ID: 501907
Sample Name:
YdACOWCggQ.exe
Cookbook: default.jbs
Time: 11:58:25
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

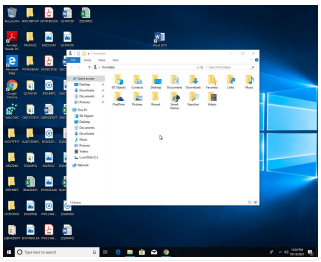
Windows Analysis Report YdACOWCggQ.exe

Overview

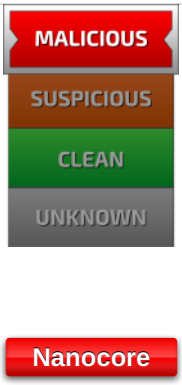
General Information

Sample Name:	YdACOWCggQ.exe
Analysis ID:	501907
MD5:	b866823e1f8f4a5..
SHA1:	fe99849ec276304.
SHA256:	ebe1bb18a77cf0b.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



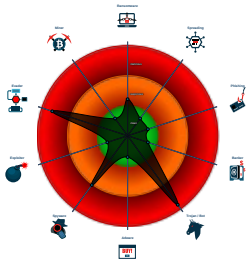
Nanocore

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

Signatures

- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected AntiVM autoit script
- Yara detected Nanocore RAT
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: Bad Opsec Default…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Hides that the sample has been dow…
- Uses schtasks.exe or at.exe to add …
- Uses dynamic DNS services

Classification



Process Tree

- **System is w10x64**
- YdACOWCggQ.exe (PID: 4896 cmdline: 'C:\Users\user\Desktop\YdACOWCggQ.exe' MD5: B866823E1F8F4A52376BD108C457DD78)
  - mmuiqlcvwo.pif (PID: 5828 cmdline: 'C:\Users\user\33920049\mmuiqlcvwo.pif' fmkkelc.omp MD5: 8E699954F6B5D64683412CC560938507)
    - RegSvcs.exe (PID: 6240 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 6272 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpB828.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6348 cmdline: C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
    - conhost.exe (PID: 6364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c213d282-998c-4a04-8f80-944681ca",
  "Group": "nano stub",
  "Domain1": "ezeani.duckdns.org",
  "Domain2": "194.5.98.48",
  "Port": 8338,
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.784677096.000000000629 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000E.00000002.784677096.000000000629 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000E.00000002.784677096.000000000629 0000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000003.300093094.000000000436 4000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7e5:$x1: NanoCore.ClientPluginHost • 0xf822:$x2: IClientNetworkHost • 0x13355:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000003.300093094.000000000436 4000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 54 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.3.mmuiqlcvwo.pif.43c9268.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
8.3.mmuiqlcvwo.pif.43c9268.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
8.3.mmuiqlcvwo.pif.43c9268.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
8.3.mmuiqlcvwo.pif.43c9268.4.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
14.2.RegSvcs.exe.6290000.8.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 65 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Nanocore RAT

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking:

Uses dynamic DNS services

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Drops PE files with a suspicious file extension

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM autoit script

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

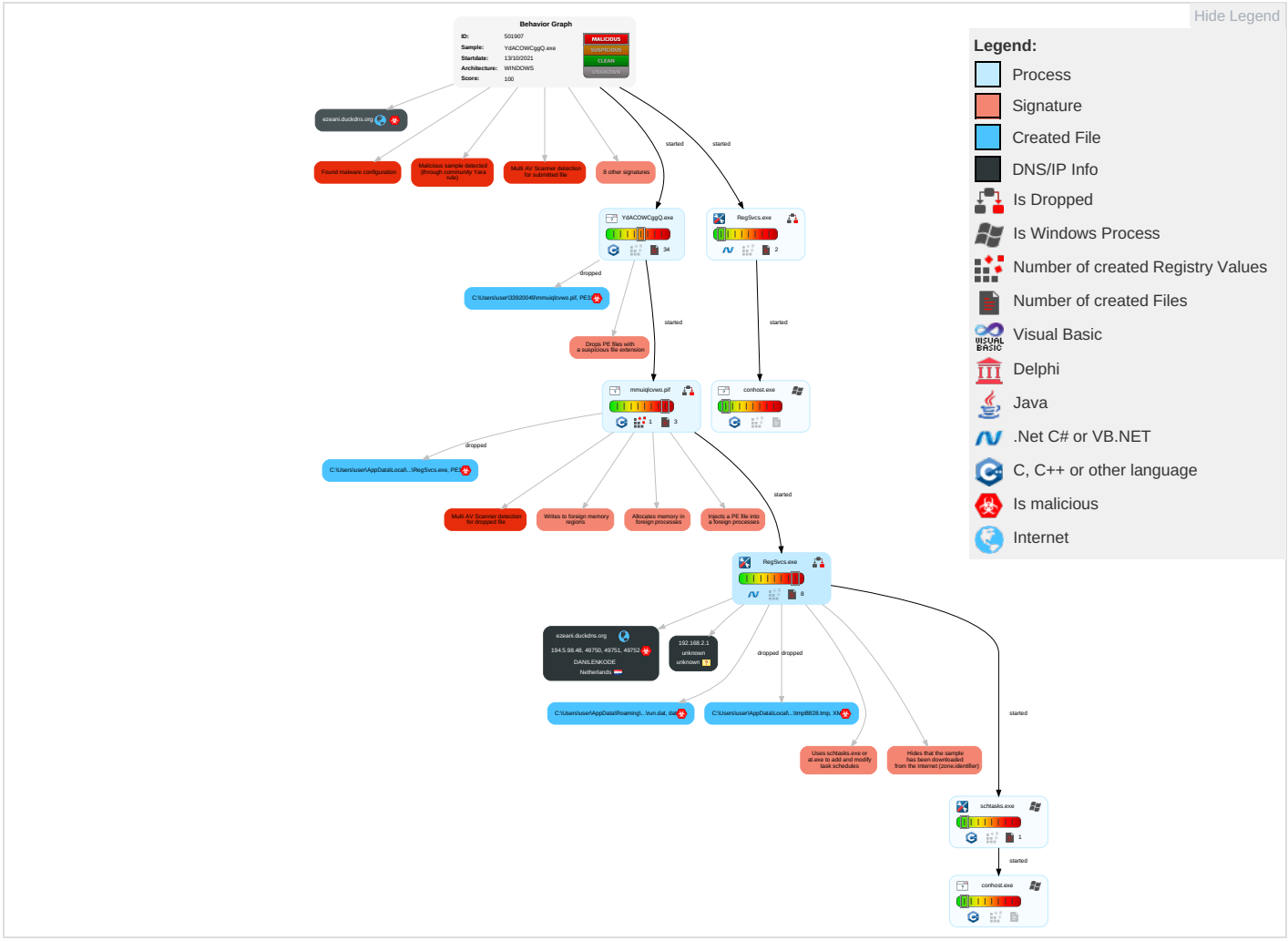
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 2	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	Input Capture 3 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingres Trans
Default Accounts	Command and Scripting Interpreter 2	Valid Accounts 2	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 3 1	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Valid Accounts 2	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Non-S Port
Local Accounts	At (Windows)	Logon Script (Mac)	Access Token Manipulation 2 1	Software Packing 1 2	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remo Acces Softw
Cloud Accounts	Cron	Network Logon Script	Process Injection 3 1 2	DLL Side-Loading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Non-Applic Layer Proto
Replication Through Removable Media	Launchd	Rc.common	Scheduled Task/Job 1	Masquerading 1 1	Cached Domain Credentials	Security Software Discovery 1 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applic Layer Proto
External Remote Services	Scheduled Task	Startup Items	Startup Items	Valid Accounts 2	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 2 1	/etc/passwd and /etc/shadow	Application Window Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail F

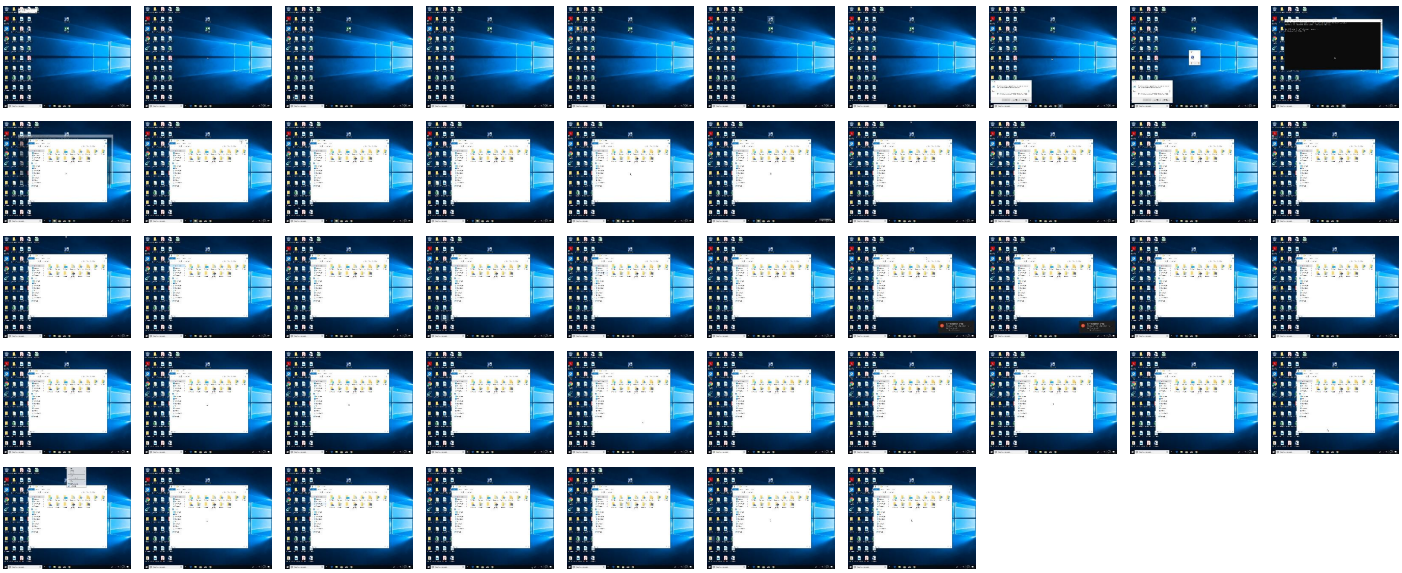
Behavior Graph



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
YdACOWCggQ.exe	35%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\33920049\mmuiqlcvwo.pif	27%	Virustotal		Browse
C:\Users\user\33920049\mmuiqlcvwo.pif	32%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.RegSvcs.exe.6290000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
14.2.RegSvcs.exe.1300000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
ezeani.duckdns.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	URL Reputation	safe	
ezeani.duckdns.org	1%	Virustotal		Browse
ezeani.duckdns.org	0%	Avira URL Cloud	safe	
194.5.98.48	1%	Virustotal		Browse
194.5.98.48	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ezeani.duckdns.org	194.5.98.48	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ezeani.duckdns.org	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
194.5.98.48	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.48	ezeani.duckdns.org	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501907
Start date:	13.10.2021
Start time:	11:58:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YdACOWCggQ.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:	34

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/36@23/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.6% (good quality ratio 22.4%) • Quality average: 74.6% • Quality standard deviation: 28.1%
HCA Information:	• Successful, ratio: 55% • 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 • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:59:55	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Windows element C:\Users\user~1\33920049\MMUIQL~1.PIF C:\Users\user~1\33920049\fmkkelc.omp
12:00:00	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
12:00:00	API Interceptor	1890x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.48	Import order764536.xlsx	Get hash	malicious	Browse	
	Bill of Lading, Invoice, & Packing LIsts.exe	Get hash	malicious	Browse	
	Quotation Price - Double R Trading b.v.exe	Get hash	malicious	Browse	
	Nizi International S.A. #New Order.exe	Get hash	malicious	Browse	
	DHL Import Clearance #U2013 Consignment #6225954602.exe	Get hash	malicious	Browse	
	soa5.exe	Get hash	malicious	Browse	
	soa5.exe	Get hash	malicious	Browse	
	PO SKP 149684.jar	Get hash	malicious	Browse	
	TECHNICAL OFFERS.exe	Get hash	malicious	Browse	
	17New P.O_signed.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ezeani.duckdns.org	Import order764536.xlsx	Get hash	malicious	Browse	• 194.5.98.48

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	Import order764536.xlsx	Get hash	malicious	Browse	• 194.5.98.48

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	swift.Telex.xls	Get hash	malicious	Browse	• 194.5.98.95
	details.vbs	Get hash	malicious	Browse	• 194.5.98.206
	TWAueCcfK3.exe	Get hash	malicious	Browse	• 194.5.98.107
	DHL_1012617429350,pdf.exe	Get hash	malicious	Browse	• 194.5.97.16
	Enquiry- 0076HGF21.exe	Get hash	malicious	Browse	• 194.5.98.141
	DHL_1012617429350,pdf.exe	Get hash	malicious	Browse	• 194.5.97.16
	1012617429350,pdf.exe	Get hash	malicious	Browse	• 194.5.97.16
	AWB# 2617429350,pdf.exe	Get hash	malicious	Browse	• 194.5.97.16
	Product-inquiry6243424243_PDF.exe	Get hash	malicious	Browse	• 194.5.98.211
	Charter Details.vbs	Get hash	malicious	Browse	• 194.5.98.184
	VHp0AIIIQG.exe	Get hash	malicious	Browse	• 194.5.98.107
	Product-inquiry6243424243PDF.exe	Get hash	malicious	Browse	• 194.5.98.211
	Yeni Sipari#U015f # 765-3523663, pdf.exe	Get hash	malicious	Browse	• 194.5.97.16
	Nuevo pedido _WJO-001,pdf.exe	Get hash	malicious	Browse	• 194.5.97.16
	765-3523663 ,pdf.exe	Get hash	malicious	Browse	• 194.5.97.16
	Zhgafxcfrzzlbcdvuklhrmxvmcufzxktju.exe	Get hash	malicious	Browse	• 194.5.98.145
	Zhgafxcfrzzlbcdvuklhrmxvmcufzxktju.exe	Get hash	malicious	Browse	• 194.5.98.145
	Yfqbmuahufznqznknlmwfrtnauqppwcobt.exe	Get hash	malicious	Browse	• 194.5.98.145
	BIOBARICA OC CVE6535 TVOP-MIO 10(C) 2021,pdf..exe	Get hash	malicious	Browse	• 194.5.97.25

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	Swift copy.exe	Get hash	malicious	Browse	
	KRSEL0000056286.JPG.exe	Get hash	malicious	Browse	
	tT5M57z8XiwLwf5.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Suspicious.Win32.Save.a.7200.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	21ITQXL080104122T7.exe	Get hash	malicious	Browse	
	COSCOSH SHANGHAI SHIP MANAGEMENT CO LTD.exe	Get hash	malicious	Browse	
	319-7359-01#U00a0BL#U00a0DRAFT.exe	Get hash	malicious	Browse	
	HSBc20210216B1.exe	Get hash	malicious	Browse	
	BANK INFORMATION.exe	Get hash	malicious	Browse	
	PO.2100002.exe	Get hash	malicious	Browse	
	dorlla.exe	Get hash	malicious	Browse	
	dAkJsQr7A9.exe	Get hash	malicious	Browse	
	QT2021154 NCX Glasurit Rev.1.exe	Get hash	malicious	Browse	
	Order specification & Drawing_PDF.exe	Get hash	malicious	Browse	
	payment.exe	Get hash	malicious	Browse	
	SWIFT CODE.exe	Get hash	malicious	Browse	
	SWIFT CODE.exe	Get hash	malicious	Browse	
	TRANSFER REQUEST FORM.exe	Get hash	malicious	Browse	
	swift code.exe	Get hash	malicious	Browse	
C:\Users\user\33920049\mmuiqlcvwo.pif	Import order764536.xlsx	Get hash	malicious	Browse	
	KRSEL0000056286.JPG.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\33920049\aauo.exe	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	512
Entropy (8bit):	5.6047097806645825
Encrypted:	false
SSDEEP:	12:o9RRQXCGiB+IGihOZEkUYz8laDkucQq1wA3RT8jTW:oPRuCh8OEZEdwkucZ1w2T8jS
MD5:	3A48081CF7D4D709399A376B3A8AADF2

C:\Users\user\33920049\aauo.exe	
SHA1:	E0D7DDAA464FC3565D92DF4ECC7BD30286D519CA
SHA-256:	7EBB903522348C2326DFFBC66B5D20C8E7C120C4D7CEE15640CAE5187C5741C0
SHA-512:	4B0077AD1E29FC4C7703B7525167ABB1A80E409D7E4685EA977689B3DE12CF5CFA02BB843D62E1EA391F18FF4C609D66262116E01B52C59616E3A266F0E40726
Malicious:	false
Reputation:	low
Preview:	7Wq2t660muPw9Ke6505108Nqr733V3ey4715Mnl1tK584..xy2u6f8997C1l72Xc9877f5666UgJI88f50gM5PSiht354AzpPmC0fL6TsXG1K41vO4Dkm9..46tjB20c7L BG210W860g694jFP6918666lmHe1c7XI71YIljgi5hp12J0oQ690a15cD60yD7KVgw047u4j6A41klBxn2Ok2L386Lb22mMFoB69F2..P213L3BW17Qa6OT37d10A3N36J 105N6dvVEJiz4h0aj833P18x910LvnZ655s06IFlBf63Gu5HKO28ErrHC5b09mo2vq..z4D72VM..Sz42896scdb7kPgw0qW6q81vF8..0D5lF..m4zAR10BO6Yk8M..5B GR826P42tCT1t73Hk261Pcqliz7AoTir59j..661Qb74gOprMNMaV9FBPR0TzEQ6H92poW22LHCzotRBEn3R97T2So4F0113007zgj459pt6JBRy1w4p8HlK..

C:\Users\user\33920049\abjtjj.gcm	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	416786
Entropy (8bit):	4.0000117868606
Encrypted:	false
SSDEEP:	6144:vq8GcfPnL6mYkonW8inBO9SEmDafe/kgtwIf:vecfPemYZWJs9NmDaW8gmG
MD5:	1E44C5E2D839F53AC114916DFA41912B
SHA1:	9B67ABC94E2959683B5D784C8B076D6171AF7237
SHA-256:	0FB93824D410F1E4BA2B233F405027D042EDF2E729FA34A41BE910B50ED99416
SHA-512:	14895D2F67585415D7D25807BBA20F6AA8C142E8DD3483ED8E10F4280820CD0849EE828E3134BEAF4A90FB8E41C9C524DF01547330DFD3928470B3EEB95946A1
Malicious:	false
Preview:	263C9AF54DD4BF4F7E0C5198D2227687C93C7661722FE3BF313F3C309BC6DA5B7DCF8CC2FD93519BEEA48BC3F85F444A4DC6F35EE0C7421245FE1ED2 9C939140AA744D02294CC3133D1C4574F4178BD44CABBB3E1D4DECD39B635890338BB701862A32E1DF18C77C1467AFA0EE1A1C0E2FE212F58868971A 359F1A0051337BA3E49B4186689F644914CC0532EE1E2191D02B5E967124EFC714F108E42312A57BB206933E0D80F0CE85016C65EF6DEF77E6D282FE DA01C7C5E87E75884D5A2A071F0DAD2F068C403C58342FBB1992E8429411FBC7D211702D5B2CC25840B6745D5C4DCD998E61535598AB03F837F91DAC F69F1A8AB681C1844FFB4E72BA0239829E8F3869CC79BAC6D3FFB9D0B99DF07443F914D0114D8E543D012146B2FBEC7553587031F90693C06F307664 E5579F5452330E0CDED3F23714F20E723C950FC3ED17E97CECB51E98E8DB4CC1FC9BB79E0373AC4964FD9AB88DE32AEECEF0EF35F9C084A95125E107 5C7930534E78DF5AD151E0E61ED15DE7C3CFDA715AE279046B90370787F52959A2A2EBDC6291A89D9CAA296B7EDEAE91A9695B2B35498AB1161165F6 FB3C07DF2A46F51CBA870B02A83E0DEB4AD17E5FD212878466CFDCA81948E75C1B58BF293B55CC6C7D17EBADD267142649CB9C7D745346164549A751 534E975FE2AE562BE19C67669A149FC6FA4F74F3

C:\Users\user\33920049\aricevnrq.msc	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	605
Entropy (8bit):	5.421101092464615
Encrypted:	false
SSDEEP:	12:/wP7JBvQ76cFT1DeNWO+9EjcJujbW/e8Rz9ZoPgIA6+1mpkfwLD:/gJBQzF0NWlvmEeYBmgI7+1qLD
MD5:	AE35EB6B3B57EEB5BED5821AA2E6D92D
SHA1:	9D8C94DEF5AE1D05D727E19EFF0A55917094DD67
SHA-256:	565B05521D79388A417C7210739CFC5EB4F8E41E50D0D76D6710FE7533FF4B98
SHA-512:	7A1F352907FA7D9BA4B414331EF15B9CDE5949744CA7BB47EF5AE68D03391512E80308DF06B82B4FF54746C3A06EF9A2E590CE7331BC9107EB66CE257F73FB63
Malicious:	false
Preview:	08Z3h01TYEDB7juv33IVTN5363Bm3x58X99O3qk6hF7UILvA93I5x2B34m55pQbb86qi61jSmmo01y7L78Gwfs9C56D785gw679242F1769ed446vL0jU59bEkk5..1395 w9H2420o41EHZ37Q5H625u59KgkGl4KJluL189E3l40DpWwl4h7TMm76R29z5b96tsEc5j6DiN0..vZ06s6R0Y4d0yWO1..4w156A660bZ5wtP8wq8CQk08f56Y0434Ke2 w16Fb34b123Xy8172qUfZGDs18wBj3H22yc456ZNg39Htm4t8Ht1C..0pOZe952HYIt0eiF989Ha59NxD930kMRbd46n2oJ99C0nZ844U18X5t5W989E3U3t751387Y573 08372635fg3AgBF77355T8m19upI7tk5g8kp854rBT451470..07L1594RI53310x74fd3QH8Y28a6b..n321hoQ..14EY338q0CU1353Bi29mK5aLq46FR5g62fKj027u 487718wB49X72539654H1904u67y65v0541Dvh3577feFfN3UBF27ie2zx9Jf50r66194x7h4Z3r895w8Lo..

C:\Users\user\33920049\bbofcjswrb.bmp	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.395393519734533
Encrypted:	false
SSDEEP:	12:gIhpZX8zRyjfRafC1Pmu/r6V7w5TSKocSZVjjkrK+zlEVBIy:gIhpV89ESeFp2xVjAG+zl0BF
MD5:	152ACD87F50B620928B85D1F6EA00588
SHA1:	5A704ED20090C635BC28A71A343FFF741F482D06
SHA-256:	B8F8B30B8BFDFE6E4EBA9D663264F8DE1FEC9A94B1530E0DC13001953324DDEE
SHA-512:	CB312CF46E681121EF1B75F723405FC5A0C243AD44E027F115DDF578E8B639B080127FA133FE69D3367983CEA1677879276F3BABD89B5DD904F5528545E4C6E2
Malicious:	false

C:\Users\user\33920049\bbofcjswrb.bmp	
Preview:	h2d4pGf54q2132P42FX65o8122rw2M3584rBd5j277l6g409G48j794253kT80z6470FejY94Dw56HJi347A2d332d4uTYn75X96o340J4iE822y4dc5D4304zhwy0w6is 08ur6600cqe259OHm2157u48UI99..jGj2b8N89e24f771RD59L8oR83p5d304m1u74w420ABk2706a6LiN0pdSCl673r..S9k2NF75MmH737cH45o9t2JmF04Yuj6wr23 X340r01375VJRod..47ztV9lZ6642J9T86nN11ama6680j741Zy74850R526m7foe8N36q6XO74z8l8sE77..a0oP0Tm3J014NEBb612H6LEj31ZgMPw592740nm95n4uG P65f9SkpNzJ8D8fN..64728i4M47R06Tx796zShlGl0dy4fF70doY6Pc1k6mMnk1YQL81Ehqueh0T6j9026XNNyOO8gsZTL6c059e2wRe702ye39u115W2..

C:\Users\user\33920049\dngb.txt	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	628
Entropy (8bit):	5.539990812470243
Encrypted:	false
SSDEEP:	12:WEMHRgaG7Oq6Rypby91dT2XV8vyy9SqSOQn9KtzFwTPSMJw7PYV7xy:DMx1G7SRyRE1dSFtyYZiGTPSMq7PK1y
MD5:	7F801B2F630068DE6D4B7F9358261246
SHA1:	9F1FA78880CC820B11BF4F50FAF02B47E717F0B8
SHA-256:	2BDC81B1E28470666DB0FB6E23AA590C4B9CA2E251170DEB506FAD164B8ADD4A
SHA-512:	5C0CAD366569BD1B221ADD033A111A2A5B17A117CB199BA3DBCDE4BFD6F2038815E8EFED40FADCA9D805A63CEC0CC8BD12CF6F50C1BD57F9AFC991E5F25A EAA5
Malicious:	false
Preview:	74442u09G0N700Yq4ygAEEd300Cirh39..5273lTr5QsO75A..7yf1L9G32D8w751Wrq2gD62o43eS9MGe1kA32FSnu0l54Ri5347718mTeNeX7eZw5s4ED16V46S2tMV5 2im5UYBh1r57nk0vQ458i7a31885RP..u68l00495g68lZ8094W221Mjk03894g..63efV24by8V0g21U2L2atYc7gH1r8j938D569M9k301KoKXBu6c6Z7S7d527A22SX 6p5w0Xp608062792k68y80jXoW6FYi74P7HtH9oBxVof35r3..Uw60247993a6ZtbU3rUB7b13D4YGwC8Ks24xb4ee9L5Av1yLU9Y6z28rD9ZY356G2K2..Sa1f5KYsA47 ymA6388zJ6MSQpk7z75at005PrR61eL9t69b50dMqu35r15v7lH0a96o0i82OqofPg712Ky1y2..IWC85L..B3916i4cD9906Z381tW6xJz7W1b841rXpa8P45EA6NEg97 71V5R2Y25r693Xm83Y7epLAYL9k4VSfd3DhI1623XpI50Wh6bWay3FlL53Iapo095whR8km7Q57ZW26K66LbdKnv19G49y8tt5SpW3182k..

C:\Users\user\33920049\dopnobhqej.xml	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	574
Entropy (8bit):	5.3882957771470705
Encrypted:	false
SSDEEP:	12:IynViaAcFBLGDlBRqNZJC2Q/nrsAF6eCyh3kOIiEuP8G:WcfMYw2OrMd+3kOpEPG
MD5:	9F6E0D61C826AC091CD857D118713477
SHA1:	327C7FD7ED8AA08C09C104FFC7BA15894C25424A
SHA-256:	44269193851D3CEA2ABBADCD4DF83DEF02397189A74E239D0719D9D2F69BA8FC
SHA-512:	63038CB3D42BA8A0C20957F2D67719217FE00A6A85EDB18C837F4779160AE65B32F3D7BEA9814CCD02CB90CF92B8027C20D2524647C66CC36B31B9FC45C98D1
Malicious:	false
Preview:	M041g15259W98w2l84hDJ792g0OKe81MI1U47G340a9G63763N5193G6Nc4T8ij6yd79z90pq8541P04z84KX01v81Ou6eMR81xMh090i14Pm5Hx0hU3Xq6801b23z570c eDt1c640oeh4244IPxC0za0l6P3o9hT9..q8zuT464596Q..ynjZ10Si95D9p9034wD9rPG923e3w64MQ9Om4x9MD4o6a48c5E42XH7YN93Zd4C3O047KH9G4uBv8467jw 79X247D488M68701X2623..rdxd928740r5285uh4O3XoT9h9e54e2p0z06n0l9e2a926Utsx1qU2Qa3U02l6a7899457K81gd61732WrdAY3200GYumf7drDy7Ip99ty9 7b8F..n24xt9nJT0572D5r5xn9BEWP5P6f777R832..rX0QU14dS95q46eqjM36PI6w787q48gU7Q4F84d12TD2Z11UM5ukFf46lo2kTf41613syARA7W6Gd6y4n3769tM 50jdC9LF2t423b78LK86y96pNpeBu7NP0zI58l597209030I039g..

C:\Users\user\33920049\dwipjhaqq.jpg	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	565
Entropy (8bit):	5.568775268532097
Encrypted:	false
SSDEEP:	12:puQF5w4r+LqEcY2/ioIPKtpzzFgOv+7rg0/ScUocADn2:wQ3rrDwoIymO2YrcyAa
MD5:	A36CB4828F8264BF744ABAA2F8842B53
SHA1:	1E0B2BF80891B29BD078129A90364B14ED95EE57
SHA-256:	1F7F52165714243C75171CCDA40E5E0C66F8B6EEE59C2F224B9C5033A7D32FE0
SHA-512:	4032EA58CFB0B2A1B333D306A43AF6F1BE6FF8342F09F22AFC6072F601C903174D8CBA893C71984AC7814548B27C6B3CC4FFF5C046408E96C96397CD4003B057
Malicious:	false
Preview:	4M3h0Rw700K2tH81iPVxYFL3yaj81c5f7fP3..ToG0A6WwPam6R08..Rz3011XwEl9..P5qb48A64ON490387i5X0z3ICKLY58pNWLy6C8a999W28x18D..VaF2691v5FQ Umw1N9FMxvtV18f84c024218TK0tLX3VUhNP3R8852e45ve4lj4V6Rq2P3i27T1dB7a6ER6q5OE4O8c9IYA4e3v1d1501yFIL44XJG56qp0uIjV3Z2j15041p9S65663rW dm2k45Zn3O..51O8y4lP9217QAlu4dD4H4413281mm170962OGMTtv3c35G38P31o62MGo5r9zx24j81b9IsWJ50LUM3Hm9fYF46nC1kQ269UM0gB8t52w4i5072t6CQ6A 177DB9EUHF7h4IIR0fv3pn7xI5NUfiY5C97A5..59EYK388Y9Mhe35GYGR50L94yRB..f7k39qWX4t5F0G4f6B828I88X7F6q5gY6CT9n607902ja2x01L7LyD47s98dZl 7fz0mR2SuH26Sk108E322n61oo6G60332k4bV59f6NF..

C:\Users\user\33920049\eeppjmhbj.icm	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\33920049\eeppjmhbj.icm	
Category:	dropped
Size (bytes):	593
Entropy (8bit):	5.516485008605424
Encrypted:	false
SSDEEP:	12:Xo6hrLh4fvDosoUkZajbPcdHcOgRsSHesaKEQWSTdoT6rQpWvn:X5rL6/oEbPcFcOgG6esafShz6Wvn
MD5:	4050A7160604551C4CB625F60086536C
SHA1:	4110CAFA390AE23E74DC5B110CE98F0C3B342CF2
SHA-256:	8AE0F3572F5B03EFA9C93C88E62F61DF4C59341817BD5E883E7B0D48A82B2346
SHA-512:	75335BDE6AE3B4D4DA060FB425E02965B62CB6DCBB52EEA6F52CC071AFA8ADBD0176687230123F850FB6D097ED36357ED283C2707ED15006E5719AA24CD588B
Malicious:	false
Preview:	67iuCF1c4N85L87b7KKDTk67ry6XW8L7njzq45q283zYDp4w8l67msr0do972..52XQ488PfD7P020634s937H3By8yE..O8HcogrgwKop7s837c56g6KRN5j2RU98K6I26SoNZ..841236lv1941K3jac2N6v4ABA538Z1l28BUY9hKwv9cf6Fq3U20tSm68b8J6j4wc46G250JS99203M03h00ZqFlyH7M5752330LNS19B8170T0r4rITz2DH7KdvVX5..2oVq5659S7238u0CCY9NKU2bjc74g2s7fRkn1VM0jcwFW212w1cCs21l53B46249aW2584tVm71T452ZafB..L60ze680022X4Vf7zrW120az1G6Wa8Nh337RDbt9h9s0MQFiP..93B3Jbk51F3646kSd7A4t9X78P0pZ93Zwg3075RJ763EXT296F3JllnYQEFSJ69E6..BHPU8K32y1338b67Y6qe9694X6M31H302673N53N4n66L7G5tU9znqkBB5c0PH46472d3SATD3iygGP711Z328x1X550821387q906jv3aMd66h8A5reS8Y739K..

C:\Users\user\33920049\egwevtj.xl	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	570
Entropy (8bit):	5.5477291315599615
Encrypted:	false
SSDEEP:	12:/kIF2BqahGlKUEq4YCQeFq20TD6QlfkL8GCuKLB6wWem+HixRnoQ84qsK84:sIIEdltFb93L8Gwqe/0oHP84
MD5:	B8B1C71088CA6B30B3029554CE05CEF8
SHA1:	67D1C180AA7C8B079819F9013828827947456D29
SHA-256:	A5FC7DBE940C698DE68E900516AE4EA33BC7B7AB2435C0D5B74E9E474A58A09E
SHA-512:	C262AC053268459F8800BF3F7BD219E0C0DFA063D12D1EF96D563EE60F337C99AA0FC69496A535975A0B682AA732C0C1741D2748D4ED783E2C2E0D0ECA65D01
Malicious:	false
Preview:	xjv7HSA9163Q94401EarUCp317HVZ826n0u1334J4s99160l09Iu7Oq0lqU20Y3O7hlu4038164bq13rl65aPJ1C4hqnDAwx0IxYKS5s0458gtY0Im8C7w55W9n04Vz3Y15oA2Knz7qLEX6n043E1Q0j5OC357p..jK2283TuR..SC9g4uT5XpwmR..1h909j4F555Bn86iNvPyV2N0BY70IET344F4U6471ecr5v45WO9K72J81Ky3..dxi4tbs70w..OAAoH5h70347vEz05dpRR9n390G1XK57Y4ati87p44y7K199frf1bVs118mW3709JB385uk33sl80at12cP9qSmmPa0k3097fg50itw7Yo3..0ghuk8K85Al809..1U4k778WgW10jK6l907rAUW1wA109l8fjl3TH2R9t32s112iTt8466T77S1ob5vI6jIW250RuuW8miX960BmWd1z66vG8332n8f4S68p492a3Bj7dH78hryje2uw8auR8w2C3918Z5OjD9f6dXr4T6bUxU4wj3K51MtR98gN350Z272S8WmXBt..

C:\Users\user\33920049\ewkvwqles.xl	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	545
Entropy (8bit):	5.527751285637128
Encrypted:	false
SSDEEP:	12:enqYhOyfzX8x2nPPegEhlSDu30ExDkHHiD/Gn0:uqYhpfAxSGhlSy30ExKH6O0
MD5:	A7864C4D1F211A09CB7BCDB60FC1BB9C
SHA1:	06CD14C958FA5C0870C3148BCD874208D6EBA192
SHA-256:	D3BEFD3CD87AA43091B2043616C0D57B5DD5C86A9BBB933BC7F1CE359FDF2848
SHA-512:	3659FAB569E5D7FF8F509EF2B0B2385EBD80114CD1ED782B19A440131FAB50EB6AB489A9A274503BB08751B5173E97E81B8931047DC1F6B7C440558B80AB34F2
Malicious:	false
Preview:	6NK42n6r92q74lD845rJVr4ZDDPa7dqi672tQ1Mh0ma5hE5W127e40U8D4d6q4K157NCE5PR0pC9W5M1707r9k2gC4P8E5kZU486ZdBEizbh02X0S8D5095fx1b732t229q4J37ws686oEKo09p9t6017lT0P0oRd..Y5AIzxe0GL7y4o6apa42dji73791I1..xyzf4j39l852K5Y77cI5fN36Z2CqG8q3H..rZZ15D93u3yvm0Q355u9Q4PyJ2aL2787FF6XCb5a0b..YJkR5hE93i1z421qF0TqJv01e17cQVG4WWm3b63pr9hSJz8Hnv242t02e1P8k78F86L3R24578r65lL7Q72301s4wxN9at0Wff5w9B04rN9mf5cDh..W83G0vc1xyM774C52aFH1m35GIP12q1w43qanvHm972Qax458NkghP5Xp20342ZUef3F5nfOZzx15c57q597304H1h463szzL532y02575nVXBm490A8243701393R7HP0R4XdAn88RU1b3n175Gv84qN6..

C:\Users\user\33920049\fmkkelc.omp	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	151163464
Entropy (8bit):	7.076418205558757
Encrypted:	false
SSDEEP:	49152:EcAALhfk8v8UOvPpDnYZVOCzhK2BE1Mnu8oQLpzEwE5AhbaSpqX+FST+CJtIJlz6:A
MD5:	66D7B16F566AD4D6F73CD6083C7B1D51
SHA1:	C71715B2546908A05A28A91555534F04BDF11432
SHA-256:	440D3B688F65BD11C021206C50D7B7C4A75C7BA66BD2E1AA4137ABE65D41079A

C:\Users\user\33920049\fmkkelc.omp	
SHA-512:	7EE084C1DA1AABE2F7FCC084B4A9C5A9E5CFB86FB4FD45BC6EE08CD3E67FE41380D8FA0F0F312EC50198DC50CE230E36127EF5931ED455D9CE61EFBD43E1A0CA
Malicious:	false
Preview:	..;...q...I*.&..m.y.....7.e.....?..h.5.....R.I.V..wq.....0..../f.x7;...J;t...)_.1....P~....Y.....q..F.....qA.....[.....#.c.s..N..s.....)..G.....i..oB.-..Ll..S.AN...p....=..]I?qzO.*:.H..-.?..KH.. .....]...T..z{...mkQ_b$.Ld....g...S.zX.mT...Q....y..W....(EdK_.....U.....8l\,...d.kZ..{P.;!svF.....T.".vX.*...^.O.....g..LJC`.V..b..%....LG.....H`-..=....T.s.s.v..-....*...C.....!....(.Q.I.... .%Zb..:!.'..'.L.b.P..'EZ..:..Y!...?...j&..J{k..?;a...'j.~=M...N@....2.wVN2..L>.....7.$.y0.....sr.kt.j....Z.E.....4)/.P.>.D-..}z...3?.RqXNZ..a..l..P...*w..(8.s8Em.)?.bs...L.....vNg..... .....D....Y.. .H...(5Rvv>._.Ax.....4..~?.../)z.....gq.,8...5..s..M.6....IN..<.....y..l.*G...lv.1..je>1b....W.OB..4.Q..."...2>.X...@.9S.. .qj...R.n.3...?D.h.B..e.ES.79.Z...Y6i....Q. ..8.b.....i.5.8.2.7.e.....4.A..x.&.)g.....C.wS!k..P....5~Cw....j.D....v.....6.3.G.K.N.7.n.w.2.0.n.e.0.j.c.9.n.9.5.9.6.4.e.8.z.Q.H.k.4.2.s.7.Q.m.J.j.....ax.....e

C:\Users\user\33920049\ggaoddlfq.pdf	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	581
Entropy (8bit):	5.484135377500105
Encrypted:	false
SSDEEP:	
MD5:	97DB150F517B42A67914B55B9FCC0855
SHA1:	53FA78E1F13BB71038D02D9C8911415B5C2912C5
SHA-256:	D4FC9603286BC88744BDA31D71B8464EA7CAB510244B3C21128774513302BFC8
SHA-512:	545A19B01D8423099C1CB414B4754E10C7C1A98ABA50BBEB7330B82843BEA877DB761156CA6B306EC4A67954CAF1E9C0493E0722BB6345B19CD8678E6A7BD532
Malicious:	false
Preview:	L60IP8VyXr8j652U7c4EA16q506Yc267O5B7n4W6d9EC6Wr..Z5233jgEHS42S8jkR620DAZ8w68m60520LFT9bEhlgC9mDpBzH845DF60..1y528jK2RP5V39890u00G3 624K55R112O0W6073G86rY4ADPJ0L23378Rb24UXE3H97g2MHvXD93aS29..j80ANqDzZO2kb9125241S33538C7w606w6v35BFaiy1l46Tk2Vt052qKd2nR7r29pFl8L. .GwNQ1wcq3EG2WHRg58C4yriBtymd40H4dUHL247P9o3VdRAI267l371CPXW0v98Su8a73XEsIz746545XG7yOqe64Z5Y00j82g24j4q02Pj159YQq08UQ8..417n1LPG3 O9nb41794272W58hcC2Hyv38L91361m1z74TMlz16EMi3mbdjD3394B8Z3k99u92322eXEr1..Dp706GD6R69y836495M79uL245i5P9508eX256K24ao04S25B18167xL pZ09h47Vd4bf3QrqzPKU5T65ynrizaEl10Q8Di30790619Pt215NEVV57Hl..

C:\Users\user\33920049\hmjc.jpg	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	582
Entropy (8bit):	5.508024577075607
Encrypted:	false
SSDEEP:	
MD5:	DCC53F5459120236A9DD260CBCC7CFFF
SHA1:	4039FCA91DD943A269B6180906E347F44E26AD45
SHA-256:	2DD6BC5BC770D576565692E8D014611ECE5614A615B83832756959163EDA3329
SHA-512:	AAF0B1864FA1353C8BE403BA257FC86E963AA1C5C6343CD83AC9B47F4D4AD0C4DFF12589C17E4BD0DB6F626C8446332BBFE87819E2ED37709DC1DCD59909D4A
Malicious:	false
Preview:	6TZgv2r6O98PiGO8Bh7NU14GOCk793S2T03rq31B0hy5OJ7PEoTnk815B9zq85mIvt29Y6Cg6SnKsBd489773Sj513K9gCIld8645479Z6dg75w0o2j3wR0Jd93k900Glz Nd..OhBWTv50bvjel9V8Hn1D8g608f604Dxp37E77B8xetl6R7uElCk8jpS5i7BkYNxA7jM6O90y9O..u267m58f5O8C2v0Aj692c2rh6X2l27Whby14k6p0n9A75RI64m 06ZTlZRG51Q0H2PPHx94iY1348z9K14W6Iy59y513dMFAUWZjxLF32714ZlP58n5S216w64v0pT5J..4c4W592OCU2498e97AP7tP54788328fF9dSY1k421Iq3810W4.. 64Kou07keHf2K103H901f4TS8x3594704LK009837n6v9380qA7U3qr2Zo30ZtjN3A9nv363EeO7StediyWh19s1665H9H8W4RKO01G3844fX40p6TkvnGwBGX7R3OWq20 t3e4l705e908r1c0WjO2213q3507e28y1u1Y7G7QT22g2YyO9X09hUm45sh5..

C:\Users\user\33920049\ipltm.pdf	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.404238302840432
Encrypted:	false
SSDEEP:	
MD5:	239B0A24A1A86CDB9E336BAFB9671B60
SHA1:	D604B815B4C5FC72E38700E060016980CD3F013C
SHA-256:	F71F990B573AA4CC7724769C08F9EF0FD5E3897FDEB567966323E1AA5C7AAF84
SHA-512:	8214623D1FAE28F7BE93CF1F762DF3BE8475331613FA1949B643D6A739FD5EA705789499E91D1A8CBD25FA8159F0450681EB2D3977B9B698B89D1332245DBE57
Malicious:	false
Preview:	27eVjsZhC09FTf59eg4E80Hf5aR9z867Do5C984995469Me62Kn3MYF72V58juX5QZ27Bt0X33295lds87mvzB7il1649F6481nWyJ1td54Pm758615wJ4e..xF3gqw4xE rwn85099L42448fh405T5702d7x2S52c53hL0Z33J61AQJr8I..GL2ASEC1268x1d1J76QK51jo8L3x108Bwz6781Zv35NbPkV30406BEK7CAY3GM123hS79z2xyL43769 e9Xr6h24u33U557S53334pT6h2Sqo6989..tbo1742YcZ1nE04NR1961860q1v42mVFGNL2d6JVa1683E48Mnl8d2r21D0MX10voM0X90oJY1A56383e4222a4P24SbPac 0N8E6S6q6ha78jnx2G4H2Q2CwF0988v8314H38JR..KlO082yx7r10VD80057Y6P9D9fY87Q98740R629c1YdL7Hs4w1N6w82T0jxa4KhC46522l4qX194gvn05t68u614 7O268Xz8Lw9T19N695oJ6S5F0x941..

C:\Users\user\33920049\kwhibpnou.exe	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	566
Entropy (8bit):	5.3766864975280875
Encrypted:	false
SSDEEP:	
MD5:	D60ADFE8CC5346DF0C2C5A191039AFB7
SHA1:	B2760A6B3E71AA9441F771A31FA7CAB80DDB792C
SHA-256:	4D5CB8CFF9DCC0F1536CAE9299295B4422F49B8377FDAA9057427AE40D74EB8B
SHA-512:	F7CD8F6FE84970944955343E5699BDFDB05174E9CEEB3AFE2ADA12B2F2BBED4B945E8B2D16B9B7AD1A796C37DA991E3B81F284076170805CD45665873411A76
Malicious:	false
Preview:	Qp7VxBTqkal64icS8B1C513riL6X0A6cB27O2Z932R4Bm1T2b3WzoQ96N0fp1M3x69f11t62o1Q7A488p0472QK4Wx9w56mx663h6n11n53e1ix194KNk295v2284mw0y09IPEXD37c6AFr5F344F13n81x88s2KlkM53Os9u0XE8868u..7EbC1ws0wR9778U88034J645l21Z16E8FTPp80U8MT38R3y9u4FY070R382sve8xJ99mOD7..10cKFw98468v6E5636uv3l17cv9r036kGr8aX142AqTx667e622Aa727A32rI43FDM31v1w0Uzxsn9r2Bm4afK0314D571B24T1U7651jp56r996515M7O0t501615782n371..64X27Ucy58l9Q2W2C0Px781420P2N59j2Y895PbAmu0De379MvT2Q50MA10421375xX6L0T475A8Y..1w4XSx8276T2594X2Q1b9q4632iU4qUR59C92Q4c3u8vn1zb6ubNyq1K050hmsbY0R99q31nV47xS6q5EHW1MTh4Jn3fz7r3BS..

C:\Users\user\33920049\lueww.jpg	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	5.509794522095491
Encrypted:	false
SSDEEP:	
MD5:	F25CE49283A8CBCDAE2F3D447B00DE0B
SHA1:	5ED22433392F6FBD1804EF94473CF465837575AD
SHA-256:	C6B4F1EA2A48D13050C20A3D4CC3614909E694B494037432610053DA675FC627
SHA-512:	2FAEBF76B5DDD7505BBBAD4B6ED730667BBCE856C10FD476E28607B0C41E409FC661360F39607D38F5E54AA5CB6B27403E9F54A3BD918AA127FB7AF55C0094D4
Malicious:	false
Preview:	q4KlYkM8K7KM9dTa2..O05bC2qu9fW2a3S91357EO2Uz4M59J55eL65tm397YG6o67d915gQlA7S741S9bY6RvSbdS71pC882XwPAEX..F5DbHvcLJ76H5W6S666gM1143f5va98ul5Zt4ET9FoD..86S7w19on3Oz1Fxjknb3q2f202289174u3Jq37K702OT52esq499w5P4657o551Gi2osU9cb63U3Lk492AY800101en9FTPtTqO46G63SM2Q8nT35k4868Tazzx3SoyYNO4..6J6852X5y89mY22Jg9L5NX10zryN2SYsk09235f1m8H6JMxz871G419XpAM5b86705530DKi7kcpF0..2XMT91Iri7qxaO30t39887Ux9J01jLDQ1eY3S4Q94q79qS749dz234mW2b9QN82j7ew0A6PM..iwW873592D8T8Y65VGfpr4uu7b0TaV99s02eZD6936q36147yvpG3606SL65Py0uR1s0Jg9332453UmkwD16JcTXNTM009r582856vE4QbVAKk..

C:\Users\user\33920049\lxvjfmbxgn.icm	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	529
Entropy (8bit):	5.417334677129549
Encrypted:	false
SSDEEP:	
MD5:	B8D1527AD41B6877D1B63609604A2114
SHA1:	831D9DB5D7ED05A8397EE8A3E34C35C3DC769CE0
SHA-256:	86DAACE3C786D9AA8BBDBDA09F69456A0260A20E5AB4CFE9A02628A73A9E0AA4
SHA-512:	15DFC12B02F3D8F10A1785BD192C1DB146B7CDF12AA1B1CBC30700F24DCFEAF333A117221C45BF65225B249F88A3506C77F57B2667DD50A851DAFD32DB604DC
Malicious:	false
Preview:	D1E8h2HEX937c5F63ws5Hy095U3mf9Y77980..V00K56s224Ejgp1J9M7f6Gf912RvvQr..01t27zB04..4ugwZb62895b42g5QFtR097yD5Ky9g34heCyxq5Y3h4Zm9qN8LwHQ89088680hKMCOCC0hBc05kRm3P28349HdnbADp7oi0I42O124eT5t6V995A3ruyCVG0f152985Ai1c3dP6UTPva89094B7q7Jq..B2j1v7152u912E6K1732305X05621350nS917217248LwXgyb9697H6juS6f58cbWuh8o7H3077542z5g02C22Aq9600q0L8r5EBo3841L87X99DA1KTJ5O4NR939Qg06l9ZF1z40L7v88a0901o..fT7815R486y0u9U514P824n89A9pN9587k3HI2L44e82..K29Tq0J9Q2mN0X754YL65LXlT4D893J4esJZ68h2ZdA0c5G2405v692St6I6C7nCd88dg579010909EqtbQ29PuKhcmQ1Y7F..

C:\Users\user\33920049\meuuljggm.jpg	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	608
Entropy (8bit):	5.599021625489054
Encrypted:	false
SSDEEP:	

C:\Users\user\33920049\meuuljggm.jpg	
MD5:	909355BA1B2ADA7E01CB81E2899B6B96
SHA1:	98ED232FB52CB179C60C6988480BB28D5B247263
SHA-256:	8ED9F9F9295D32C849D9939BEB83763955BC0C6925793FADB4A0A0735378338A
SHA-512:	C15AD4E028A05CD34F0C22B4DE80B61A12B901DE4994083C9717C9B4F3BBC1CF29431894ADFE3B7FEC934642741AD9A4226FC9EA6A2B3DA91D351387A2F61B2
Malicious:	false
Preview:	6d15n35xEkeNzvd8QC944717Bh2FA0xw70aOlPK18GE476j31Ln35goNmgC7yE3H3yjvwObH7t0znM9i024r..8RI733eZy64eVk8pHX2w1SN5y6v6yNKdry7sIq6bGaKU6b965019b477O9B8P..n0ZH6GU1802M3nK9S0v5lo398C9052955p9f603b8CW3K..Volo5E8te4h6j95z7ZVlgh31Jn13KO90MH24gO1ng3nnE52fphIaR885A39UeNy2Q9m0860ah5qV21790rvhK31yO7Z745c72MqBmngr..2IKl67mKUK6s14WzI1kBr4MNgTP83133o40Vsc4VF9465nu..9575..g63DF6si6uA7THw5dhOXgww16771k6hpca8wdag3Y20wW245x61TN8236OiM8E9A69o8lUh29yGXR207Oo2fKM6x8baR2F8A6k39w0757aw0v..0H7P30G5146F971454dTaypI05wZ6g8YhhUPw030vH37GO510LHz43BU4nf7adSF23ceZjWW6NV8d0O8fY2gF2g402biuDsTK336912d78q0T2R0XR0L5N97igRC159yix7I96hLDd..

C:\Users\user\33920049\mmbdcs.xl	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	548
Entropy (8bit):	5.47877878102614
Encrypted:	false
SSDEEP:	
MD5:	1A4DB14134A67966C903508FF04DCB28
SHA1:	612D22CDCF9CA81EBB295642346E3F0F9214D522
SHA-256:	9C66FABC8AC533B56109E3BA00591892A18B30831DE74B933532C5727E0F4AC7
SHA-512:	3B3588CC2686AE47E1AA66DB11D2EBB662D0C8F99DA8049BC1D560289D9A06E194266260D918D515B3470C7684DD85FD989050BE63CEBF731D89A6761102EDE
Malicious:	false
Preview:	09JF78Fh11lv273Ap1ugc9E7cGuu3..2tytW281h9C2PDSeI1lY1EVqZU..507ie6QZ889TNk3B91If1328iy39Xs8Yu4S88983G2916P25eY6k752X8zW08k3c7g33330om0d37L35Ki2Q791T48aO6b0S1r5UmSzw918VUxlH60Zr0V707Ad9t3vq62A51379S3g48580g6Xz9dX4aV5G15sS2K6rV7808ztG2howf42lydQp65..c950bpN27Zd5x16608tZ2BYeT51aisEmMJQ54k32Gj86M586D777E11221Kf7158Ef4Q6n740t4nhsjplG8..aD9O2o33Z03ry292VH0774ndw15ng5Pt61O127kc2O329355b56q42871SI13YswAz..jbp0jJk58X149s095365Tn0141cAZ7Cn71W47HVKMG0HaC4zi624d777g5G3135G63Y69RE09g9s30f6QQaU9q720E54fBQ0787U21HouAz1Wc08P3S1Qh8218a06NW4iDN27AX7uE3FtliR53..

C:\Users\user\33920049\mmuiqlcvwo.pif	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	777456
Entropy (8bit):	6.353934532007735
Encrypted:	false
SSDEEP:	
MD5:	8E699954F6B5D64683412CC560938507
SHA1:	8CA6708B0F158EACCE3AC28B23C23ED42C168C29
SHA-256:	C9A2399CC1CE6F71DB9DA2F16E6C025BF6CB0F4345B427F21449CF927D627A40
SHA-512:	13035106149C8D336189B4A6BDAF25E10AC0B027BAEA963B3EC66A815A572426B2E9485258447CF1362802A0F03A2AA257B276057590663161D9D55D5B737B02
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 27%, Browse • Antivirus: ReversingLabs, Detection: 32%
Joe Sandbox View:	• Filename: Import order764536.xlsx, Detection: malicious, Browse • Filename: KRSEL0000056286.JPG.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q....y....i.....}...N.....d....`.....m....g....Rich.....PE..L....%O....."..... ..d..... ...@.....0.....@...@.....@.....T.....c..... ..D.....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc.....R.....@..@.reloc...u.....v...H.....@..B.....

C:\Users\user\33920049\qhqulleu.mp3	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	57578
Entropy (8bit):	5.578086176536263
Encrypted:	false
SSDEEP:	
MD5:	5DC5D3365BAE36FC41072D92D22F69CB
SHA1:	91CE48060DCCCC9806AFB9979A3A1759041036DF
SHA-256:	067820A70679BC812C16421E4F759533DD91D8124ED36966436601B1F2013C94
SHA-512:	CE2119181FCBDA7C1B08068F918C7282DEFC8AD951E129458BB75F6CC9EC4CA105482B5F4AAC4C16E425736FA45DA790D10B4ED9346A93B23B4F4F713A912A5

C:\Users\user\33920049\qhqulleu.mp3	
Malicious:	false
Preview:	h2p1f27k11D4928Yg10sp4yM45..N0ev22LGA972g7108t53666312NEQ936013H6IGyekvJ71615uI45076O1PbOp00bA59fZew2Q3uW74G1..k861Wl190Fi62..u038 289Po5303Y375wD97P2t0nAp79EjMGK3wI35dT61673071a86A620afy8DJ870rVU48212I8s..ncD25Fb62q65jJ0HVPugF6YI7X7Eh0i993D1glNppq17371g73bR49x hOC7w18T9St7n7t6VA38VV077l5NF92F1F..e6Q3NRFdkG1n39Rd6h73S234193I5DKK125k40h0YM8838N3299r82GUBMO1Yp3G90Iw45xJ7P33jr6f54rDuo3GVzlg63 J..j8A8nb2007l654wnz1y587053Z98G2W3Xy9800UO800f..4cB15n61ea13513367yB73oJVg6c..hOi4T720885078n0fh5i8Y8C5b235f8Y0..6PQm64Yx0AR5VCwD F77jt5TP41949X26Q1Fz3uz6059s8U364jW51iZep4dp7084LpOw..O4o2V8ELjw7l8111mlDOskR3Z0b369z4P43g220128bCH43235sh72Oz2B11Mo4d..5UK7HGAHv6 64260sU7J31..bP98bUe5lC4453Km3AGjhGF1bb58Qzj6k6C834Tg95..d0j10z556j2bC471373U8o8HhEi5222I1q3lUt262J803vC24t5dl6Q30eK0i6r3nMO8F141J LXg8DHv2M7Zy3s24..P0rW6Eh4XgHS9F4n79T8oQL0T9v3p77qi5fX888Zy17T3o58OQ69L213E7..qotNsDVE53Sqb17Pa42ZY6v4125671zj5S75..F3o864Et7a6069 dE60Or8qp064D78XaH4EjN46493QX7DoM0SGp0881...Jqd84A2MR57zhMr96439g32590wWg025KOo768L987y6883

C:\Users\user\33920049\sdstvfk.ico	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.3732701590754415
Encrypted:	false
SSDEEP:	
MD5:	84DFE2A08AFBC32793395799841D38E4
SHA1:	1E040C2A1032335F15C39C60A01343A58889B5DC
SHA-256:	AC294F23A91818659CFC3210CB058D3D9C7DDA4EF9D4CD933269C8428DED3AC5
SHA-512:	9B6B65C14499CCEB0FE8276CF33CE9B92091A7D1EB2BE8DE4497F7B418B57B70675BCF706425630D9210DF7EB1328E443F4D2F08B0CBD088DA579EAF086CE9 5
Malicious:	false
Preview:	1I533y4o2432sC09mPm14467Qm6RA4L3630s7YE9op7c6b35odL61Lv..E7R51t4675ep5Ne6BiS0EVrm7941A62Qm50xJP378E4830gEMF779o28LuQ85658RPRC5z5wE d607f9x27tEx8D542xU8xPHPe3o67493w47..m68nw5a8Y8EbK695k64w59v32815nelJ8iD81512w56m456Tm7JwER87Xn4g743VO..b582271uI6v1889C253tZu7Eol 9r48z96EP902UcK8N4..Q99p11T43P4U9DdHofE6n0V7E688JLM77fJ1Bg1A27hl37H0CG12nJJ3..413p6lt95893mo4w0O5P62957LSuqhwb006fPl0t3i9DXt1bo8wt D7MR3Zx20865TV4zn64V2ka5cHZ8zR5w58476k94u9RWF7Qd8763KL041A54pJU3fP824dlbfzgRBtpQ919S269X77SNg4975u0z276n8mo584012t3Er88LRv7o02V667..

C:\Users\user\33920049\srslmbkgam.xml	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	545
Entropy (8bit):	5.5258847043058905
Encrypted:	false
SSDEEP:	
MD5:	B98459F0500F47B7B583B0C519CCF3CB
SHA1:	5D8012DB878B3F72B7A5736525F587330F988A96
SHA-256:	E52F7062BE09E0B5653629D3E3738EF2B514BA971CFA25EED7BE051466EE0E26
SHA-512:	C136360F2444CBB26A4DC20B7BBE04F1040D2F796D75FCE5274F612DB869E4943C7687E7AC457C705C5925545641A891E7CE242BAA2E7A993F9849F891E8D465
Malicious:	false
Preview:	GfD67N14eP8m1bN0fj0735N5f7v16q74W0C6Fs1q9l0o69se079um04K990PHo534Wi01vo5283qCXNJn83jG8m82PO61d1Si516K91925Qj542034Q5iq89tsas25j3Wo pZ65477Z08bF8mg48O9..vt1Ml5Z9yNR2m04028522aBAD99a8yr110Y655K5F8pDBr8wVJzJN75b1SDb7p616j10G18saj8x2In7wu2as1zt28768OU69P21D0Fj47Hmo 6CVCz7yog178l25q68238TZ45fm7CC96P323948b8S3zK6xxz3..Z1C6n3556UD4dEJN7n5ZM7Lwdk11258DL9xP2uHt9D13L0GJ2HLiuOP8CyF1o9pT652GHr51TTl..Q H2YsYeY2I6vg9..0e664n6Q39X5cs61w0Tc6A1nb1RZETK43DtvyY7OA35S15SLXM722on443pD183T88lFNr3b..4n766KanwrN8GUh21b2lzn0G691JTqM0xOe72G67e 681m9242JaaxmlQTr32R511..

C:\Users\user\33920049\suktleoxtu.msc	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	540
Entropy (8bit):	5.547551481633137
Encrypted:	false
SSDEEP:	
MD5:	BA57AA240C24091DC77E1E2EF7A99C10
SHA1:	A013814DFDF3086EA88DBAA42D1D5269CE08DC0D
SHA-256:	619C6857EA9C69C098E3AC990BE2B99B25EC1A75821081EAD723C9EF6F718FB2
SHA-512:	498B2133DDF75BB946A763216E8E757E902F7E6AEF565DB689B02B0A02526455EADAD1C1642924E7A611537428CF2D79B8314A7A05E041963F4D9328C61C4168
Malicious:	false
Preview:	7UeM9q9Mw18la8h385V2TY2J67875Z415miZD33XVD0fWsExvLj56QAB58zX50n866r0NMz3B91j75lAXO7664KTr03P97iu5a0e3ok9m1x8129442b30jF..bs835342O D650H5VCHlYXK5D9q4G0c4r365k4T5w6089C5ltN642O88P45K4d94fZ5D25Dp2x..o19q50od04s7y9uAfLrQ16c56n1J1Hw8501Va8Yhh..S002hzAenP3Vw8fbX26Xm O3..6G07391a8EW371DR721Be1RrMyP7..zW017Nt62Z9m63V1B3KU58U52U67FRZRp6954lN4m3AnMWKz1Td5XR317VBtmPA47Tq3bRl5u..5221XFy1Ly4 z3KR5898U54vHI1590032Q0A5J6J004FlS7FiSyZ34Z2R229KecLYwHuYohCaJ0y41344EOEH12107gfpU3B3t655Y3noEi92m1g5..7Jom47612d63Ulao436XWsS378O 888QuW2Rt11526Hn302bDdS067x9..

C:\Users\user\33920049\ujhg.cpl	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	535
Entropy (8bit):	5.501943056038449
Encrypted:	false
SSDEEP:	
MD5:	5F2BBE62D3EB28228186CD6964305381
SHA1:	46E019DA6F7ECE17D7500B963C80FF076B3B449C
SHA-256:	68C1BA695059F1E975FA07FF00BF77FD3B6E56EA4940E9E4AB5F7AA0FA33416E
SHA-512:	2F5AD3C6E6602C9980C530CD9380FEAB3CCDF1C2D836174F25EBF30C924D08FB958235B27C016CF2A0EEC51BACF50DAC685546778B893567AE3B51A89BEE1AB
Malicious:	false
Preview:	WYk9Z859egc932519..B1M893TLb60Wf52J8ek0NdwiS96mdZg2e6X3V4DQ2VK63x83ud6I7II593y276RNF9f9Lyzof8xR7HQa..N5k36V5598E7m2Ge3sZnA1cR0X9A0 840084Z4610jL3Y38ZtWkdx8W03CGX2C5p5bCy4992Eh6r93p9tim053v1KPOjlY6J2E9CscL2CD8J835FPZZD36tBAcE3r204118YY5Clk7718n8529957Y09Sge8gYEJ O466L..dNXk7sz8P4O49..f4ipv3W5RpW67D3W2rRW97v75N2veXA2C..QZP0q13Qf5771nOH6Y1r324r4244134971S9137oajWV519gX83400I85a218uZUs279IFN96 ..p0HuyY80xR8V7v6lh90hHN4e7OL6jG745402303t23Cx738n2GQ52R69S8Y7Z8t874EBQYG4229Y250Du3vVQ587an210h4gko80F462F2cw4g49xM226E4k091W4092 cauuq5zUZ0yDB..

C:\Users\user\33920049\vuskIntwi.docx	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	554
Entropy (8bit):	5.451419215130869
Encrypted:	false
SSDEEP:	
MD5:	9D55DE9BCF880293EFC22A6EDF63D727
SHA1:	91BFA94E624F6A6C9891922931A650F3BDF014AF
SHA-256:	2EF84FFD76915FDBBAF0CC328B1AD11F7F0967D295AC7077F68C44F2DA67B75F
SHA-512:	3303BDC222A120225D36B48C6DCB24388FEEB8BC90A5FC84D8174C9CE487645D9435B31482E5D64057B52727ACC5EAF782E4B07D74FC29B32314F361186DE9E
Malicious:	false
Preview:	e970K3K6t9k2e7O15tdejT7Sn7Qq5APO42D5c8DI2fzf170P7dM5E3URj68949M63pB660308..0Z7nFeV2Aj4d45E50826tzsFsCPc95Od6GlD5568n52Zb572al7J0J2 6cMon4..1004c08I4Vc1vEb84a1O05D0929v1dyJ3UTASw95H4X6il2g5qExNde32LC..E0P9AHDhBC160i4up784p9oJ210L9q5n45q1RF31L6O980D51ll9l010621T6 9ldG2xIx78ffqsCFS45q91gZS85i6R3sQ98xCR66HW9wZ7auPo2e3s25g5u0d762507u00ziT24V..43093P76L72429500832170O89Tu2g375949v..35ln5As955lr0 m8073125L228boRR8623c2y99W97zd3vCc5R1QLck4nPi7XsmTH354817AY25392CS00..2O56h1BS43V8xK7905G6Lk64Mye6SI830p8TLf13Z05oQ74oGN 49D651WnZCp46aN8BMMTmKs7X02F635ZS4M07D48a0..

C:\Users\user\33920049\weqn.txt	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	559
Entropy (8bit):	5.441373794856656
Encrypted:	false
SSDEEP:	
MD5:	E887844DDB3C6BC8C9BA7ABF0963B162
SHA1:	5B1955F3EC2985EDA50632650FB71150AD311794
SHA-256:	4E47AFF41CBC53A8C36A9F3446DB8EFCF8B4BADD7808F7B58D57BB6F4082CA1F
SHA-512:	5F856E4D003D5822FEC6CB2A4F633259073D3BDDA70C475449213247B69DB68429BBC487B6DEFB016984FDD539599C00AE54DC941E686A115DEB0C0FCF9ECB B
Malicious:	false
Preview:	VP1g07wz1m0513k47YE8U851zGONd88Z5px79e2NjXh10s645JS0S7034NpbhvB09zFfF66h5aLQyJaVOBRC8o7088Q30uxsb08Isv0D613D0wC4965d63Y14Q2o583v36 64v2229j11X027..7v8K42r01w7T5LN3Eni4i6qu0NZj30S7h84H7A2Gt11L26O6O56F46..2I83MCFHIt12qK028V141AxZ6HLD5..617284669S3o8669s4p4v1Q2ep4 j9AK1r9pDaV797ADlp..oo6yHV670255r7sJjSt04Th4O644Q16Njs67OA8B1TtOmI0d5747bFL6kjm6765778jtU0t7415r545lqn3wx37Dxi53133N41dI9874v41iTD44XG51s8Lx Sg8Ce88X6y3752KC39Wf0Z54194yUS0t2H..cvFZz9g9J20eZ9JE2znZf8tT858064t3w9XN6Zj4S35083O428Yw76Ol5s916tP77o3b6O81798HR479p1132XHb30IfQk 8Le07Emvxj8K8xE1065Sj1359Pk..

C:\Users\user\33920049\wsxedltsm.cpl	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	5.5485404237595715
Encrypted:	false
SSDEEP:	

C:\Users\user\33920049\wsxedltsm.cpl	
MD5:	CEE5E8C575EC77654A20CB99615CEBF6
SHA1:	D43519CD61E556D88080FF2640150B2BBE34AE7D
SHA-256:	2A4C2DF427A70334733E5CB06304BFF74499D6850AE736F82B06A52B0D850D61
SHA-512:	573E6B89DC25A143F133993435C60719439EF51409199F433DFD12E772A4222F2DF8EEBDC155A42C102C17440A88B37B20F7BE698F368E34B174F0BD490BA0E8
Malicious:	false
Preview:	j29pidJ632cP7m999gkKsD0j6ghShsM38o7044RP7Ry1v0D888gk5htmLu663YfJhO06X446m494rW5q430s25224nA5oW246424z99b4P9zAu4EB4mF235YE764yX91e592790Ihqq893Z..T4bA1h5yY30ud1Tvjy154Dt77m922w607kylHTt65zj3p157727D361go3W3H276..Ha90V8hLz4c9Jm20xp957FDjDbQU75K5e19l2uCiqYcYnRzxG4wtX12X9m81TN32tH6..DuZb30cne54764l51E6C03OC1H6Wm35D..9M9mH5E9u9CT4ag00JHrjP804Qj62h9lwODNBQ01ub8211o4Vpa5lZ32v243x3kv26V7Mz3CWF106X5Q081BU2P7HgUU670739762Iec6jkup5VgFT611hA0cSK3Qy01BYz720na9FGc25s3Rb059M87b2BalfPH0rH6PI0K6v2aBeT4R602716..t1r6T88039gP9D0FS64p9475N8TCSJ34RrJ7tylz1cN954P1I93Qi34418xA0bR3Q077B2S03nw5cXNvEV8997yp2S8l7K3Jv7Yjy9I..

C:\Users\user\33920049\xtax.log	
Process:	C:\Users\user\Desktop\YdACOWCggQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.459797846755074
Encrypted:	false
SSDEEP:	
MD5:	32834BAFB3B1871301A6BA9BEF2C5687
SHA1:	786CD933E49C5657480DB1485B0609F8DFEC11CE
SHA-256:	DF899EAC1B5F6515CBDA8B816319FF0F89D7FF9E4FBDAEC52C75E1505105CD95
SHA-512:	A3864E623BA6AD918138D3BFA27F8F2E7AFC4F2005BA7DB655D1798CEBB5CAFDBF06D44929364CF363AEFD3F7B4AB48C37B75B3548CA711E5C6B3AB68CEC1714
Malicious:	false
Preview:	909r1Px20Vlvk4D76LUZf57A31de05v0R7709Vp87M5t3r167Gb1wF24F573H0MiBP1al6x1l5142F6Hki..69kqz2S7IQ32t2YP58S4P2OC88MxtyYLNV6Rcl39564b85881x2216800eMh1519wQ24OQxher8l87B64L8be02406Iq..9wzX9PTl5..16x766JTG2I2l13885Tm69G4R4301657a39p3R38YIaD898fExjk7U8LO516629613D115o6WiB6F6043kq7f6TphpsG6V83..425be6T7gC64b703lXA1W1E9338S3c64O3c0B487ut5dK2vq4Ev4P5ZbwzxY2v5z78mg2rj860fmFhB3Tu2Gbzmv..1D82sAGc954k747g6a8F88c76au6O4h93306DJgBe54Ik2SU8rfE2On356ZsD3i2517eg3F2Py9007Zh2Oab5LR8494p0h72G894zZ38FZPQ3F80D1D7Wzc3Vs9867t6mlLttd2e4w6..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
Process:	C:\Users\user\33920049\mmuiqlcvwo.pif
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4DB42
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
Joe Sandbox View:	• Filename: Swift copy.exe, Detection: malicious, Browse • Filename: KRSEL0000056286.JPG.exe, Detection: malicious, Browse • Filename: tT5M57z8XiwLwf5.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Suspicious.Win32.Save.a.7200.exe, Detection: malicious, Browse • Filename: Purchase order.exe, Detection: malicious, Browse • Filename: 21ITQXL080104122T7.exe, Detection: malicious, Browse • Filename: COSCOSH SHANGHAI SHIP MANAGEMENT CO LTD.exe, Detection: malicious, Browse • Filename: 319-7359-01#U00a0BL#U00a0DRAFT.exe, Detection: malicious, Browse • Filename: HSBc20210216B1.exe, Detection: malicious, Browse • Filename: BANK INFORMATION.exe, Detection: malicious, Browse • Filename: PO.2100002.exe, Detection: malicious, Browse • Filename: dorlla.exe, Detection: malicious, Browse • Filename: dAkJsQr7A9.exe, Detection: malicious, Browse • Filename: QT2021154 NCX Glasurit Rev.1.exe, Detection: malicious, Browse • Filename: Order specification & Drawing_PDF.exe, Detection: malicious, Browse • Filename: payment.exe, Detection: malicious, Browse • Filename: SWIFT CODE.exe, Detection: malicious, Browse • Filename: SWIFT CODE.exe, Detection: malicious, Browse • Filename: TRANSFER REQUEST FORM.exe, Detection: malicious, Browse • Filename: swift code.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(...~....,(....~....o....9]...

C:\Users\user\AppData\Local\Temp\tmpB828.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1311
Entropy (8bit):	5.120237537969728
Encrypted:	false
SSDEEP:	
MD5:	9CC9B31561289BF47DDBEF114BE4B6FA
SHA1:	C901987D5F8BBAD7231B7EE4A65ADB93BB0F56A5
SHA-256:	984AA44429B06B17C290376A8D741A2DAE62FE6F38EEBBF434A0781230686097
SHA-512:	075F148FDD9187FDD6BA56D1CD3D81641FE8D8F9FBA903F98B307463B4BCDC77556B542CFD73C9BC2C34D364245D5B8080DE69DC968DE9070D44FE180741D4C
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	
MD5:	76413EBF84A4F46D01F8C8CE608686D8
SHA1:	8B1633D1647DDB8EB542F3E046FA47C734A7CAA3
SHA-256:	0CE3B1E05B72CFCD8DE944495B2A4CF5EF3B10B99D6D0D998A3BE6A042287639
SHA-512:	0B9923CE31C74E61A831CCBD3E8C6B79FE78FF7627EABA940D04E00C28A06094EC68E5BC2AEE389854A843DBAC9BD30C74F9E589B861C2441BBDFD18E39E29E
Malicious:	**true**
Preview:	.~..{..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.556127542695029
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SSDEEP:	
MD5:	71C86F4534ED6EA4C1E9A785F2EB0A92
SHA1:	D065F0540580FC2E0ACD365784FD5A60F8235829
SHA-256:	DBC475B81DC4AACF70235516B8FB463D4FB170C3E72E647C0BA2A30D3B9EC4E3
SHA-512:	6D97D624C0A2B3D3B8D51A4F2502B8874E59E29538AD0477F1DE32FEEDAE38890F68532B591EEF0FA0DB23CD4929890DB256ACB8E4B73F6F790BB11C1347368
Malicious:	false
Preview:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\qhqulleu.mp3	
Process:	C:\Users\user\33920049\mmuiqlcvwo.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	95
Entropy (8bit):	5.071141961542051
Encrypted:	false
SSDEEP:	
MD5:	E241BA8C7BF12A7128E7C0AD28348930
SHA1:	ACFC821D16BAB7535369917F41BB21ADA15E3BC0
SHA-256:	0B64183C8B6E30C78D7EB1997E3686A1CE832B3CB0092F09CA76BA5FD5EE0B9C
SHA-512:	26A78974A6794751B052B58EB01C3BF9030E1116050C24A86326E31F1F11E1289860AC915F055B13F29AF3D0BED1E73CE9C5EAFC1196DD1C9CACA9C2E560237
Malicious:	false
Preview:	[S3tt!ng]..stpth=%userprofile%..Key=Windows element..Dir3ctory=33920049..ExE_c=mmuiqlcvwo.pif..

\Device\ConDrv	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	215
Entropy (8bit):	4.911407397013505
Encrypted:	false
SSDEEP:	
MD5:	623152A30E4F18810EB8E046163DB399
SHA1:	5D640A976A0544E2DDA22E9DF362F455A05CFF2A
SHA-256:	4CA51BAF6F994B93FE9E1FDA754A4AE74277360C750C04B630DA3DEC33E65FEA
SHA-512:	1AD53476A05769502FF0BCA9E042273237804B63873B0D5E0613936B91766A444FCA600FD68AFB1EF2EA2973242CF1A0FF617522D719F2FA63DF074E118F370B
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....The following installation error occurred:..1: Assembly not found: '0'...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.832162830296474
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	YdACOWCggQ.exe
File size:	1073384
MD5:	b866823e1f8f4a52376bd108c457dd78
SHA1:	fe99849ec2763046308044533779 8eeba8000a02
SHA256:	ebe1bb18a77cf0b34d3ad06919a9adfff2aa69cfafa5b96b670534b890e3e2a8
SHA512:	fd1732ca7dc310395581d835ea3df1e7ad664c75c9c7f68ba55c0b2e521383a0c8781b490f7cc05428d6e534b356a585bf11b57e57808cc37ea08dabf4a09e13
SSDEEP:	24576:rAOcZEhU3Pv6cxzVQ5WP1TKyENXWPl1sDx52gWbh9dlfQ:tEicRPwZ1sDxlrtG

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y.../y..#...&...._....._..'...._f.'...._..'..

File Icon

Icon Hash:	b491b4ecd336fb5b

Static PE Info

General

Entrypoint:	0x41e1f9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5E7C7DC7 [Thu Mar 26 10:02:47 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30581	0x30600	False	0.589268410853	data	6.70021125825	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x32000	0xa332	0xa400	False	0.455030487805	data	5.23888424127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3d000	0x238b0	0x1200	False	0.368272569444	data	3.83993526939	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x61000	0xe8	0x200	False	0.333984375	data	2.12166381533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x4c28	0x4e00	False	0.602263621795	data	6.36874241417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x67000	0x210c	0x2200	False	0.786534926471	data	6.61038519378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-12:00:04.635221	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60501	8.8.8.8	192.168.2.7
10/13/21-12:00:04.720504	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60501	8.8.8.8	192.168.2.7
10/13/21-12:00:16.594375	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51837	8.8.8.8	192.168.2.7
10/13/21-12:00:37.676948	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63668	8.8.8.8	192.168.2.7
10/13/21-12:00:48.500016	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60338	8.8.8.8	192.168.2.7
10/13/21-12:01:20.355715	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50860	8.8.8.8	192.168.2.7
10/13/21-12:01:46.346307	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59730	8.8.8.8	192.168.2.7
10/13/21-12:01:51.665856	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59310	8.8.8.8	192.168.2.7
10/13/21-12:02:12.493659	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64296	8.8.8.8	192.168.2.7
10/13/21-12:02:17.809141	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56680	8.8.8.8	192.168.2.7
10/13/21-12:02:23.162203	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58820	8.8.8.8	192.168.2.7
10/13/21-12:02:44.037075	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60983	8.8.8.8	192.168.2.7
10/13/21-12:03:25.959416	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61457	8.8.8.8	192.168.2.7
10/13/21-12:03:46.660830	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58367	8.8.8.8	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 12:00:03.515513897 CEST	192.168.2.7	8.8.8.8	0xd9c5	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:04.606597900 CEST	192.168.2.7	8.8.8.8	0xd9c5	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:11.043402910 CEST	192.168.2.7	8.8.8.8	0xc01a	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:16.482105017 CEST	192.168.2.7	8.8.8.8	0x1731	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:37.563050985 CEST	192.168.2.7	8.8.8.8	0x8ee5	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:42.873667002 CEST	192.168.2.7	8.8.8.8	0x3dea	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:48.388473034 CEST	192.168.2.7	8.8.8.8	0x1e7c	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 12:01:09.613409042 CEST	192.168.2.7	8.8.8.8	0x2b6d	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:14.884824991 CEST	192.168.2.7	8.8.8.8	0x6eee	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:20.244256973 CEST	192.168.2.7	8.8.8.8	0xf63b	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:41.013844013 CEST	192.168.2.7	8.8.8.8	0xf900	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:46.232563019 CEST	192.168.2.7	8.8.8.8	0x4098	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:51.553874016 CEST	192.168.2.7	8.8.8.8	0xa2c3	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:12.380646944 CEST	192.168.2.7	8.8.8.8	0x52ba	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:17.695481062 CEST	192.168.2.7	8.8.8.8	0x23f	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:23.050698996 CEST	192.168.2.7	8.8.8.8	0x37a0	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:43.923697948 CEST	192.168.2.7	8.8.8.8	0xcf15	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:49.381719112 CEST	192.168.2.7	8.8.8.8	0x3871	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:54.662554026 CEST	192.168.2.7	8.8.8.8	0x2eff	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:03:15.359188080 CEST	192.168.2.7	8.8.8.8	0x5838	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:03:20.644177914 CEST	192.168.2.7	8.8.8.8	0x715a	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:03:25.845478058 CEST	192.168.2.7	8.8.8.8	0xcc67	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 12:03:46.546413898 CEST	192.168.2.7	8.8.8.8	0xbd14	Standard query (0)	ezeani.duc kdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 12:00:04.635221004 CEST	8.8.8.8	192.168.2.7	0xd9c5	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:04.720504045 CEST	8.8.8.8	192.168.2.7	0xd9c5	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:11.059782028 CEST	8.8.8.8	192.168.2.7	0xc01a	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:16.594374895 CEST	8.8.8.8	192.168.2.7	0x1731	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:37.676948071 CEST	8.8.8.8	192.168.2.7	0x8ee5	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:42.891959906 CEST	8.8.8.8	192.168.2.7	0x3dea	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:00:48.500015974 CEST	8.8.8.8	192.168.2.7	0x1e7c	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:09.632004023 CEST	8.8.8.8	192.168.2.7	0x2b6d	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:14.903381109 CEST	8.8.8.8	192.168.2.7	0x6eee	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:20.355715036 CEST	8.8.8.8	192.168.2.7	0xf63b	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:41.030483007 CEST	8.8.8.8	192.168.2.7	0xf900	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:46.346307039 CEST	8.8.8.8	192.168.2.7	0x4098	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:01:51.665855885 CEST	8.8.8.8	192.168.2.7	0xa2c3	No error (0)	ezeani.duc kdns.org		194.5.98.48	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 12:02:12.493659019 CEST	8.8.8.8	192.168.2.7	0x52ba	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:17.809140921 CEST	8.8.8.8	192.168.2.7	0x23f	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:23.162203074 CEST	8.8.8.8	192.168.2.7	0x37a0	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:44.037075043 CEST	8.8.8.8	192.168.2.7	0xcf15	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:49.401587009 CEST	8.8.8.8	192.168.2.7	0x3871	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:02:54.679204941 CEST	8.8.8.8	192.168.2.7	0x2eff	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:03:15.377491951 CEST	8.8.8.8	192.168.2.7	0x5838	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:03:20.662653923 CEST	8.8.8.8	192.168.2.7	0x715a	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:03:25.959415913 CEST	8.8.8.8	192.168.2.7	0xcc67	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 12:03:46.660830021 CEST	8.8.8.8	192.168.2.7	0xbd14	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: YdACOWCggQ.exe PID: 4896 Parent PID: 6080

General

Start time:	11:59:30
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\YdACOWCggQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\YdACOWCggQ.exe'
Imagebase:	0x190000
File size:	1073384 bytes
MD5 hash:	B866823E1F8F4A52376BD108C457DD78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: mmuiqlcvwo.pif PID: 5828 Parent PID: 4896

General

Start time:	11:59:49
Start date:	13/10/2021
Path:	C:\Users\user\33920049\mmuiqlcvwo.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\33920049\mmuiqlcvwo.pif' fmkkelc.omp
Imagebase:	0x830000
File size:	777456 bytes
MD5 hash:	8E699954F6B5D64683412CC560938507
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.300093094.0000000004364000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.300093094.0000000004364000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.300093094.0000000004364000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.300748651.00000000043FD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.300748651.00000000043FD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.300748651.00000000043FD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.300023978.0000000004397000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.300023978.0000000004397000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.300023978.0000000004397000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.302510420.0000000004331000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.302510420.0000000004331000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.302510420.0000000004331000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.300163395.0000000004331000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.300163395.0000000004331000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.300163395.0000000004331000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.302257446.0000000004792000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.302257446.0000000004792000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source:

	00000008.00000003.302257446.0000000004792000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.302075228.0000000004397000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.302075228.0000000004397000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.302075228.0000000004397000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.302576684.00000000041A6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.302576684.00000000041A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.302576684.00000000041A6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.302365365.00000000043C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.302365365.00000000043C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.302365365.00000000043C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.302148632.0000000004364000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.302148632.0000000004364000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.302148632.0000000004364000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.302206640.00000000043C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.302206640.00000000043C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.302206640.00000000043C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.299948083.0000000004331000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.299948083.0000000004331000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.299948083.0000000004331000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.300057334.00000000041A7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.300057334.00000000041A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.300057334.00000000041A7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.301942248.00000000043FD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.301942248.00000000043FD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.301942248.00000000043FD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 27%, Virustotal, Browse • Detection: 32%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: RegSvcs.exe PID: 6240 Parent PID: 5828

General

Start time:	11:59:55
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xe80000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.784677096.0000000006290000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.784677096.0000000006290000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.784677096.0000000006290000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.783237000.0000000004829000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.783237000.0000000004829000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.784402740.00000000060F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000E.00000002.784402740.00000000060F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.775408567.0000000001302000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.775408567.0000000001302000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.775408567.0000000001302000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6272 Parent PID: 6240

General

Start time:	11:59:59
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpB828.tmp'
Imagebase:	0x1190000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6280 Parent PID: 6272

General

Start time:	11:59:59
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6348 Parent PID: 1104

General

Start time:	12:00:00
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0xbe0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6364 Parent PID: 6348

General

Start time:	12:00:01
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis