ID: 514608
Sample Name: ADJUSTED PO3917NOV.exe
Cookbook: default.jbs
Time: 13:23:15
Date: 03/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

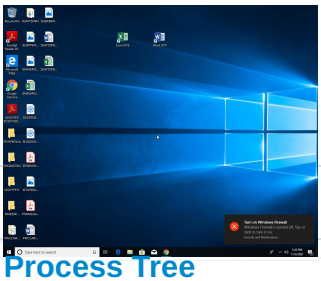
Windows Analysis Report ADJUSTED PO3917NOV.exe

Overview

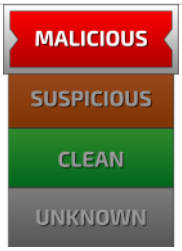
General Information

Sample Name:	ADJUSTED PO3917NOV.exe
Analysis ID:	514608
MD5:	ec46f95f234b893..
SHA1:	d0600cdb17f86f3..
SHA256:	01bbef21bea94b6.
Tags:	exe warzonerat
Infos:	

Most interesting Screenshot:



Detection



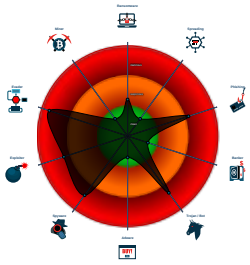
AveMaria UACMe

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

Signatures

- Yara detected AntiVM3
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Uses schtasks.exe or at.exe to add …

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	
00000004.00000000.319379461.000000000400000.00000040.00000001.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

Source	Rule	Description	Author	Strings
00000004.00000000.319379461.000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000000.319379461.000000000400000.00000040.00000001.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				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Exploits:

Yara detected UACMe UAC Bypass tool

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected AveMaria stealer

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Contains functionality to hide user accounts

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Contains functionality to inject threads in other processes

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected AveMaria stealer

Tries to steal Mail credentials (via file / registry access)

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

Contains functionality to steal e-mail passwords

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality:

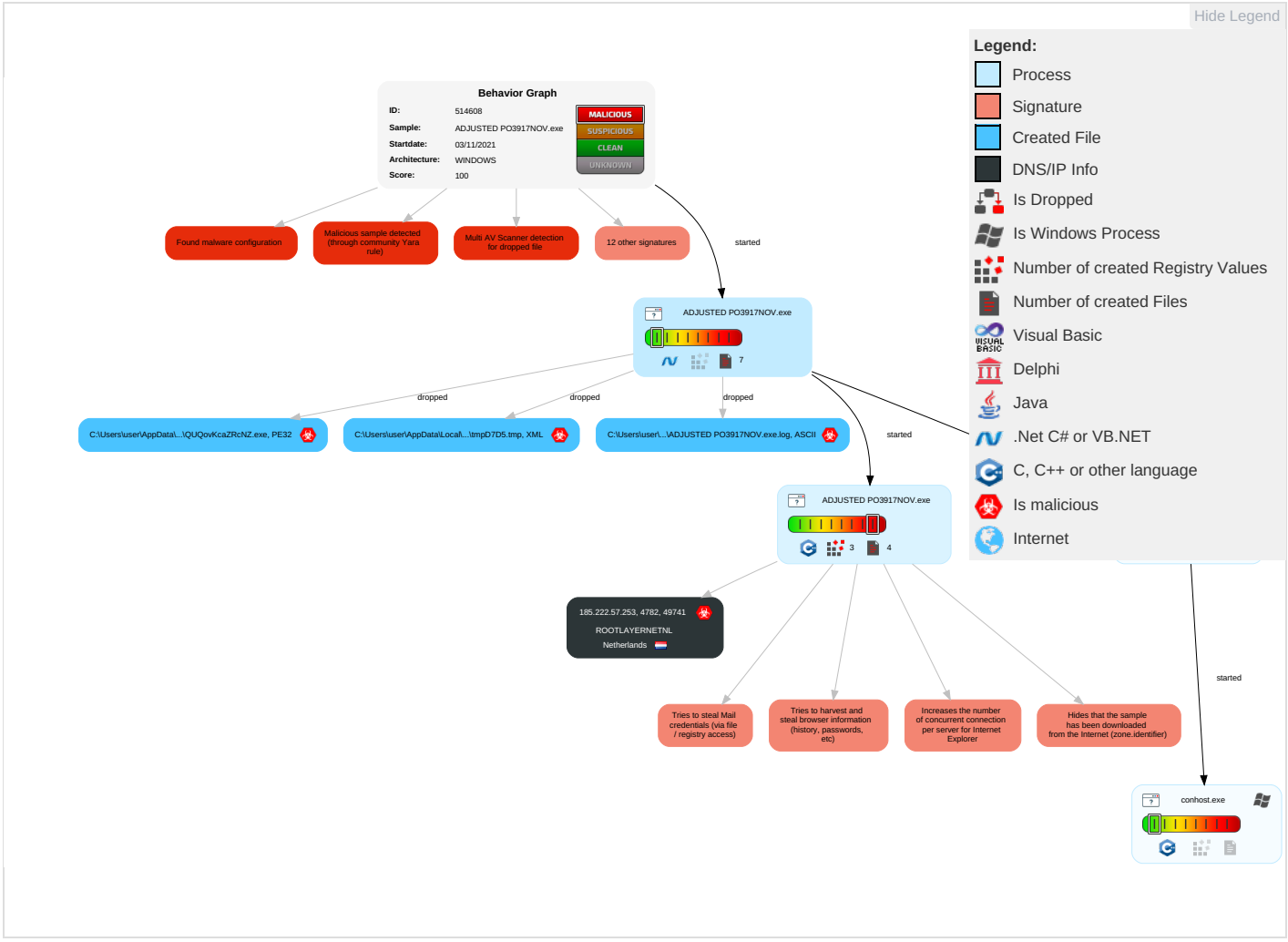
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commar and Con
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 T Transfer
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	Encrypte Channel
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-Star Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commar and Cor
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	Applicatic Layer Protocol
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
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 Commun
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	Common Used Por
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	Applicatic Layer Pro
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 Prot
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 Trans Protocols

