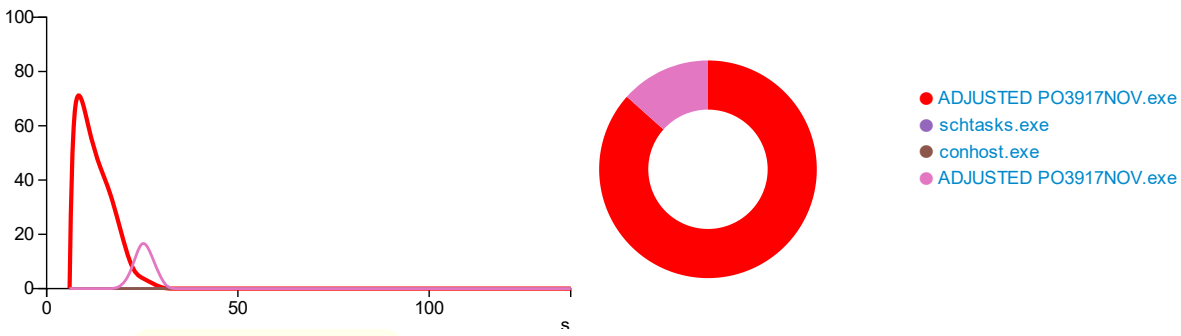
Download Network PCAP: filtered – full

TCP Packets

Code Manipulations

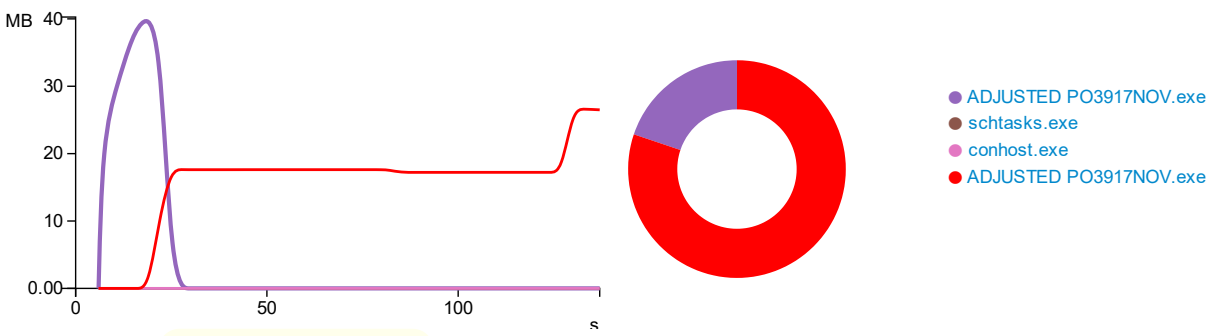
Statistics

CPU Usage



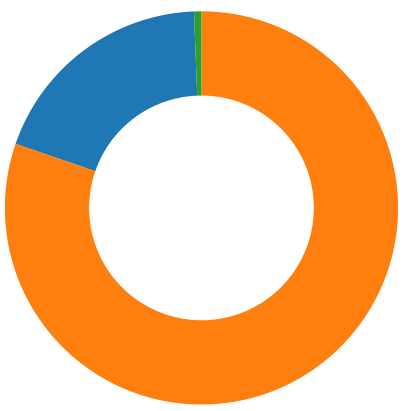
Click to jump to process

Memory Usage



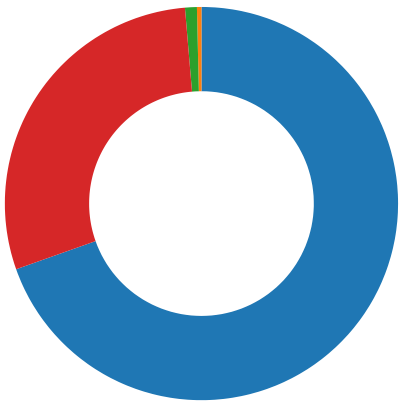
Click to jump to process

High Level Behavior Distribution



Click to dive into process behavior distribution

Behavior



Click to jump to process

System Behavior

Analysis Process: ADJUSTED PO3917NOV.exe PID: 5404 Parent PID: 3608

Function Logs

General

Start time:	13:24:11
Start date:	03/11/2021
Path:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe"
Imagebase:	0x990000
File size:	963072 bytes
MD5 hash:	EC46F95F234B89325E198104D1887B1C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.327281323.00000000030A2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.327281323.00000000030A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.327281323.00000000030A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.327281323.00000000030A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.327014581.0000000002ED1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.327512166.0000000003ED9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.327512166.0000000003ED9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.327512166.0000000003ED9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.327512166.0000000003ED9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Opened

File Created

File Deleted

File Written

File Read

File Attributes Queried

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Key Opened

Key Value Queried

Key Monitored

Key Value Enumerated

Key Enumerated

Mutex Activities — Show Windows behavior

Mutex Created

Process Activities — Show Windows behavior

Process Created

Process Queried

Process Information Set

Process Terminated

Thread Activities — Show Windows behavior

Thread Created

Thread Execution Resumed

Thread Delayed

Thread Information Set

Memory Activities — Show Windows behavior

Memory Allocated

Memory Protection Changed

Memory Usage Statistics

System Activities — Show Windows behavior

Language or Locale ID Queried

System Information Queried

Timing Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

Window Created

Message Posted to Windows UI

Process Token Activities — Show Windows behavior

Token Adjusted

Object Security Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

JoeSandbox Cloud BASIC

General

Start time:	13:24:22
Start date:	03/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QUQovKcaZRcNZ" /XML "C:\Users\user\AppData\Local\Temp\tmpD7D5.tmp
Imagebase:	0x12f0000
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 Opened

Section Activities — Show Windows behavior

Sections loaded by Windows

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: conhost.exe PID: 4412 Parent PID: 3244

Function Logs

General

Start time:	13:24:22
Start date:	03/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Attributes Queried

Volume Information Queried

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Mutex Activities

Process Activities — Show Windows behavior

Thread Activities — Show Windows behavior

Thread Created

Thread Delayed

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

Window Created

Window UI Enumerated

Message Posted to Windows UI

Window UIs Event Hook Set

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: ADJUSTED PO3917NOV.exe PID: 1328 Parent PID: 5404

Function Logs

General

Start time:	13:24:22
Start date:	03/11/2021
Path:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ADJUSTED PO3917NOV.exe
Imagebase:	0xf70000
File size:	963072 bytes
MD5 hash:	EC46F95F234B89325E198104D1887B1C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.327703338.00000000015C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.327703338.00000000015C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000004.00000000.319379461.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.319379461.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000000.319379461.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000004.00000000.319379461.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000004.00000000.321459100.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.321459100.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000000.321459100.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000004.00000000.321459100.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000004.00000000.317402875.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.317402875.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000000.317402875.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000004.00000000.317402875.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.327531363.00000000015CA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.327531363.00000000015CA000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000004.00000000.316730524.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.316730524.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000000.316730524.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000004.00000000.316730524.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000003.327615222.000000000159F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000003.327615222.000000000159F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.327638100.00000000015C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.327638100.00000000015C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.327579370.00000000015B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.327579370.00000000015B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000000.319990653.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000000.319990653.000000000054F000.00000040.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000000.321513614.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000000.321513614.000000000054F000.00000040.00000001.sdmp, Author: Joe Security

- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000002.554723844.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000002.554723844.000000000054F000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000000.318229472.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000000.318229472.000000000054F000.00000040.00000001.sdmp, Author: Joe Security
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000004.00000000.319952873.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.319952873.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000000.319952873.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 00000004.00000000.319952873.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000004.00000000.318207568.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000000.318207568.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000000.318207568.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 00000004.00000000.318207568.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.327676957.00000000015CA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.327676957.00000000015CA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000004.00000000.319416601.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000000.319416601.000000000054F000.00000040.00000001.sdmp, Author: Joe Security
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000004.00000002.554668873.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.554668873.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000002.554668873.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 00000004.00000002.554668873.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.327479352.00000000015A5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000004.00000003.327479352.00000000015A5000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities — Show Windows behavior

File Opened

File Created

File Deleted

File Written

File Read

File Attributes Queried

Other File Operations

Volume Information Queried

Device IO

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Key Opened

Key Created

Key Value Created

Key Value Queried

COM Activities — Show Windows behavior

WMI Operations

Mutex Activities — Show Windows behavior

Mutex Created

Process Activities — Show Windows behavior

Process Queried

Thread Activities — Show Windows behavior

Thread Created

Thread Terminated

Thread Information Set

Memory Activities — Show Windows behavior

Memory Allocated

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

Network Activities — Show Windows behavior

Socket bound

Socket connected

LPC Port Activities — Show Windows behavior

Chronological Activities

Disassembly

Code Analysis

Analysis Process: ADJUSTED PO3917NOV.exe PID: 5404 Parent PID: 3608 ADJUSTED PO3917NOV.exe COMMON

Executed Functions

Function 0121C3E8, Relevance: 6.1, APIs: 4, Instructions: 127 THREAD COMMON — Download Yara Rule

Function 0121C3F0, Relevance: 6.1, APIs: 4, Instructions: 120 THREAD COMMON — Download Yara Rule

Function 0121A0F0, Relevance: 1.7, APIs: 1, Instructions: 197 COMMON — Download Yara Rule

Function 02E90AAC, Relevance: 1.6, APIs: 1, Instructions: 120 COMMON — Download Yara Rule

Function 02E90AB8, Relevance: 1.6, APIs: 1, Instructions: 113 COMMON — Download Yara Rule

Function 01215344, Relevance: 1.6, APIs: 1, Instructions: 101 COMMON — Download Yara Rule

Function 01213E18, Relevance: 1.6, APIs: 1, Instructions: 96 COMMON — Download Yara Rule

Function 02E93070, Relevance: 1.6, APIs: 1, Instructions: 93 COMMON — Download Yara Rule

Function 0121C610, Relevance: 1.6, APIs: 1, Instructions: 69 COMMON — Download Yara Rule

Function 0121C618, Relevance: 1.6, APIs: 1, Instructions: 62 COMMON — Download Yara Rule

Function 0121A551, Relevance: 1.6, APIs: 1, Instructions: 55 LIBRARY COMMON — Download Yara Rule

Function 01219460, Relevance: 1.6, APIs: 1, Instructions: 55 LIBRARY COMMON — Download Yara Rule

Function 0121A2D0, Relevance: 1.5, APIs: 1, Instructions: 47 COMMON — Download Yara Rule

Function 02E90CF8, Relevance: 1.5, APIs: 1, Instructions: 46 COMMON — Download Yara Rule

Function 02E90D00, Relevance: 1.5, APIs: 1, Instructions: 44 COMMON — Download Yara Rule

Non-executed Functions

Function 0121F2D0, Relevance: .3, Instructions: 315 COMMON — Download Yara Rule

Function 0121CE74, Relevance: .3, Instructions: 265 COMMON — Download Yara Rule

JoeSandbox Cloud BASIC

Analysis Process: ADJUSTED PO3917NOV.exe PID: 1328 Parent PID: 5404 ADJUSTED PO3917NOV.exe COMMON

Executed Functions

Function 0040C1B2, Relevance: 36.5, Strings: 29, Instructions: 218 HDC COMMON	Download Yara Rule
Function 0040AC0A, Relevance: 28.4, APIs: 5, Strings: 11, Instructions: 406 HDC FILE STRING COMMON	Download Yara Rule
Function 0040A6C8, Relevance: 24.9, APIs: 4, Strings: 10, Instructions: 404 HDC COMMON	Download Yara Rule
Function 0040F80E, Relevance: 14.1, APIs: 4, Strings: 4, Instructions: 130 COM COMMON	Download Yara Rule
Function 046994E0, Relevance: 13.7, APIs: 9, Instructions: 151 COMMON	Download Yara Rule
Function 046D6B50, Relevance: 12.8, APIs: 1, Strings: 6, Instructions: 588 COMMON	Download Yara Rule
Function 0040CCB4, Relevance: 10.5, APIs: 3, Strings: 3, Instructions: 45 COMMON	Download Yara Rule
Function 0040562F, Relevance: 8.9, APIs: 3, Strings: 2, Instructions: 151 HDC NETWORK COMMON	Download Yara Rule
Function 0040CC54, Relevance: 6.0, APIs: 4, Instructions: 49 HDC ENCRYPTION MEMORY COMMON	Download Yara Rule
Function 046A42D0, Relevance: 5.7, APIs: 2, Strings: 1, Instructions: 486 COMMON	Download Yara Rule
Function 0040CAFC, Relevance: 4.5, APIs: 3, Instructions: 46 HDC MEMORY ENCRYPTION COMMON	Download Yara Rule
Function 00401085, Relevance: 3.0, APIs: 2, Instructions: 6 HDC MEMORY COMMON	Download Yara Rule
Function 04699970, Relevance: 1.5, APIs: 1, Instructions: 44 COMMON	Download Yara Rule
Function 0040F93F, Relevance: .1, Instructions: 89 COMMON	Download Yara Rule
Function 0040B67E, Relevance: 47.5, APIs: 10, Strings: 17, Instructions: 219 HDC LIBRARY COMMON	Download Yara Rule
Function 0040A0D8, Relevance: 33.4, APIs: 14, Strings: 5, Instructions: 160 HDC REGISTRY STRING COMMON	Download Yara Rule
Function 00413435, Relevance: 26.4, APIs: 11, Strings: 4, Instructions: 188 HDC REGISTRY STRING COMMON	Download Yara Rule
Function 0040E703, Relevance: 25.6, APIs: 1, Strings: 16, Instructions: 121 HDC COMMON	Download Yara Rule
Function 00411136, Relevance: 19.5, APIs: 4, Strings: 7, Instructions: 278 HDC FILE COMMON	Download Yara Rule
Function 04698D90, Relevance: 16.0, APIs: 7, Strings: 2, Instructions: 208 FILE COMMON	Download Yara Rule
Function 0040C118, Relevance: 14.1, APIs: 5, Strings: 3, Instructions: 56 HDC REGISTRY STRING COMMON	Download Yara Rule
Function 0040C4A8, Relevance: 12.6, APIs: 4, Strings: 3, Instructions: 371 HDC FILE COMMON	Download Yara Rule
Function 0041290F, Relevance: 12.4, APIs: 4, Strings: 3, Instructions: 138 HDC COM COMMON	Download Yara Rule
Function 0040B559, Relevance: 12.3, APIs: 1, Strings: 6, Instructions: 54 HDC LIBRARY COMMON	Download Yara Rule
Function 00402CEC, Relevance: 10.6, APIs: 4, Strings: 2, Instructions: 107 HDC STRING COMMON	Download Yara Rule
Function 004099A8, Relevance: 10.5, APIs: 2, Strings: 4, Instructions: 38 HDC LIBRARY COMMON	Download Yara Rule
Function 04697820, Relevance: 9.1, APIs: 6, Instructions: 79 FILE COMMON	Download Yara Rule
Function 004057FB, Relevance: 9.1, APIs: 6, Instructions: 75 HDC NETWORK SYNCHRONIZATION COMMON	Download Yara Rule
Function 0040CBA8, Relevance: 9.1, APIs: 6, Instructions: 73 HDC FILE MEMORY COMMON	Download Yara Rule
Function 00409D9A, Relevance: 8.8, APIs: 3, Strings: 2, Instructions: 34 HDC REGISTRY COMMON	Download Yara Rule
Function 046DA880, Relevance: 7.4, APIs: 1, Strings: 3, Instructions: 430 COMMON	Download Yara Rule
Function 0469E600, Relevance: 7.3, APIs: 2, Strings: 2, Instructions: 317 COMMON	Download Yara Rule
Function 046A4DF0, Relevance: 7.3, APIs: 1, Strings: 3, Instructions: 283 COMMON	Download Yara Rule
Function 0040B203, Relevance: 7.3, APIs: 1, Strings: 3, Instructions: 252 HDC COMMON	Download Yara Rule
Function 004055A5, Relevance: 7.1, APIs: 1, Strings: 3, Instructions: 52 HDC NETWORK COMMON	Download Yara Rule
Function 00405CE2, Relevance: 6.1, APIs: 4, Instructions: 55 HDC COMMON	Download Yara Rule

Function 00411E21, Relevance: 6.0, APIs: 4, Instructions: 48 HDC FILE COMMON	Download Yara Rule
Function 004047EA, Relevance: 6.0, APIs: 4, Instructions: 46 HDC COMMON	Download Yara Rule
Function 0040FBFC, Relevance: 6.0, APIs: 4, Instructions: 37 HDC COMMON	Download Yara Rule
Function 046A4060, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 155 COMMON	Download Yara Rule
Function 0040FCB8, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 65 HDC REGISTRY COMMON	Download Yara Rule
Function 00405A10, Relevance: 4.7, APIs: 1, Strings: 2, Instructions: 156 HDC SLEEP COMMON	Download Yara Rule
Function 0040CED9, Relevance: 4.6, APIs: 2, Strings: 1, Instructions: 54 HDC COMMON	Download Yara Rule
Function 004035E5, Relevance: 4.5, APIs: 3, Instructions: 23 HDC STRING COMMON	Download Yara Rule
Function 00409F71, Relevance: 3.5, APIs: 1, Strings: 1, Instructions: 23 HDC COMMON	Download Yara Rule
Function 0040FA1F, Relevance: 3.5, APIs: 1, Strings: 1, Instructions: 12 HDC COMMON	Download Yara Rule
Function 00410FC3, Relevance: 3.1, APIs: 2, Instructions: 56 HDC REGISTRY COMMON	Download Yara Rule
Function 00403554, Relevance: 3.1, APIs: 2, Instructions: 54 HDC COMMON	Download Yara Rule
Function 0041106C, Relevance: 3.0, APIs: 2, Instructions: 47 HDC REGISTRY COMMON	Download Yara Rule
Function 00405EC5, Relevance: 3.0, APIs: 2, Instructions: 16 HDC COMMON	Download Yara Rule
Function 00411D0C, Relevance: 3.0, APIs: 2, Instructions: 14 HDC SLEEP COMMON	Download Yara Rule
Function 00401F76, Relevance: 3.0, APIs: 2, Instructions: 12 HDC THREAD COMMON	Download Yara Rule
Function 00410283, Relevance: 3.0, APIs: 2, Instructions: 8 HDC SYNCHRONIZATION COMMON	Download Yara Rule
Function 00405EEE, Relevance: 3.0, APIs: 2, Instructions: 6 HDC MEMORY COMMON	Download Yara Rule
Function 00405EFF, Relevance: 3.0, APIs: 2, Instructions: 6 HDC MEMORY COMMON	Download Yara Rule
Function 00405F53, Relevance: 3.0, APIs: 2, Instructions: 6 HDC MEMORY COMMON	Download Yara Rule
Function 0040309D, Relevance: 2.6, APIs: 2, Instructions: 53 HDC COMMON	Download Yara Rule
Function 00413936, Relevance: 1.6, APIs: 1, Instructions: 143 COMMON	Download Yara Rule
Function 046F3550, Relevance: 1.6, APIs: 1, Instructions: 139 COMMON	Download Yara Rule
Function 0469D4E0, Relevance: 1.6, APIs: 1, Instructions: 100 COMMON	Download Yara Rule
Function 046FA982, Relevance: 1.6, APIs: 1, Instructions: 52 MEMORY COMMON	Download Yara Rule
Function 0469DD80, Relevance: 1.5, APIs: 1, Instructions: 36 COMMON	Download Yara Rule
Function 0040F481, Relevance: 1.5, APIs: 1, Instructions: 30 HDC COMMON	Download Yara Rule
Function 0040F76B, Relevance: 1.5, APIs: 1, Instructions: 28 HDC COMMON	Download Yara Rule
Function 00410F6E, Relevance: 1.5, APIs: 1, Instructions: 28 HDC REGISTRY COMMON	Download Yara Rule
Function 004031D4, Relevance: 1.5, APIs: 1, Instructions: 27 HDC COMMON	Download Yara Rule
Function 0040FC7E, Relevance: 1.5, APIs: 1, Instructions: 26 HDC COMMON	Download Yara Rule
Function 00403272, Relevance: 1.5, APIs: 1, Instructions: 25 HDC COMMON	Download Yara Rule
Function 00403335, Relevance: 1.5, APIs: 1, Instructions: 25 HDC STRING COMMON	Download Yara Rule
Function 004058D3, Relevance: 1.5, APIs: 1, Instructions: 23 HDC NETWORK COMMON	Download Yara Rule
Function 00401F4B, Relevance: 1.5, APIs: 1, Instructions: 21 HDC THREAD COMMON	Download Yara Rule
Function 0040FDA5, Relevance: 1.5, APIs: 1, Instructions: 20 HDC COMMON	Download Yara Rule
Function 00410298, Relevance: 1.5, APIs: 1, Instructions: 15 HDC SYNCHRONIZATION COMMON	Download Yara Rule
Function 0040FF0B, Relevance: 1.5, APIs: 1, Instructions: 12 FILE COMMON	Download Yara Rule

Function 0040F71F, Relevance: 1.5, APIs: 1, Instructions: 8 COMMON — Download Yara Rule

Function 046F7FF2, Relevance: 1.5, APIs: 1, Instructions: 3 COMMON — Download Yara Rule

Function 004109D2, Relevance: 1.3, APIs: 1, Instructions: 95 MEMORY COMMON — Download Yara Rule

Function 0040CA78, Relevance: 1.3, APIs: 1, Instructions: 53 COMMON — Download Yara Rule

Function 00410969, Relevance: 1.3, APIs: 1, Instructions: 49 STRING COMMON — Download Yara Rule

Function 00404E5B, Relevance: 1.3, APIs: 1, Instructions: 46 SLEEP COMMON — Download Yara Rule

Function 0040CB67, Relevance: 1.3, APIs: 1, Instructions: 30 MEMORY COMMON — Download Yara Rule

Function 00405E22, Relevance: 1.3, APIs: 1, Instructions: 17 MEMORY COMMON — Download Yara Rule

Function 00409FCE, Relevance: 1.3, APIs: 1, Instructions: 9 COMMON — Download Yara Rule

Function 00405EB4, Relevance: 1.3, APIs: 1, Instructions: 6 MEMORY COMMON — Download Yara Rule

Non-executed Functions

Function 004089D5, Relevance: 45.8, APIs: 17, Strings: 9, Instructions: 286 HDC KEYBOARD COMMON — Download Yara Rule

Function 0040A29A, Relevance: 31.8, APIs: 9, Strings: 9, Instructions: 296 HDC REGISTRY COMMON — Download Yara Rule

Function 004130B3, Relevance: 29.9, APIs: 12, Strings: 5, Instructions: 119 HDC FILE STRING COMMON — Download Yara Rule

Function 0040D508, Relevance: 17.6, APIs: 9, Strings: 1, Instructions: 55 HDC SERVICE SLEEP COMMON — Download Yara Rule

Function 0040DA5B, Relevance: 14.2, APIs: 7, Strings: 1, Instructions: 167 HDC SERVICE STRING COMMON — Download Yara Rule

Function 04698C40, Relevance: 14.1, APIs: 7, Strings: 1, Instructions: 105 WINDOW COMMON — Download Yara Rule

Function 004079E8, Relevance: 14.1, APIs: 7, Strings: 1, Instructions: 97 HDC INJECTION MEMORY THREAD COMMON — Download Yara Rule

Function 00409DF6, Relevance: 14.1, APIs: 6, Strings: 2, Instructions: 61 HDC FILE COMMON — Download Yara Rule

Function 0040D49C, Relevance: 12.3, APIs: 6, Strings: 1, Instructions: 52 HDC SERVICE COMMON — Download Yara Rule

Function 004118BA, Relevance: 10.5, APIs: 5, Strings: 1, Instructions: 48 HDC REGISTRY COMMON — Download Yara Rule

Function 004120B8, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 45 HDC PROCESS COMMON — Download Yara Rule

Function 046F5FCC, Relevance: 7.6, APIs: 5, Instructions: 58 COMMON — Download Yara Rule

Function 046A8720, Relevance: 7.4, APIs: 2, Strings: 2, Instructions: 401 COMMON — Download Yara Rule

Function 0041002B, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 90 HDC COMMON — Download Yara Rule

Function 0040A632, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 62 HDC MEMORY ENCRYPTION STRING COMMON — Download Yara Rule

Function 046997E0, Relevance: 6.1, APIs: 4, Instructions: 70 TIME COMMON — Download Yara Rule

Function 0040F56D, Relevance: 6.1, APIs: 4, Instructions: 63 HDC MEMORY COMMON — Download Yara Rule

Function 046A5B40, Relevance: 5.6, APIs: 1, Strings: 2, Instructions: 369 COMMON — Download Yara Rule

Function 0469BCD0, Relevance: 5.4, APIs: 2, Strings: 1, Instructions: 196 COMMON — Download Yara Rule

Function 0040B15E, Relevance: 4.6, APIs: 3, Instructions: 61 HDC STRING ENCRYPTION COMMON — Download Yara Rule

Function 0040F619, Relevance: 4.6, APIs: 3, Instructions: 60 HDC COMMON — Download Yara Rule

Function 0040D418, Relevance: 3.1, APIs: 2, Instructions: 57 HDC COMMON — Download Yara Rule

Function 046B3030, Relevance: 1.6, APIs: 1, Instructions: 127 COMMON — Download Yara Rule

Function 046B4D50, Relevance: .2, Instructions: 157 COMMON — Download Yara Rule

Function 00419172, Relevance: .1, Instructions: 93 COMMON — Download Yara Rule

Function 046B4EE0, Relevance: .1, Instructions: 53 COMMON — Download Yara Rule

Function 046B4C40, Relevance: .0, Instructions: 50 COMMON — Download Yara Rule

Function 046B50E0, Relevance: .0, Instructions: 31 COMMON	Download Yara Rule
Function 046B52D0, Relevance: .0, Instructions: 27 COMMON	Download Yara Rule
Function 046B4FF0, Relevance: .0, Instructions: 25 COMMON	Download Yara Rule
Function 046B4CC0, Relevance: .0, Instructions: 22 COMMON	Download Yara Rule
Function 00410620, Relevance: .0, Instructions: 20 COMMON	Download Yara Rule
Function 046B4CF0, Relevance: .0, Instructions: 17 COMMON	Download Yara Rule
Function 046B4D20, Relevance: .0, Instructions: 17 COMMON	Download Yara Rule
Function 046B4B90, Relevance: .0, Instructions: 17 COMMON	Download Yara Rule
Function 046B4C20, Relevance: .0, Instructions: 16 COMMON	Download Yara Rule
Function 046B4F70, Relevance: .0, Instructions: 11 COMMON	Download Yara Rule
Function 0041094E, Relevance: .0, Instructions: 11 COMMON	Download Yara Rule
Function 00410619, Relevance: .0, Instructions: 2 COMMON	Download Yara Rule
Function 0040902E, Relevance: 40.5, APIs: 22, Strings: 1, Instructions: 277 HDC REGISTRY STRING WINDOW COMMON	Download Yara Rule
Function 0040E3FA, Relevance: 35.2, APIs: 9, Strings: 11, Instructions: 237 HDC REGISTRY COMMON	Download Yara Rule
Function 004095AA, Relevance: 33.5, APIs: 16, Strings: 3, Instructions: 214 HDC WINDOW STRING REGISTRY COMMON	Download Yara Rule
Function 00411AB9, Relevance: 31.6, APIs: 12, Strings: 6, Instructions: 90 HDC SLEEP REGISTRY STRING COMMON	Download Yara Rule
Function 0040882F, Relevance: 26.4, APIs: 11, Strings: 4, Instructions: 135 HDC WINDOW STRING FILE COMMON	Download Yara Rule
Function 00408E66, Relevance: 24.6, APIs: 13, Strings: 1, Instructions: 147 HDC FILE STRING COMMON	Download Yara Rule
Function 0040EAFB, Relevance: 24.6, APIs: 13, Strings: 1, Instructions: 135 HDC PIPE THREAD COMMON	Download Yara Rule
Function 04692C00, Relevance: 23.1, APIs: 6, Strings: 7, Instructions: 366 COMMON	Download Yara Rule
Function 046980B0, Relevance: 21.3, APIs: 9, Strings: 3, Instructions: 299 FILE COMMON	Download Yara Rule
Function 04699340, Relevance: 21.1, APIs: 14, Instructions: 140 COMMON	Download Yara Rule
Function 0040D58D, Relevance: 19.3, APIs: 10, Strings: 1, Instructions: 71 HDC SERVICE COMMON	Download Yara Rule
Function 0040DCB2, Relevance: 17.6, APIs: 4, Strings: 6, Instructions: 111 HDC REGISTRY COMMON	Download Yara Rule
Function 04699020, Relevance: 16.6, APIs: 11, Instructions: 127 SLEEP FILE COMMON	Download Yara Rule
Function 046ABCB0, Relevance: 14.3, APIs: 1, Strings: 7, Instructions: 311 COMMON	Download Yara Rule
Function 04698970, Relevance: 12.5, APIs: 5, Strings: 2, Instructions: 212 COMMON	Download Yara Rule
Function 00402961, Relevance: 12.4, APIs: 6, Strings: 1, Instructions: 108 HDC PROCESS THREAD COMMON	Download Yara Rule
Function 004119C9, Relevance: 12.3, APIs: 5, Strings: 2, Instructions: 49 HDC REGISTRY STRING COMMON	Download Yara Rule
Function 00411A3C, Relevance: 12.3, APIs: 6, Strings: 1, Instructions: 46 HDC COMMON	Download Yara Rule
Function 00411855, Relevance: 12.3, APIs: 5, Strings: 2, Instructions: 38 HDC REGISTRY STRING COMMON	Download Yara Rule
Function 00405CA3, Relevance: 12.3, APIs: 3, Strings: 4, Instructions: 20 HDC LIBRARY LOADER COMMON	Download Yara Rule
Function 00410D24, Relevance: 12.2, APIs: 8, Instructions: 164 HDC PROCESS COMMON	Download Yara Rule
Function 04697C80, Relevance: 12.1, APIs: 8, Instructions: 140 FILE SLEEP COMMON	Download Yara Rule
Function 046D7270, Relevance: 10.7, APIs: 1, Strings: 5, Instructions: 205 COMMON	Download Yara Rule
Function 00412D0A, Relevance: 10.7, APIs: 3, Strings: 3, Instructions: 168 HDC COM COMMON	Download Yara Rule
Function 046991B0, Relevance: 10.6, APIs: 7, Instructions: 137 COMMON	Download Yara Rule
Function 00407948, Relevance: 10.6, APIs: 5, Strings: 1, Instructions: 64 HDC SLEEP PROCESS MEMORY COMMON	Download Yara Rule

Function 00407CB7, Relevance: 10.5, APIs: 3, Strings: 3, Instructions: 33 HDC LIBRARY LOADER COMMON	Download Yara Rule
Function 00409ADF, Relevance: 9.2, APIs: 6, Instructions: 229 HDC FILE COMMON	Download Yara Rule
Function 04698500, Relevance: 9.2, APIs: 6, Instructions: 195 FILE COMMON	Download Yara Rule
Function 04698780, Relevance: 9.2, APIs: 6, Instructions: 164 FILE COMMON	Download Yara Rule
Function 046F6E64, Relevance: 9.1, APIs: 6, Instructions: 98 COMMON	Download Yara Rule
Function 046FA43A, Relevance: 9.0, APIs: 6, Instructions: 47 COMMON	Download Yara Rule
Function 046BD4A0, Relevance: 9.0, APIs: 1, Strings: 4, Instructions: 264 COMMON	Download Yara Rule
Function 046AD660, Relevance: 9.0, APIs: 3, Strings: 2, Instructions: 229 COMMON	Download Yara Rule
Function 00410B2A, Relevance: 8.8, APIs: 1, Strings: 4, Instructions: 61 HDC WINDOW COMMON	Download Yara Rule
Function 00411936, Relevance: 8.8, APIs: 4, Strings: 1, Instructions: 55 HDC MEMORY STRING COMMON	Download Yara Rule
Function 04697FD0, Relevance: 7.6, APIs: 5, Instructions: 82 FILE SLEEP COMMON	Download Yara Rule
Function 046996B0, Relevance: 7.6, APIs: 5, Instructions: 72 LIBRARY COMMON	Download Yara Rule
Function 046978D0, Relevance: 7.6, APIs: 5, Instructions: 72 FILE COMMON	Download Yara Rule
Function 04697980, Relevance: 7.6, APIs: 5, Instructions: 70 FILE COMMON	Download Yara Rule
Function 046F6757, Relevance: 7.6, APIs: 5, Instructions: 68 COMMON	Download Yara Rule
Function 046976F0, Relevance: 7.6, APIs: 5, Instructions: 53 COMMON	Download Yara Rule
Function 04697680, Relevance: 7.6, APIs: 5, Instructions: 51 COMMON	Download Yara Rule
Function 00410C79, Relevance: 7.5, APIs: 5, Instructions: 44 HDC PROCESS COMMON	Download Yara Rule
Function 04697760, Relevance: 7.5, APIs: 5, Instructions: 42 COMMON	Download Yara Rule
Function 046FA19E, Relevance: 7.5, APIs: 5, Instructions: 34 COMMON	Download Yara Rule
Function 0040B9A9, Relevance: 7.5, APIs: 5, Instructions: 25 HDC COMMON	Download Yara Rule
Function 0040B627, Relevance: 7.5, APIs: 5, Instructions: 25 HDC COMMON	Download Yara Rule
Function 046A0860, Relevance: 7.3, APIs: 1, Strings: 3, Instructions: 288 COMMON	Download Yara Rule
Function 046A6BF0, Relevance: 7.2, APIs: 1, Strings: 3, Instructions: 233 COMMON	Download Yara Rule
Function 0040FA42, Relevance: 7.1, APIs: 2, Strings: 2, Instructions: 135 HDC LIBRARY LOADER COMMON	Download Yara Rule
Function 0040F33C, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 54 HDC NETWORK COMMON	Download Yara Rule
Function 00413251, Relevance: 7.0, APIs: 2, Strings: 2, Instructions: 48 HDC STRING COMMON	Download Yara Rule
Function 0040F3BD, Relevance: 7.0, APIs: 3, Strings: 1, Instructions: 47 NETWORK COMMON	Download Yara Rule
Function 0040F4CE, Relevance: 7.0, APIs: 2, Strings: 2, Instructions: 28 HDC LIBRARY LOADER COMMON	Download Yara Rule
Function 0040F51D, Relevance: 7.0, APIs: 2, Strings: 2, Instructions: 24 HDC LIBRARY LOADER COMMON	Download Yara Rule
Function 00410C36, Relevance: 7.0, APIs: 2, Strings: 2, Instructions: 21 HDC LIBRARY LOADER COMMON	Download Yara Rule
Function 0040D17D, Relevance: 6.3, APIs: 5, Instructions: 92 HDC COMMON	Download Yara Rule
Function 04697AA0, Relevance: 6.1, APIs: 4, Instructions: 95 FILE COMMON	Download Yara Rule
Function 04697620, Relevance: 6.0, APIs: 4, Instructions: 40 COMMON	Download Yara Rule
Function 046975C0, Relevance: 6.0, APIs: 4, Instructions: 37 COMMON	Download Yara Rule
Function 0040EA89, Relevance: 6.0, APIs: 4, Instructions: 35 HDC THREAD SYNCHRONIZATION COMMON	Download Yara Rule
Function 046AB410, Relevance: 5.6, APIs: 1, Strings: 2, Instructions: 312 COMMON	Download Yara Rule
Function 046A8E10, Relevance: 5.5, APIs: 1, Strings: 2, Instructions: 286 COMMON	Download Yara Rule

Function 046A58C0, Relevance: 5.5, APIs: 1, Strings: 2, Instructions: 224 COMMON	Download Yara Rule
Function 046A3A90, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 197 COMMON	Download Yara Rule
Function 0469C4D0, Relevance: 5.4, APIs: 2, Strings: 1, Instructions: 182 COMMON	Download Yara Rule
Function 046A65F0, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 173 COMMON	Download Yara Rule
Function 046A3290, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 173 COMMON	Download Yara Rule
Function 046E9320, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 147 COMMON	Download Yara Rule
Function 046A36E0, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 146 COMMON	Download Yara Rule
Function 0469F620, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 142 COMMON	Download Yara Rule
Function 0469EEC0, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 138 COMMON	Download Yara Rule
Function 00407AF1, Relevance: 5.4, APIs: 1, Strings: 2, Instructions: 120 HDC COMMON	Download Yara Rule
Function 046AD450, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 93 COMMON	Download Yara Rule
Function 046A0760, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 88 COMMON	Download Yara Rule
Function 0040DE1F, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 60 HDC REGISTRY COMMON	Download Yara Rule
Function 0040D9B6, Relevance: 5.3, APIs: 1, Strings: 2, Instructions: 56 HDC REGISTRY COMMON	Download Yara Rule