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
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.comitudl	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	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

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:	light
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: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:24:17	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
	Q4EtLThkYlEkFvu.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
	RHK098760045678009000.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
	Payment Supplier.xlsx	Get hash	malicious	Browse	• 185.222.57.85
	BULK ORDER #RFQ REF R2100131410.exe	Get hash	malicious	Browse	• 45.137.22.70

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

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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ADJUSTED PO3917NOV.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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	
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/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBgAPtn:cbh47TlNQ//rydbz9I3YODOLNdq3yy
MD5:	1C1A65CA91C09759C032BDB8A9D63E5D
SHA1:	99404B26FCF77D27761690D71EEDB2C2B41B8755
SHA-256:	14C38D65AA4C38350AD298E9742BC7982B635FF0D82C1B973710D84BAFB53C2E
SHA-512:	9ACF01FDBC35568D22E53C21723C1B4EFB488EEC84E17B8444823A628F5D09EDEA04EEFF76A3A524C0C8C050D2CE819FABB6DA845767B531F260614C72B165I 8
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	
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+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU: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	
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+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234

C:\Users\user\AppData\Roaming\Knptwsn.tmp	
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
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":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Roaming\QUQovKcaZRcNZ.exe	
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+4dZN0lTwI:Kk/DeV5YTZHPTesTW5JF4MN4dU1wI
MD5:	EC46F95F234B89325E198104D1887B1C
SHA1:	D0600CDB17F86F31EFF130D029A87717FDE2CC7A
SHA-256:	01BBEF21BEA94B6EC60C739DF3E40E887CF0EA1DF7BA2F1678CE708BA10A6203
SHA-512:	C3207A8C9C4639A40AD72308C7AA6710C78C4AC014704CF6675AD7D724CFDBA9D7A0AFD292E7B133EEB964342A1B0988A6CFC8C24D0EB84A43787405227968B
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.....+... ...@....@.. ....@.....D+..O....@.. ....H.....text..... ....`.rsrc... ....@.....@..@.relo c.....@..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	
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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
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

General

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+4dZN0lTwI:Kk/DeV5YTZHPTesTW5JF4MN4dU1wI
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
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6181EE70 [Wed Nov 3 02:05:36 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	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

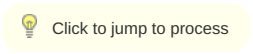
Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior



System Behavior

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

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 Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3244 Parent PID: 5404

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

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

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

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

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: 00000004.00000003.327551592.000000000159F000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000004.00000003.327551592.000000000159F000.00000004.00000001.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 Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis