ID: 502390
Sample Name:
XnQ8NBKkhW.exe
Cookbook: default.jbs
Time: 21:13:35
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

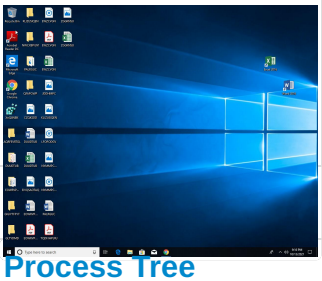
Windows Analysis Report XnQ8NBKkhW.exe

Overview

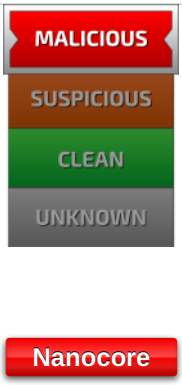
General Information

Sample Name:	XnQ8NBKkhW.exe
Analysis ID:	502390
MD5:	c2f9ae069b62008.
SHA1:	3df08169a1cb6ec..
SHA256:	1ff5df8d27ee598…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



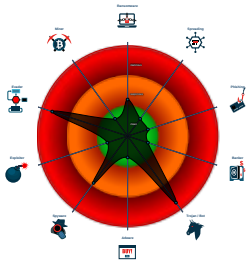
Nanocore

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
- 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…

Classification



Process Tree

- **System is w10x64**
- XnQ8NBKkhW.exe (PID: 1500 cmdline: 'C:\Users\user\Desktop\XnQ8NBKkhW.exe' MD5: C2F9AE069B620080B761D9280473E7AA)
  - plfiqbrm.pif (PID: 1700 cmdline: 'C:\Users\user\68821130\plfiqbrm.pif' mofcxpne.aan MD5: 8E699954F6B5D64683412CC560938507)
    - RegSvcs.exe (PID: 3620 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 6436 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD317.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- plfiqbrm.pif (PID: 6416 cmdline: 'C:\Users\user\68821130\plfiqbrm.pif' C:\Users\user\68821130\mofcxpne.aan MD5: 8E699954F6B5D64683412CC560938507)
  - RegSvcs.exe (PID: 6684 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- RegSvcs.exe (PID: 6576 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000003.333450416.000000000417 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf9dd:$x1: NanoCore.ClientPluginHost • 0x427e5:$x1: NanoCore.ClientPluginHost • 0xfa1a:$x2: IClientNetworkHost • 0x42822:$x2: IClientNetworkHost • 0x1354d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x46355:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000003.333450416.000000000417 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000003.333450416.000000000417 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xf745:$a: NanoCore • 0xf755:$a: NanoCore • 0xf989:$a: NanoCore • 0xf99d:$a: NanoCore • 0xf9dd:$a: NanoCore • 0x4254d:$a: NanoCore • 0x4255d:$a: NanoCore • 0x42791:$a: NanoCore • 0x427a5:$a: NanoCore • 0x427e5:$a: NanoCore • 0xf7a4:$b: ClientPlugin • 0xf9a6:$b: ClientPlugin • 0xf9e6:$b: ClientPlugin • 0x425ac:$b: ClientPlugin • 0x427ae:$b: ClientPlugin • 0x427ee:$b: ClientPlugin • 0xf8cb:$c: ProjectData • 0x426d3:$c: ProjectData • 0x102d2:$d: DESCrypto • 0x430da:$d: DESCrypto • 0x17c9e:$e: KeepAlive
00000008.00000003.296707219.0000000004E9 9000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xfe5d:$x1: NanoCore.ClientPluginHost • 0xfe9a:$x2: IClientNetworkHost • 0x139cd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000003.296707219.0000000004E9 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 104 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.RegSvcs.exe.6110000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
13.2.RegSvcs.exe.6110000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
21.2.RegSvcs.exe.4914d2d.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x241f8:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x24225:$x2: IClientNetworkHost
21.2.RegSvcs.exe.4914d2d.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x241f8:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x252d3:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x24212:$s5: IClientLoggingHost
21.2.RegSvcs.exe.4914d2d.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 108 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:

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Nanocore RAT

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking:

Uses dynamic DNS services

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:

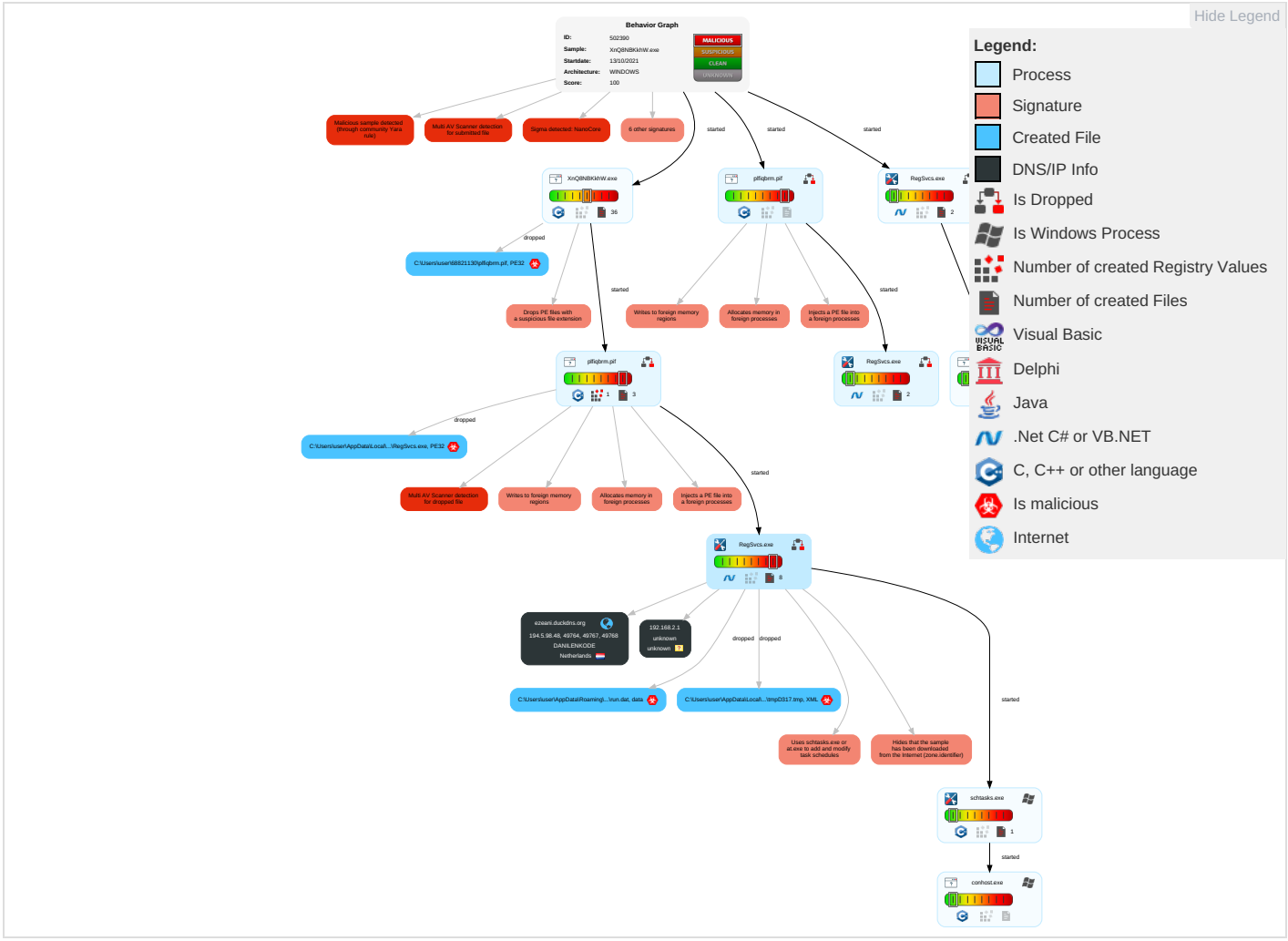
Detected Nanocore Rat

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
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	File and Directory Discovery 2	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	System Information Discovery 3 6	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	Query Registry 1	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	Security Software Discovery 1 2 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	Virtualization/Sandbox Evasion 3 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	Process Discovery 3	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	Application Window Discovery 1 1	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	System Network Connections Discovery	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	Process Discovery	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
XnQ8NBKkhW.exe	39%	Virustotal		Browse
XnQ8NBKkhW.exe	46%	ReversingLabs	Win32.Trojan.Lisk	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\68821130\plfiqbrm.pif	32%	Virustotal		Browse
C:\Users\user\68821130\plfiqbrm.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
21.2.RegSvcs.exe.1300000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.RegSvcs.exe.6310000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
13.2.RegSvcs.exe.1000000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

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	
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	false		high

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	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502390
Start date:	13.10.2021
Start time:	21:13:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	XnQ8NBKkhW.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:	29
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@13/38@9/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19% (good quality ratio 18.3%) • Quality average: 75.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 76% • 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
21:14:58	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Windows element C:\Users\user\68821130\plfiqbrm.pif C:\Users\user\68821130\mofcxpne.aan
21:15:09	API Interceptor	752x Sleep call for process: RegSvcs.exe modified
21:15:10	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\68821130\bitv.pdf	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	557
Entropy (8bit):	5.466223670451294
Encrypted:	false
SSDEEP:	12:wDXbOp+ctqdHXWqKm83yP2IUpDGHIrZzZxiKHVS2RfyTmg/2zqy:wDXigctlexX3rDTf5gjy
MD5:	4BA0BE4906547CFF8D68F1664FCB19A3
SHA1:	5722437038DCFC1427C2EF88C1166C01C496DF4D

C:\Users\user\68821130\bitv.pdf	
SHA-256:	A4B07202EC983DF04A8A15477C101E287F422977C606D08958FC21E5B7B84E90
SHA-512:	36F0A08993CDBF1227FBC8AC347DB1ECCDBB46844726015FE8086C5AC8E7F238BFA1765A4028C9A0D8199B2EAA7686C38356AE7B9F1D0575ED868E005DA67DC
Malicious:	false
Reputation:	unknown
Preview:	S2mnH52rgoI825T3JTsNt1M669WYndVg4qC8k18c14V0J42tKlh15631f1097qv1708Q84J65vj31h990i4Ej812dK5397nszn11ZH2xo613c17H9X93419s7KJO..4C80 407E755YH10r4Y2yG20Z2At1NC9BV4P15Eomkp4Zo72Q88tl6ZU2z005bPz..KmRF6Vh8108f6722q6h67y19orckm6u97C68ft0gS01o141Q1Uy9ye3dj1714o8dCLk60 1..4S8sGJ1FkqB8X645u9m86314CzK6EY8hE2Lkk715M20276PJ521yZ8C5712o9p6q6XO77k66Df01WZ08A56qv980Up959CO47567REM9yB6175V88nu6iyD8hD4Hj51 qS..8lez0oJX991BBBIIi2NECzS03OCPv997Q659c33XG30kCY99l9G17S817m22VKtW4se88hLJ14IY0PO27379894U6E8IH1vd..435S0q34wDn30S003Z4ryvlmj1Id f91xW42140a28Z0Mq25s8AawDpp0404BEWf..

C:\Users\user\68821130\cavjofbut.icm	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	646
Entropy (8bit):	5.501085040576136
Encrypted:	false
SSDEEP:	12:bWfYfYv7PIHL/ANf28SzUqznYzDaPBjZcI7r9mGoym9AMZFmny/LVbi:bWfYfs7UUSazDaPwI7BmGNTMZMnqbi
MD5:	2369BB5A01CBE315E482C0C1B003BF19
SHA1:	0256FA4FBD05BF0EF623FF2D643F0662F0236AFE
SHA-256:	2EA218BEAC4887C68375F2EDE0117BD98B22D6249317BF877E2E06E161994CB4
SHA-512:	2BCCB52BCCF09BF38A6756966D2A1B34DC9F971832EA436BE53860060A0D33003A536183CDA0B751DA657900FE74216F15E857F0288A2110A924D90BBD390282
Malicious:	false
Reputation:	unknown
Preview:	kW47ENJxAd20jY8K61B040G0Z44J0o78279Q58908K6gBdfV31owP89716Y91s2iy4Vv97evc4v6uKf350628Ey9454G3T080xZ3PbN5xSW84D3U4Ilx8U3Lmbe1E73jE4 j6g7e691v0ZB1U1j5P4Gjfe6..tWt02Ayv5108579x7CW8El4m2Vq339r3S6o50W3eAfQ40eN61581540Sps3XaE60JqFB3NUj25Zv74uzywp1z5218P7..3J5OgfD0G2N 37ovNj0Ts1eTG1Z1RS9Yi7X4456XH2fVu8i22iHN1X8669h7GB9zNE06S59h055351C90o644exRa0ddOq3F1XJ7u4C3917en8qMb27fPV4f5r25h7o4JiN..32EBJ1C9f M26Tq2k0jw0lQ725EQY3sRhU2N5Xq26f8a43222xw7Vn199034Hl9I1566Bo7rw07059u7Xg8ChMeZz4K5..q1298g3400li..4usatyQmJO2vsh84H670PVD36C234RK1 mF4Q1Y225Kmi7pW3082oO6l1uTf2l14l4W6088yo44l28tz979883yPLP5i784M2x84d5ER897RNJoz673221H9uF8E7X49j535EkyL1y7B6o18X3xi64vs783p3..

C:\Users\user\68821130\dcxtmvu.msc	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	533
Entropy (8bit):	5.494236541799768
Encrypted:	false
SSDEEP:	12:WRp3w4DUjT+alRHhU9sEhLcT7xc/eyC4KFcg:WRpHk/lRHyJYvxcZC4Ir
MD5:	E9E3FF28275A07913516C4572AC6A4BB
SHA1:	9D0758A025915E80350BC1934AB28D9F1D10FF95
SHA-256:	329F7E4270097E99CE634783042B71710CD0F27A50DF20F4A960EB6A85B8EE3B
SHA-512:	0A4B07ED780D9BF07A460BA67CF48DBA8B119273FC7F6BE810CBCF562684AD168E8B3EB60433C4A8B4DCC8D86BECE31F491365540526EDBEA7F7EFC2269438A
Malicious:	false
Reputation:	unknown
Preview:	t4C5eF072zVm76H04D3O5..A6k8Y2C526t370ku625RNq9f3nsbSk3664b7i0o79GkD15X..Z77RM1V78ju6r6y39ZJs3P27211lUcQ71GDV29w4j789I20190099882Fc T95..b9uyn88v9ju6705te842lrm342U1g7q836ld48..r06k054n799L0n0A82h3BfXhV6EjABjj123Xx69LQilhxD4B7..eDn028a0In07g57M5wRxW658lw68wCZ1C1 9MO1w7120hIemgXcR84H999p417mT6K70aKX4w1cq9xD25H6yFp43bW2yF638i6nfe3Y60E55iz8p21853..Q56L3TcfNyf25wt2CQ9gC3704224F5f0i..XI2J9b86LA8 82GHhEV1Op84011D345TV2M2k13pde9Gy9N1uz3R91y0430151l8T2jdP25G2W7o4059L79l9lw2B623AYw405o7c50gc95t0QEG9945In23Cg0fzc4YO1K2xsb8S58oU6 o4k7o79ouUI..

C:\Users\user\68821130\fvnexf.xls	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	576
Entropy (8bit):	5.4475963792195135
Encrypted:	false
SSDEEP:	12:O1SmuCBnXm+LLhnoID9kdzNgU1fnIZNc/5HOZRQPW8A47PFkTreM:ePZ3hnoID9kdzNgU1fnIZNchHSi9b7PW
MD5:	DC7DA903DAF313371A0579ACBA043CBF
SHA1:	0E3A0F5E7AAA8E975F643909B99E7C7DD397243F
SHA-256:	B9041B6494364129AA4DE649F953040BD6054C9985CBEBAAEF705522AF1F0C0B
SHA-512:	1A42BF1F7702FC5EF4E32EF80F53C83F5E30DF5811516956588B9DF1FBC81B67B89C16D0F52DDE10909856956DC4CE858D4ED0813A180FD4302FB4BFD3F885B
Malicious:	false
Reputation:	unknown

C:\Users\user\68821130\fvnexf.xls	
Preview:	02u706J064L13694Z2ikQ3FM4cOu8Z99Z5EtlF37763285219rujR42935y4DvQ2uqvgLC9CKr1vX2ixR0iS2WW3e2b8B98C42z1c22i28537YGUQB23vX8k488xnUKQ64 wTM9Q400U417242n621i8WX7E63Q152Zju0U33973Q37ol..Phk8P4LiV34O6tcfh31D6q8G035303L69614n35C20b6Dv5wS7bh4MTuUA0XS2xycM9BzU0Vw..pp8sB55 876nL41CJCRKm36y78Q0P84TZ6xE39B52AE8T2JeG38A2M2gvIc81Rd97193012ig3C3180w88970hkij530aj80e0Xgs1612b92..5z4yR7K39mz427C64gwgY039573D UihN49I32917tcF8sH0y5SxYG24Bke5z9y3522..6yrOX1wiE452w274C6G184uygt8UizKMKL21RCz662374l8sz2276CfmE3YF3j1SjzA764L0nU3957Rg9j91gH2pO5 O34672aqzlvy739r4y8Av569C63n2VW1Fu6b3dEPOP7H18986171Fs..

C:\Users\user\68821130\fvokcn.ppt	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	508
Entropy (8bit):	5.493645123258151
Encrypted:	false
SSDEEP:	12:ZxdPWng5ywnqGLzDMVst3ntygonxJTHOrfn:XMnunqOoVJl8fn
MD5:	78202699D218DACC967443B68817F47D
SHA1:	9DDA0D9E794048F54CB1BA792E87FCE14A036182
SHA-256:	6A1525873F5B166C8C45068AD295C1A0321D9DDF30E50D4DEF2ECEF9AF713A55
SHA-512:	497787AD586CC689976264BB72F68FF9B5C48A3B3389DE7A967772AC589A902FC6381CAF301CF05BA1AC7811FA644F11EAB642D9A625B65E8F1E48510C9C123E
Malicious:	false
Reputation:	unknown
Preview:	8e5cg3A57G4i8R2B02f2sKle0CVD1Ch5HR9juw2M55i70m1Al..7r7P8YfR0420PA4c6dWPq4o68yn3cuA8J420j1YPs28s2769718QT3d5Zgh2qBMJ5c1z08A58VzMFg8 9kVOLbi892qKf9VoH43dNj748vGIRrB431589Vrg17iK7640q74b6987h134849R14..33beJ242i909v6T80SqOv0mr184sKA544dQ9zd43v4kq0393l7X13r62oqFTao 4Z3D0..Uj8k94173oT58DP3Sy3764l9nSa118WHxwGA08Da4t7p3wI345717..Tpq0Hc4rj730ri96Ul0aJc2ZcJ059LAZeH6OM890w3qo9wXC1Oh56le1GTA..Dj17K21 627023W305..6J728Wn4Y4P08fPF383713Dj58fHl0kEEHP18CLXc34279wQS7Oga531b0050OMB1K48E..4657fO6R5Cc0..u4KO4Wq702vw7594fDg..

C:\Users\user\68821130\gctbg.xls	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	672
Entropy (8bit):	5.486863867804244
Encrypted:	false
SSDEEP:	12:cT+TvPsxs5sRD0Z3MDr+X2FfALHM5FRP/C527KftI0mzyNvVTcSIYIw13WzOop:cOv0xs5s906Dr+mFMHM5Fh/C5gKfS0mB
MD5:	B2801B3E4F1F579912A88A757D0B2BD9
SHA1:	83CAEACA911CD21D26DE9689DCA51962FCC829B6
SHA-256:	6672A9EECDE9DF150B86A99A1592BE0C995E8FDB7C2653350C859C03676E6A12
SHA-512:	7102E2E514DD64E4D5AB0E889FF20B554975A7BE99623FAA855310EA9B667481FB7AFA512B7C6675E4D96572E36B78AB83D46501A63A633D4AAC88DFF2046B6F
Malicious:	false
Reputation:	unknown
Preview:	k59O16RhOUP4vqltAuJ2ye2hS9dh8u4875Nc406w5827E0a8mn..V52tc8778396539J0r40m3y59Ey4q997t108B9X85PWTw61jFzVd0upv8yyrRwD8..D9A8iAB4E483 z391g654l6Fl65O98hdVw748g2P34Vejm0675yP6d19fSQi49D..kXJ0kV8eYdnxx18Fk5TG3XU2x28326V4IW2RD6iw40960pP92ozV235VF60573gi259013W6Uh2q7u t4T7M26kn..F4n94M2rvtaN1f62k7e017Lh40hj74J5N38x6C24h6882g1Zlg7tA3t805FEqz644J84l7Px978g517Pg68960j2w7I9N548bBxC25D3N70Vv5w67X46154 ww2929096j0g5p83..tv99v0T292wCK8n7jie47M70VApOJeQ91qE472634a2u314M8xeHWLPz1iO93oy7AG0z0fhvl6y4W1548..rpr2Qg7Eo55319we5Yfx4n2BbJoDV 6is39e0j5k9No6Bc5511617R0raB978088590ouI59sKN2429lrWe83ziZ0d1j5vm61mmg86GHAE46AX72Nk9BU79q6V8kd6o0K077SNv12N3x8B89H4p8m4MT8ro3w8bz 9Uqol40oXwi7T59L753q..

C:\Users\user\68821130\gtttp.jpg	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.5679539900788795
Encrypted:	false
SSDEEP:	12:GJ8YS9rpmqEF8PTnbUQFV7Q4WmtQbo2DopnSnQ1QnjskkAwZo+vn:y8/9FM8rnb3V7Q4W+fXSnQ1yskIv
MD5:	98D6F21219096CFF49908D8BF99D4D72
SHA1:	5D3FAEDB818C93E5C4C971E555F72C526ED5A3CF
SHA-256:	50856CE35A3CCA5132A8D820F4220DC70113A7EC1EB8C464B2E89BCD2A2B7833
SHA-512:	79708B7AE1B057874023AD1F78A85F62724E70733881F2F56781C4F26EF70F1CF880B7B0C24D07D25F1D9F3BBCEC1444781E59A8D1848751D870692BDE2F8F14
Malicious:	false
Reputation:	unknown
Preview:	6t98Z4bG4f9205W8Ht1513232L94247K5CpQx44B3E3Az1M7o..j8A2730J6jq3G79uUo42c92ko923Y5ie3X5bwg683624W75240KDzT26l..2p656d08y7Av91l0932R G222530QMqn04KbFZP9rg4Lyv840T6szu..4KNK..6UJsi..fTX0QWBRbK38wm2CrBp25C786Y91kc9SaBaS555L726gvLS9E55kjnf67H56Dlx8d2OCv7NSo8a9D65F80 P8377kA..TX37w70g9RK3vD2of4O3o..Y1Aw9GX5Kmyv6E7XfV5R030U7YfMXd829Crkix0uM7N894k9d7RCm2ifE3z8mX1RlsL918EaMDj7cf88j7E6423594t1p3FMfZ m5v41l6F6L..851HCVul02ByNb65698VXS7648Ic874RmH0lB58V5MN63s93uf0621rapfl89tpa8uUn3j8X3c5..4qeM943KzmSLV3s39ipU79114288vxu3nu0Q27f7R KaU101UTs5h5LB46R0a70YPonO65cJ7s40D7H9..

C:\Users\user\68821130\heakhaws.cpl	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.451796800769334
Encrypted:	false
SSDEEP:	12:f2BeYzCotsJ83wQNWurBVQ/o2AfYdVTul5ZFz8gQTu+lRf8e5:OymJWuVV92u1FogQTVRfz5
MD5:	826EF7A1DC539675535B27E499CDDB44
SHA1:	352100556618C50D49BA06A525ABA03E72BE9504
SHA-256:	1B3FA6BCF195ADCC2ADE144FED32D0257CE9F5A1CF68271B7EFBAA502926930F
SHA-512:	269D54D7A6F10096E52BA8CAF777E3C5DF1DDD9FF0D788BDCE839BE6C51B02D547FD0A434E203DAEBEFEC1AE4941A040FA0C8A981603B723E0F97CF6A97BF13
Malicious:	false
Reputation:	unknown
Preview:	2GW3T1hl435RS9n387UP6s78zVH93s2X8M211R9o08ON503ukj1AK40vli5E2Q29V31193J33b68N4It5zg5xC10K4Ua14k05u5VkK03O3246r69y2F40P5H368M9V16YU0sT2P8vz2dvfi6..4XDa2SD9x431h05C392EpU3siT0gHUA61C53MB26Yc802L..i4Lb97Nhx56TOp0BRCFCTI30F6838Xb45c54583xg4j6SH6pAd9Hzs2Q047016VW8fSZ3tH04mkm2d948qg74knn2m0693P5q508kk836..M3Ucxk0UPj5G469C76fK4i5Z3qk2Q3..19S91Id5dl..rclT7whd4T4B6Efl4zb8v6fv144E7ln0750159CH0k383377v56Ta850G6p3s20s67Z5456Wj1fRp3G9kk2y7268UO942fd22xD6864H0f728hh156697yS0k79nh10Ussan06D74uP546V..9SUlK3H86u4b17650C8Ge0H92C43FtMB5j4256707u427RH160qAeN45dO84wP514701w8hhio31RUNo67zrB0xO024ac24W16n77Rw4o635D91537006uQlVP04f8XXeO15h2Dm15CLd4tHV2mafNUIS847iFw2B6N69487kV..

C:\Users\user\68821130\hgvswqfand.bin	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	553
Entropy (8bit):	5.496798251649183
Encrypted:	false
SSDEEP:	12:0cp00BZGyIuVhmro88Fall6GfQCmUOzL+ubBqqCxLd4fWkKC0v:0cGwZGyIeQrobIb/oL+ubOLdkWQ0v
MD5:	C4AD8591C49C80D72807D2791D586D31
SHA1:	D2B29F91582DF645D62DC7315977C1A5D142BAF1
SHA-256:	583D48A09314D9C9D92635FA2A24641DFE64947208523C9D5252418CE4EC4BD4
SHA-512:	048E80A9C633BEF89A69C234AC0AAE7F89E59213CC6E71D594FFA730C89D40AD7D6A7C638E04037793114EE8127A2D3776C70FC848E2966DB0C8805345D7466
Malicious:	false
Reputation:	unknown
Preview:	ax940z0x85gC5W9Qs281S5nPk6q40K02z64268wmsZ8CV3H3199n5f8B66r341B424ADN6r8366O2u020dOKIdhvRLVg127ucDO93EY8119QiJmB7y3gCl313Mym5X8p62p79S0axed1uz98XX94xb0Bq0086u5aL3sZm0429Hjl..GN4kgc762389J48R792t9v70032039..93Acm7X1Z941sI746e7FUc5d4A75GotF5s2ARFRc6h27512nE031420P96DV210ACK89n8177220TYAszD6BD5L1DaLhO62y8p1p773gV0H5amtYrDUk8wPY05sfxBB7TF2Px795135142RQg348V8v4..QF758kB4Ek58iH7186P7uuI666Sd4J2zK2ov0UX8rX30qf3A6d15JH70rWij1a8q2X32p0sw7bd1309Aka7co4K0qJ8400OJ25gK02T5Ok380T4b7Y4UC0vt6wn09C8bsNy..rs9GdMJ223N344w334w5PFwO980065rg939uwAFL7G0W44Q3S736i37037..

C:\Users\user\68821130\hnjw.txt	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	586
Entropy (8bit):	5.436153215893494
Encrypted:	false
SSDEEP:	12:OCWUJe3qScdktbseq0AAlfeAtUoAJuNoPyZHxemrO+kLz/86Fn:fWUJaVc2Pqilf7qPJ0G+cJn
MD5:	037FAB9961275617950CEE4AE4FBEA02
SHA1:	0FABD1FC0895F89A0306B69952DCC6C0C49BA945
SHA-256:	A30A15D45D76F8C3A2E306D60E765E80D2BE58C2D733C82F5ADAFE3E4CA7F28F
SHA-512:	2FBF82C7AB5E8956A64DE787912D5675503FC750D1738048F73C0AA980A7C03B98C76660435968AB4495133C1C85B32756F72B307EAEC456E51096DA7F4959A3
Malicious:	false
Reputation:	unknown
Preview:	8H327s33wH261w4k0o387d0061FEJ9v9L89822xqnF055Q2StQ8N57Z5o6MO6r941yzk9Z5kB15F8m66J1f5S2mow4..88D3IY6DXv0qt8skK91hyreC5S1511517V46Y27991..Kfk7A6k99103Js25B82F0G6Afth3P4j57RKJM56l6hN9FF752E424abD29083M33384dAF4tq01oOi976G..6328HJw6rFeDy0fNPL26Y641hP2rr8843OF675rP13VCN42PJr8yJ360Gz30lA30x1Lr3FV8ePM0u7n00Pm020w052321RVZ8..45003CqxT07432171h6lwvv4M48tgUGV99e01i5E3Hyv2104U6ydyKlp2V55892L33Le3R6Pvr92dV27jWwT80j79457LSf7Cn555Tj3HpVFGu661F9589117ZD0Nrez9zZu0G8w6H9Yh98YpO135Vl5mgy45o22sP770dZc9j61JZ40H..528GUhuvjD18Q1G8Uc0sY74Kf56WvE0KS031P4079A02d25ZC5k64JJ991l46ia3Z3Hd56w31XWa34K5631598..

C:\Users\user\68821130\hqsnlpl.msc	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	545

C:\Users\user\68821130\hqsnlpl.msc	
Entropy (8bit):	5.412666062462004
Encrypted:	false
SSDEEP:	12:rskb5FCkzrQwvRFIdW0es3zdPg4Ee/8VUd8LCmv4YlK5rL:jXVTv7Z+5o4EeGfCmwYlQL
MD5:	DE9C9034A0BAE6580EC717C52FE26963
SHA1:	961CA19ED41D1F735EB6438E164BDED77B1C7F4A
SHA-256:	767F283865BA225CA72055D11D7151094516A1687921D73C2FBAC8072706F5C4
SHA-512:	128CDBB66C3E3D0BB15FFDB1326CDB11D90DAA3BC412F317D6509C7010C053CA01F2DA2A2BF8A32AF2538855011025F5765B3C0A3249ED3756640432BC20558
Malicious:	false
Reputation:	unknown
Preview:	6em05fFru0..79yS2989lr0Ec3vCO2UC2V45110n09wD0144dl3U777E1W028hDT6KtTKX32CyT2E10S4N3264..39x94a12630Z7L2prf85c91Z6l60C9Bfh521Q9YQNu 08D33h7KM8td4739w5x102IN4upl8..8280s53oZm12z4f8qz479PL7b8Pj4v65PI67T8Z117327e67v36G0A1H8lt7kd..p7q63Jhpbu0GsBny92D27F9IfoS3Z16P6m1 39z21..T7546eS6GDwy3aGJ76dkB589yi3U97186C4..4x0YgSAOec9m898OXfWB4918Sm57440td9284Cm6WL83224155P5M1c8AbA05QTAV9743Q7RFqBZ 0e83685oN592G194946RB8584X9979QY1hQ4m120A278ArPV07i0WRS41tV03WnD05Q32160n162396KUD2n0VKm..9IQq5Ge90079352CE48797H9Z196ry 4zVDmj5S37434L284WLUVh22dGG5C0x7M6kw7K22U40..

C:\Users\user\68821130\ibcwqengn.dat	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	520
Entropy (8bit):	5.474030452753662
Encrypted:	false
SSDEEP:	12:wNRNpBZCXuEQBItMyWeiTJcR8uBesjrmNLZGo6jeOUYTf:wNRNpBZKaqkZuBewrgkyoTf
MD5:	F7A8FC77B09BFBFE1CE5E32AEB3D527A
SHA1:	8F5AD145C9F78544DD20D9A9FC5F7FDEF6E7A5A0
SHA-256:	1292831B9B4C0DEDF9B047F4CA9585A07E4D7C45F8C352F2E7A7B0499BCBEF4D
SHA-512:	11E44AF9DC2B9D127C5DE17084D2EC8DCF1B6FA635D802F4E906A15C85805058457BD9FE23FBAF4A4FEF9A5D59E28EB8B7685A2093BA6D093982CCF44AAF13 1
Malicious:	false
Reputation:	unknown
Preview:	79M1P2O8682cy1Ov4A669773V1F50L6M19R9jXse40754R3X9kAzm4d08cq..8KVbbtIT6V3980p..4d6bC6U13up9s0BYVKoo6DJUps5my80Nyf844WjsgY3R153TScBd Y3TebA8l00D88473V..Gk5463wzH99x65F3211Y5Hxobmy19D6P0H9XHd78aRI80352a2wLon34D08072Np8ScU66JX..Xyd5K1b88A1sA779w169i5F02LlrG8K2ynUg7 9C3o0C949rkikH7OK9E58N7u92B7uSI6..970hp9622D1vN66Tj68Ev289O254888f8..8cyQ5959210adA6ER5k34vC5H9d8A43V79M76L..He81k3No32401PO819sFe 04Cp89Ik210P7q6aB233T9q3Kjc..3J31HB666lv2291F6TOB69dG49TSr4URcp536Sp7H5237H4rRHwXo8O3g89okQ9at5hx77wH9T5OY3vv19Rq92553XBjq6699xO..

C:\Users\user\68821130\ikbt.rwv	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	416786
Entropy (8bit):	4.000012827458825
Encrypted:	false
SSDEEP:	6144:VsrUI6Q9YYbSAmbhjlN6aVWNEQmZ+poMopKhmKTA:VkUynbSBbhjlN68WWQmlpgmK8
MD5:	9BE6ECA2A64E61972E3464DEC8B00CB0
SHA1:	AA889156BC0A7E8132D6C6114BC2FA8955ABF036
SHA-256:	442C15B300838DD80A3C4EAFBF6E6A70ED42E9DB5E9594A2A3769B7A74FE3C87
SHA-512:	1DE5EF1B9809344BA435173EBE220BD0B2EE5BF6A811BD917DB6A2659F4FEF17FC589CF0BD0866517BC09E666B4F86F51AFDBEEF79798B05253877E9C36CE4F 3
Malicious:	false
Reputation:	unknown
Preview:	54FEBCF4CA25F91F606E5E824BFCE7E62ED292EDA723F9016DD7F5514BD0055B50838CBC311B5ED2120DACB411832E6EE87EF61F18A5C1F6C05DF6E1 176050390C45C03AEAE25EE3256F11093F2142EBE75F590B2C02D7F2B24224015EE09E50920D58CBC900F50D712CBD9E1F22C06716710EB59CD2288B B2F662E2254886D08C406ECA30152EC9B97E1457E85CF3F1587A3BCBC652A8DA4F0265AECC4B386902A55DB63BAE696FBE4E20CADDE90C7DFE1FC0AA DCE316AC1FBA1E76DBE468EE43FC426F8388BDA3D22C7883CE73121FF4792073AC8AF7B58E0FE863EDC632205279D88CC622A9200126FD9131C3CC01 20D340A5BA98799F0410C5F4C88C6EE04C8427FDDE71226DB6DFFCEA6AFC05E79B819F8E842D87DB577CD0A31C979F54B221FBF0161D5F115DA71016 0A501D3BF3343D9ED24282B919EDDC073F5720EE4E751F7C1CB16FA9183834335C51A81C73DF7C3405A523568E698609B6973F0ED4BBDF5843701A25 BF97DE6A37342143D92C1C05F2A48EE1F8C17665605539D2B88083ABDE2ED2841603091897880499 1A6968E0D28FF2E77541DB28EE7CEE5ED34511C9 495770FF4EB88A17D1809F1D7D7D20D8F9B0FE58411A7225DDB634A1557559126E95ED49B58E0FF9F588378521028052803C96A363AFD8A38C1DD6CF B66D2F2187D7A47D099DD7353C1D985457B686FB

C:\Users\user\68821130\jebjct.ico	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	558
Entropy (8bit):	5.414538522632163
Encrypted:	false

C:\Users\user\68821130\jebjct.ico	
SSDEEP:	12:CQXRWPPum96Cqig1j4D4+t4kej4uuiucL6CT4YENuV5Fcwbl:rKumIFz1CA0CT4zNa5mwbl
MD5:	5734ED554EA8FE0864AC2FF44F988305
SHA1:	95DEFF77B2B38E09B0A5EA75DD61D1806AAE09E2
SHA-256:	8B26F8FE795929C991F1CBCCD2DA4013E80605FCA3611DBF81A12FEE6CBF6F47
SHA-512:	F391E3ED27710432438FAAB5F53621016054DD80CF4861F709729DF9D03A0B814ABA3D1151597896C44A84D3B2BED1A04318634C61AE3EE2F8BF5FC6AC182688
Malicious:	false
Reputation:	unknown
Preview:	D8SA270KZ3tc5aDcu7f2u0iV..1640Jk5C24395vi99UG0Y55191W3XP1QaVRu3f3MJUl37941n8AT991ov56380082377T12M5b77f5BPi2L865962u..3A4O6EW6WflV 835mx3O1Q7ZL8imo123yf731niFD3bMI23362..uTt09yK551044mXP7MqYdm947W9032G20803..C526mGqr4Oh6J3NW06erI1fR6y4D1DI7yUE574CJ2K73cL6p72c7k 27870bMW4ZYS91864Kw99G766608ns102q16GJa51v78R5G6NuLch1YMoQtQ9r1z03255Lxq7174Ye5kGC97l6257845Lor..639455B027Y6r0DbJ3W2898mh0H59hzjy 1XDOx4uZG1gG7960..B5vx5x99R9KBZ81674Tqfq5U099938a007S9pCHk89301A02CB7m4295xp292X7295U4O6b69Oy1B39DdX..Pr48028J6m1dCpG266VX5pj2WcqpCIka88i9P18l87o69130O3aaD741N2O4La59..

C:\Users\user\68821130\jgukpqf.cpl	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	569
Entropy (8bit):	5.485236454639823
Encrypted:	false
SSDEEP:	12:DQxGvi7tts5f/ujT6ibeCxh2ASDgRZ2UawFhfY9IkmUIEVfVTyois:vhOjmIv32ASSZ2bwFhfOZmifVT/1
MD5:	37473CBB9261DCD6147B50D4A441F1A7
SHA1:	BD1C936483BC7E97C7BB312A0DA5DDD6F4F4DC13
SHA-256:	36847A6B9CDC27FB86CD49E225EFA7B45B3FD0AD18FCD8650E5F4392C219EA0D
SHA-512:	DF0D776257757E2E4B813BAD6E56EB7C0D43C0A24B5998EDDFEE94516F82372DA72CEF57DAA5E4BB3EB1D9545FF873431CB682048E772BE91068FCAC88231EB
Malicious:	false
Reputation:	unknown
Preview:	mG6hqCFj38Rqqo4Oo10716F6Z3R519AgrN8918S0o9E9yD9k00NR53p1T8l4U12g5e6am9Rc8547td5975r458LOk1pa15M38Ba8mN9M7076y61..3pjOVq9d3A54d9O45 Q8Jmq71Hs4586QFX27k6gN14198m0ZF057MBG3f15TO..i606Asr3Oo0V4v4k261mt877R5K9d5bzoCkB50e5qf0X70JQ314460p8SzP708Iib1Y92vE8610Qz7c04302s 4YHsbHv2UM3K26SAhB1Ia3..553160J7V2M3DWDy29mKZM7660On941286n0Zgr9JPS7U1B858aWTe9QZ61i2349c9gv72P40h4Y6E02O3e36Ojzq5dJ75V5 q3NgmP0UfVrQR14zT..351u117T2h0..K5hrU29DEc112WX837K6j9QT4ab6T3v6F1AJ3P9L8KP0YH6Zp5bX4oq1714a82jQm4RL48T9342rj7K424Ug498Y4MN84bz4C5 12981h5a7ro7A1jNKZ6eUYD3e1ocyS01EBuF319Bv00ep28E7lZQ3jA4o..

C:\Users\user\68821130\kedwlpbcj.bin	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	566
Entropy (8bit):	5.435837082071211
Encrypted:	false
SSDEEP:	12:puyM9nkyJ9G3v2CGq40jzJWd49boerhTBoQ5ljdwlTwn:IyM9nkyT5qjnJi49boicQPuJwn
MD5:	2531BDD724AFF68FF06978C7D92781CB
SHA1:	AB7083FE10A32D3C06586C772E01C345304025FE
SHA-256:	917B82FECF7E666EEB96BD0C87BAB170DF7951771A370F519D227E1B652556B5
SHA-512:	4BB940A61084D89313F1245B6376D2D695D09CA9FE5D26E19646516F9B6688F68306B8E5D917E06E2D1CA3B72470B2743A26C8EF761E804B77CE27C51DCB7ED9
Malicious:	false
Reputation:	unknown
Preview:	0zp2iV813Kdp2jO2PC79309R17f68Y592EB0..Zk13l9l1t5tno78f1g1HP0..9N7267n4TU148126..O3E7d4V93KTQI5G80w3a9uA5n7270XRx8368Dh7A3g07gf5q90 ee484GHV5A1qLw92R..Jl1t959khaa351Ymhz1006a1f41Epor1B00rkp6GND424J732b5176o760mdo7is8y67S7kguwL1fVi652G02e7agd4h4K2Zk19F6Z3x0K6063g l3Gd7LsP5iFL41Z747O..cvppv04YQnW0pYy40S4..67t9l0azL5FG66btm..f1b3582t5l48718lPA7XHN8FTw0685O9476l3es5JZ44CHlRq2W0r2099xFGO5L4M6A32 30thF124Y5g2G60F1174f47C2U1001782H8z2n1ufF9P742315976..rc1XPHc5930e79yCYh7O7072VuvmU49H..U157F3y7oosNhWb1aw338126307G48OdI467Va4Fy 2t1SJ4j570iF3816004YS003102zA2P3109aqu079b12..

C:\Users\user\68821130\krxdtoehb.pdf	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.519579586596138
Encrypted:	false
SSDEEP:	12:EG/Eov6MzEpVKRffVhF1EqSlyfCavmqOs4AmnPKlTaKRTardTfUrFrgbFsPC:rW4ffVzNSlyfCRq145PRKoBQshEC
MD5:	9ADCF17273740814E3B6B10A89728EB5
SHA1:	D325B769814B6D98FF2145D6447AD63734AFC91C
SHA-256:	49BE3569664F38896E8365CB250983325940E0B5815FA8608CBC097E545ACE20
SHA-512:	72D8C59E586267BC63A6D86341CEE79912937099FC324DCA45589538137593BA038058193544535BFB4769AE583A4A2A44FB64F3BE44C8F6D37189437A3E18AD

C:\Users\user\68821130\krxdtoehb.pdf	
Malicious:	false
Reputation:	unknown
Preview:	W2tq0750jF36te88vl5V142Z8sSEV1930l1b4GI449n6HDckv7j1L2073V86j6t2uX00MC7Zc098xN96U2pHg3oR5c31HB7suY84T7mx992826SJ259f672..SVm176TEd 1rCcYhm9sy8q96f1j3V1F6845Zx7y80xx..2572cm6891p3ZW6qm4691rhD5J254ZjY4M4TR0Cg8HPr0641P87Zb4Ng5Ge80ztJ3MM4o01o69244moEtyN3J9a35567ao2 e617dF3g1Z4Y846OjQ5X11t10gXyXX901Luq4Ju8t4..5l0Zhdt7nZ8mTc9Mq219m6vKvNeqGkTO31QjT39FBY02cjK6d54gSUPaFj6v10g984tGlOR43BT37bwvcbZ204 A88SO761Ol46sSo2K6P015UimOeX8L554V9pxpMPcs6YMt0LJ42q27IG9b4U93313sH09j..b6e08287bE0O6n1487l0MUs02eW4PU6S790615j886Q3b2575Dx22rUM19 JD5u8t82OvJ69Nm9Fqqj1ECzfnM5uQc17CUrbi921J221Y8S7336Cqi28jy6G9x5q3055x5J9BI82HwSuG6D6C4cPn4n588lh19938..

C:\Users\user\68821130\ktwp.docx	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	559
Entropy (8bit):	5.426020407000818
Encrypted:	false
SSDEEP:	12:e6wOnxMYuB6u0nF9EV4acVGzC96dWbBVYPu+m69MGbKTVHVSkpyS7kH6dn:eJOnxMD67nFdaMGe95b0G+mWM735oan
MD5:	697F85CD3D1BD0456531FB8B14A899B3
SHA1:	9A01DB39BFCA26EAB7E412EE2B25B7FD4F677BA5
SHA-256:	FEAA28EA4AED5DFE568D2D39A68F59F933200846E56236F24BB2ADD263928E08
SHA-512:	D98BB81D9DCEB214087E11CFC79EF166E3949D51274E653844D9401671738E2C46B1E34870E1FB0E3DF7C997796DBA0A5B93D39324D102791043D9EA91B6BEC
Malicious:	false
Reputation:	unknown
Preview:	8z9vnBhu51es6H66Q4804808o95U5T920u2325F3OVAd5A1757xXb57P00392dP5S294CfEh4F9up60V5FA47c6wH060dvr23GYaQ74..374G91H8mj6LJ794e17Xd39A8 M9A0dim3247d906ej4iubHL7711Ti43699m64T73467x0U263z7w2SS0cnjgk9o1061S77o30kT0h53YuD3n42kE5967kW3X77aa1hVA0D6o15233lcw..90ok8dq33AAt M7j6cN8k6wU3v1mUK1c5R0767AdAIF8N65R3x56ziD5l3n6Vz9hH15lv79Czk32GfG74S8c1s4dND45x4476SPqh8HT21piT9oS33e4r370e7L8xljvLnM8gK..8GJwL8F bw7kR72330B8i4m8am289Yl1Unq6u2CinLjO7..L2q5m823hd6rn97eY965YTp068848BS47213047N9VfA..07V89Ro11u689572ul42C31709n42Fh89s9kMH8w4J8KF 7lLPesM6x7045T83iU48e4q4ql8D2DKT743rG..

C:\Users\user\68821130\llbflml.icm	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	533
Entropy (8bit):	5.455945159617544
Encrypted:	false
SSDEEP:	12:EsIFErdTKZmCxZp+Qkqi4V5UexrGbvAWdzpjyaE:KErNKoCwZVaWexrGbLzEn
MD5:	8E44EB24D752CDACB2FAA40CC506CDE2
SHA1:	799001993436019E4F353650BC4F3C0C43BC89DE
SHA-256:	02437D81E41DF987C1D743FBF054FB54DF6DAF47D3E4C995879C92DB7B9A4402
SHA-512:	6C8C858C6FD8DCD433A6DF2A5ED981ACF05D90F484AD08E46A5D6EC54F46327B99F79EC3C143D9AD2FB149111BE70E0439FEEF146F67A29655DAE5220825A4 1
Malicious:	false
Reputation:	unknown
Preview:	z684Fq05xCF8730PvXy52tVRfN42Fa82CE..370E556627X95S795N82v6S8b518wVe933WemB61T24iph5..1Cb340S76feRd92LAZl9c3E77o59Nnd05o6QY8k5jO739 V7wfF4P8tf2614825X37m1OW72Cl37Gp4bLmKjB0KEaO6..D051..FQkjeHPq9B589i7ae63j90Pf0xk6b7D3bA4293lPPb9Ln3AC14nY4R5C8074Svs14..1XzI335AfR 3f9P833XqSp0O0y0b3cn70i..77xOR312CCAG212o8175a17n713nZ7Mf7y19zCs1Yq2x2f161K2hNS89ch987D718O023OGM0lL7i20Jqu287Vg28E7QW20Va1458J8.. h3x58dmJ2359fH3qBB8W..rIXBU105s7J9ZOre5Cf51Ysw3t03..l0nD12j6Y11pINfP680CQY0q25743z543X2e1673z3SZE0ZS57700oDjQK68CP898N1P74985523f5 2w63ovH834o..

C:\Users\user\68821130\mamwlmew.bmp	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	564
Entropy (8bit):	5.522896281027247
Encrypted:	false
SSDEEP:	12:mtOc72uqOrc0RsmkCg/2FvQRQHNfldTba28k2dalfLL:mtOcDrc0RpkCg/ubZYTa5n
MD5:	19D83EE8855BD72EDDCC58C6EC159ADA
SHA1:	46B7FB56BA1C7BEAC33B7CE28420EEBD911D8F06
SHA-256:	F4E16B0FCD33494D42171185B7307B64BFDA982D99835DFFBA829CF1F1112779
SHA-512:	4F17B2E154299A3505D46B33F49CB53247E2A257A287D4AC5A04B63FB110EBC3039F21829594268C0FF82D40A78A616FB9C8308EC1132F8AEE9EFED5A3A3622F
Malicious:	false
Reputation:	unknown

C:\Users\user\68821130\mamwlmew.bmp	
Preview:	D6Jiam4Ad73Vz8Jfh7Jn8cPO9d2M4LF976bE5279395zRjG63t2428Bx492L2093S7HN2a5TG1Gq370pw839..33980Mw6153VQ65eh20ccK6f4N4a6A197w1..t283107 nG8j342CUKCs140Ag2977o6n6nZXN3357AC93XKh86U7D292P2UJ8F4B28c3w34T9byvgG1M5cOs08542t0OTu94b5Nm9bAD1rn8S5i6P9XhcuB10H4IL93bI9qu0664X6 pneg2JlPSW1xhWKc7qx35IVp5a93254..V99kGQ68WkTPo03t650v6lO5557aRTr5L9m91031B2s7495Zv02D6uVY3uS4r707b76S3eDw63v682D90a6LwkmFK46Fy22js fv1R1HseBm256T7ZegEC7SJ4lF..c0N4W165td3u2Yp0P84Hr09o7y4llj31hl5rSvY0aV0SP2pe8Bo8894229326Z10Ks4227qn12uzP9OV3n0Ku07a3D0J28XXg5g145 05Ry6358vN71400uJr9Pk9a6I4ksF5O57GH357GmbW..

C:\Users\user\68821130\mofcxpne.aan	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	data
Category:	dropped
Size (bytes):	101059264
Entropy (8bit):	7.117031967595777
Encrypted:	false
SSDEEP:	49152:pZIZMZEZPZRZ7ZwZAZLZ4ZwZOZ7ZrZpZHZjZMZpZ1ZeZaZ/Z/ZiZmZ5ZQZNZYZrR:4
MD5:	2850D903ECD69BE837FFC6DA1E969874
SHA1:	BF145DF8807BC568CBBCC0DCF0042179293DDA52
SHA-256:	72DAA16A8FB031497B3ED4984CE8A4F6ED8980648AE0422409C92711080EEE85
SHA-512:	32ED7E3A046977E00DA93618AC5A6DA8586F0308BFE009B4D6441B2F88AA3C34B231478DEAA91E02CCC4D37DC781F50A9EF4F7E00A03AD2FCA8D011C033DC6 C3
Malicious:	false
Reputation:	unknown
Preview:	..;...h;/S....-.Wa4..f..G%3W.z.....X...V.?...D.....]6..>b.....ILjc...S%.p/4+..zq..}..@. .\.rb}+.JL.[...S?{*.....0Em.ys..~m..JO...Z.....x.d.....C.S.#9....!j(....#.c.s...]..;%.Joy..A-..}.@. .S.....j.w....m.....?!M....N0.M.=.}_..I..+...j`5.r.xE..tB.l.+..|..U..4U. ....9.fG"...0..n;...#|^..dvQF..~.....im.T.....N_..Y..Q.. ..._[y.i..F..'..K!..m.....3.r..?.p1.5pZ.8Jf.B..#U$...A.& .Id@..$...N...M...B..[;"V...kNyG..v.j.N*..^dn.8...R..(D9EuI.U...#..1..~...oNV.z{.....0.A.n.c.w.c.3.M.6.e.....J.5.l.3.1.8.a.3.6.6.0.r.2.7.g.7.x.5.s.7.w.6.2.d.u.7.s.0.....T.8.z.5.T.4 .R.5.P.0.k.h.5.F.D.z.W.2.d.h.1.X.a.J.....y.c.4.0.9.1.F.j.y.3.Z.o.K.0.S.m.Q.e.5.5.U.e.A.g.n.c.....&*..Y.....|.{..U.1.....'..e..T .F.4`.p..09].....Z...(.i.Qh..M...N.H...F...(#..k..w.Clr...@ .fH.[NM..wt.;.5.....nH^...`.;%...!.Hr...AS..y[..I...21.I.d.....3'\!.....*NE.wY.i=!..S`;....y..-i.-.....M.....u..v...s.rX..e..=.Q...KB.oU.....k.2.Y..!O."K..UT"':.....:...y1eL...$tK

C:\Users\user\68821130\npfrp.txt	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	609
Entropy (8bit):	5.420748523281788
Encrypted:	false
SSDEEP:	
MD5:	3F98ACA5866EBE0F3912C414EE6E7BAD
SHA1:	A693BAE0DDAE030A45BD2D3CE0B512613674CB06
SHA-256:	0A4C13A0A5FC320B073C065BEF861407D28FFF382D5B55330B8A02EF88A4A350
SHA-512:	61B2A0E2198E027FA0DB4CDA3DAA4C7A57FA2FD8802E8917B33E72C06966F2363A9DECE6B5ACE93C46F7258547EE941768FBA9D61B572285A1EEAA55AF0FFD 78
Malicious:	false
Reputation:	unknown
Preview:	W7e3Ua5bF3d656I3422L189ZngUT6TH214gtC60k697wW5W4CM784x90s91HI68U590U4sV056U593EVrlgf82HzP1T968b3b7..boAIO9r6OIvx11m0h4Wl2N0Wq5MW1q d6Ew909X56E6457L7F8..5l3MB8e0JUiK5U497909723u8xlliEbgm994568514e9z58O1859kh0BN7Eao4F17F922Z594947eU5..460FJ7..W7oD2F80v15nBAeR17aS g7r648591c6376Br6eI2gh9f1Hb6..28j3u..E3U2E48O4W5P1q0FnbdI85F303s0KWBTgvpUkDFif1lu4nz162aH0W89897m666p5b607y505f32y9z..6t9De7kg9E0B I8127088H1Atf26mbyQm1S0z2t63X2M93e5ry2K5R0ruXZ6127K17ioxWrf04fz7547Cwrv1odW26j573161i85Wdxj274Kn440dJ8Q39S..XoXgejRs5145l8u4x7vW2k 50c4dgAh4U8fvs65FSrt7Tvw13b38994HyYgg3595h19455a1H86024A1j5TKu6167odH736p1869634gD8e5H6..

C:\Users\user\68821130\ntqpgj.dat	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.456201224379962
Encrypted:	false
SSDEEP:	
MD5:	DA026DE17853E86B3F8D5A1015F9007F
SHA1:	5F2221E7F8F6401704AC5C059A4DDE2013DB7188
SHA-256:	6C0685B051383FF33735D1F64980BEBDB4AD9EFAA185B67D758095B5FFD03C0A
SHA-512:	BA264A0B640FCFD523D845AAC880C19E216A50367CA0B9801FD6960E3EDF0B0220DE7CF1543BB64E96FA027333967D47C0CBB90FF08B7549F54ACA6C1847CBI 2
Malicious:	false
Reputation:	unknown

C:\Users\user\68821130\ntqpgj.dat	
Preview:	50G49W8Y63W5j83w2jT9RX0e41cN4eKheZR3785S4gY9L4WJHNy3GRSZDA6Dv77ErR868S2HR57s7H179Lz4..zh5d4ohcmc142qb071X3435apd17u3Q17H 392H0D71K1Ng4317C4tRA9vP9R87NqsTK7x19AuQxP9Ra2Oeb0u50GI7265lQu3Hap9u29jI37104p3V707qdS4GH9eFdEg1X885r76x4R1E37Kq..43tjgH0KLF08d438 6e..ur1R0m73669ZC8C6021X576h918167290t2w31flf3E01342O6E85Qgt934D857pUz819z93Rp17Qv5T546dv15SW11962iC906V3heT7Xq2bOcs2pbRQ15VoTo4Xu 10hV1Z9T9uX375461bXw5X58i0579c7CuV7..071DJlOxwSliw800Lq79hZ3P1biRYA33F6g4d000D6Z46SH34474r52s5p56cBg31nX0Z44O1..7498hKflvcpyv9oH2v eF0C493Cq69r826cB079p64h6Dgw5VX16z9KT789026NAXx3aaFAU1361H1Rn1765l4D1dF8TjoW2dRbH663Wl5s8Cz64t7OrRU4v2l690ogCy6E9YvW4R0u7436Q4T338 2627iV6A30aR9cwhN5..

C:\Users\user\68821130\palnmuffs.msc	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	65753
Entropy (8bit):	5.575706356828312
Encrypted:	false
SSDEEP:	
MD5:	DAED960F09500D943E479F00125C6EE5
SHA1:	EA18481BC7D4E5E293187C6E6D3FC5B913118635
SHA-256:	8F3067402555EEB18D37E9F5A9CD411A1AAB6D3F85A8C6780243AAD7D6485B71
SHA-512:	6DAD2A1871962E2444DCA49EF09C729A7E4CA2D39935D923FE63140DC62B8FD1B6B3AC561487F99AF3AD3722DD368420AE9764A9B11A3ABAAC7348C4C7F5E8 F
Malicious:	false
Reputation:	unknown
Preview:	XE7ZYJ2ASj5422mSY6Sma20kU86109SUK6C9hGPH8zw9Ontn..T3z72PP7S8h026WX8ln28U6m7S9Plu5972rLz05225jtR4UnKS0..9im3061pnjW1H7hjb686YEvq826 W75F9tq8XHNY843x0A10zp0oorR470RZ140e0i85..007o79kQE359Y5e2o5C1bfbA5wO088xiUn7a4Dj1xg10Y1797HJzk27M2D8Qjp4lx7BY5k8Q6E..E77u8559a6uk iPBYYVbpYAOwixT458tzKlCpr88t9h9j3S09g..pfYnXnEH5c6dR9l1eF0nsN8k86MS470YBF981y9Jza2NY9946d7zp..PU7968189wgW5Y7pzQmYG366b7286J04UEDs 3znqN8YPN7JXR9dP058..9QF711r7L54995RPp3jwfAIM9uy47GMI4sM19JaFs8FY589k803s7Y9iV18W6O00..8AQ76W6u2U0eW154X073ba373L4255a5GEN700335ZY 69g521Z14g4D6Yd7k049c66Q084l63Yof68kuW4u0C15..4sGS989g4ZS6d341X54G3FN1..lA5278754UArM3CbT03c742BkN5t965Vke1tAwy884518Ll6FZ23..8Ayr H3u06H4nh37Di4al3o4D9IrVFFM8U3u0vP086egvCN0z671j4S..9Q3P5pZs4a49471aei0EgS6804Nr711a4j2t0u641l46v1s6Lbj4rHSz278if1s9SI8l347ptATZ6P5..B921e11 L94jfHg326042Iv676160W2N..9M96Q2Wat3rjq813Bp49hR0..2oYS1VMOwB3F63m3Fo333QWk5OGnUiw3c18378vjR32U6Uzr1Zw1wpwC0kGl4q264V4E4Vu6ZbF4309 K6fl4244R7..yhVc109d4I1zmblc4kJV802MA0O31luN8AL5rV6YT0cCgh54157bi688xL8L..081tN0

C:\Users\user\68821130\plfiqbrm.pif	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.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: 32%, Browse • Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown
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\68821130\qncxknbrt.cpl	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.435100984165968
Encrypted:	false
SSDEEP:	
MD5:	BE106E4BD08CBF7E68679FE46837DE32
SHA1:	2893CEAD14461907E76455BDEA76324A0F07BDE0
SHA-256:	8B6960083235CAD56C1E2B56D99C569C61480CE566AAE890449EF882DE223101
SHA-512:	A933118BA2DCECDDB9106245F2C4AEDE95AFAFFB8E1876DF3191C8DE01E9B52A6DF26B15DB0D96985A12CA60414336C91D4779023136E79B6632CD7642B51A 1
Malicious:	false

C:\Users\user\68821130\qncxknbrt.cpl	
Reputation:	unknown
Preview:	4775719wrSZL626YtWJjg9KQ3CYb9TUFBAyOa6W383A39H0yY5439x92474149Q15X40s4oBNqj..A1O0ho886Yu6pk2TyaC1n2472Ulg4B58lQy929y587km67260538MVMF98T0F78iVdWovI2U16ZE41B72J7Ka13N2LnT4j7Z4eKsi8g26IYVZo98l74H9l8gEi56tLs7o0o..6328GQ798n78Yg6ij8758zznW8uX7IsgaC0836Sg13J2gVENI4jEze1LR40701sC06F90Bk8G9h10Z354WxHc58v8PZPL3ht9R1L710M6Vea8P85177MwV8Z..5QDXQ6M40..3T30q4Zx8wx87Oh784L401sW5P50t2577Z93522303X1009365F..60RVg6880mLnH74MbCD7b8Xuq2080pV140795p4969qy396E87605773R32iwUOX5gDhjwNI863s587DJ7Xl649Zo2Z4SO504y4z33a29g..

C:\Users\user\68821130\skglfoubk.ppt	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	508
Entropy (8bit):	5.369433538744767
Encrypted:	false
SSDEEP:	
MD5:	B9CB0C65C143DC282A7710251FE02EDF
SHA1:	C59BA0F9393EA62BF4EA4CCB1A4D2EAAB6FA2176
SHA-256:	E841F4D704A3BFB0CC84594F6B9634160F833DA354568681F61C6B1050CBD20A
SHA-512:	DC4E03CD10BEB2DE9AD047711682784A8B88379318F2C7B8D1AA46DA41A98FD99BA975CCB4D2D8FB3BCD2C60F961378CFA3EF098B4F78AB1E2C9948E93B4B34
Malicious:	false
Reputation:	unknown
Preview:	3WV43iU0w12F2eq7B09cGD43v6o5OflnQqz4hxGmQ0H7HXec9yU0z48AJg91v124736105bSw4l899KnY0291V38np9bFb886..4A0awi87795a3s3ST53D558pA02U1M3d6jn99M930D0qB9lqLjD90Vg4h07P0e34L1T40G5S8O2x472f70o27c4j4t2063ol00e7529994L3ds1BaU5Dy1Ln7co66C4K0c08fq0e..tnd77h0Iq82t0t8qyDfUD9vK34967fy31X4V59qYa4dCOq5376OX31l5w125v7653z011NKu9Axz8k31E022U94i5Zkqx585690aq73W0R1w04jU835eww2BgF86P22x8H93441XBX2773..fI79TaxQbK3q5a6wo8247o0eF4Y557g6G74Ysy4Vt06354R2Yw92wG5636CRI1lHh33Y20600339563Qh3j205..1eF0IQ219O96809v6I7Ef3n7M0J592643M0N6..

C:\Users\user\68821130\uuwtdbgub.pdf	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	588
Entropy (8bit):	5.422166344336593
Encrypted:	false
SSDEEP:	
MD5:	88F8C3EE050CEB9105A1C61DB0B345A9
SHA1:	2A77C70185E5BED6C79494111D1CADF4DC0488DE
SHA-256:	A031E58C189056F58711E736241B2782D3BA962A8DE58048550ADFB147A45E35
SHA-512:	F48F4720C38FC482D1411C96BB7EDA22E5A0AB6A429D8A29729D21A1F2594ACD6A16CCBED499BCF6CBE33FF83454B89E08FCE8E4684EE22C4E91E49AC7F9C84
Malicious:	false
Reputation:	unknown
Preview:	F63O3vy9996Qv94Np33i5Bl9Uyq2x2L2G0D4vX3T8Mu46tMFY9rSr2WDL6lt3J..7V188996Z..7Mp1585WM327Ie11scT46H57J0ykJQw1477V7Q581731966921E755G41lU0hUXN..K3zC99Z0ou6sD1f9ZCVqH93h4W55091KWJ7B5506G437JbSC5334o4IB5748WzZHr703YT0vO6I48Cv57Gv1196k603eNC682731880Q91kug3mT2k1q9h86N7C85435517B0PIIG54aQ8t439197BoMnFcCMM71f1Hm7fjM4mC..MKv4Y3M1qM7z5y05187316 9l40192o82FDuHc1dg4087vl16146n71OcaE0217Q249Yk2El39a76u5t72v08Mbd33983dlR10F3Ws13roN5Y7Z3..62N51i6c69gFW77si47He3I8Qj985FJ2wd7le3808794GsisH348GaFS03e4g7469667X55698W124Gv1ZBjj0rnJ0n550WNxORm4469uvCrU50K74qIAH9t0BfBR1T0V8y178qqRDwo7E4sU5H67V73Z8QT18j..

C:\Users\user\68821130\veppqo.bin	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	511
Entropy (8bit):	5.526256819858086
Encrypted:	false
SSDEEP:	
MD5:	5633CF07E54D8B3DFDA857534EACAB22
SHA1:	D4061718E2420736554C24742D460B748C7D02A8
SHA-256:	0703722058175BDA9D32EAFF7DD73B8B30E73638EB645990315ED82ABB5DDED1
SHA-512:	F10DDC89EDB537CC0611333EE0AEECEB05469A3D9EA94EABC717D82865AF2786BC65E70E116C054E6C9280555F2635225BFD9B0EA8FD32C674AE1200CB5642BF
Malicious:	false
Reputation:	unknown
Preview:	8TpC2gsAe378gt5SCY3x9r2whWya64SMm8N7a890v5LgJcT395N4B9uv1W9M64Vw17Iq3n0R55K6s483rhVL91Si1D965uw3tw092o57rT79886i7k54ZfEilR73x..31E2a84m04bv5g73y6Q4Y57634z8T..w27Q2MTbibk3o2J2cVlR522HL62HU49A1h22Ty4wG32O1k661f5..k3196m9Qa1566sKRixx25q49Q23515GVnX4Cr40D711i7L1v6FTNS3Qp5S19b635ctx37OZ1s14Bt95gKu9M4rA9N61eis558H001Zu958bBzLJAgEKo5Fe6YAXY2044..xpk542n8S4VA360d8VSSS3pV1Jc37s8jAfESr5sRuIU94MQX2u95pS4r628fhXtN34Z9503Z4ydAVj13X2dsYN124B45N0f335A404c0Cb7ivD1..1WI96h69zP2V4jM862701s4v..D2079h5uK40G176gwk607x9OH51qa..

C:\Users\user\68821130\whpkfkb.jpg	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	533
Entropy (8bit):	5.448670942393053
Encrypted:	false
SSDEEP:	
MD5:	E2E0B28F8037CB013541CB1CF493BA66
SHA1:	63529E00ACE3AD6C7E7D71580976EBC0E50439E3
SHA-256:	CEFBB3E4B18A04EB4524E441CD7077D40A6463AD247DE93C584E3876D6349E84
SHA-512:	4BD0390FE84812002154A73F533D650BBF8821FF89F69C9D7EBDDEB1C6584F2F47A14DF961A462DB71BE4E5E2A6F29EF40D0984728D7C60B701BCCFCAC5DF5 B
Malicious:	false
Reputation:	unknown
Preview:	43G1x8zX2u1wQIZ4iMf09S..Ch5c0eCT6WKI3K9XLtsCv832cJ143714QjToyL68v53wEH8740JXo33..L29Gv7249F5GFb9PFT42237f0Q7vsq0C326A1117ZP2zC7253 264ChJuksV9Gs1758HU06N51Y..jfV70IY9m444T05gJug0RE210maM0L7345a2a4n4flx61vWNcCR093h317J689K40h3GYm1054qR484..h5st9246rKz03v9yl33R3W hu7I1x6WMp779412q35LW6x2Sxw573VuC4242Qy04Yp6562zJ620287fZbr3zJrgGZqdV35AmP147L603776X6fctTJv7c6..3315C38oq0622233lt92N674O9994F6a5 5D90..70qf6fO3Qaqc93I6mn69laeSMs..Y2S3TLj4Qa8762y1coHFv13ua14zR036m71x7Hc5jk6R76u3KGP6RR3V2y0TdzIK4WCMk360298fM99p597qZ913Cg49yk8w 47n5eV3774Y..

C:\Users\user\68821130\xfrapvxavq.pdf	
Process:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	505
Entropy (8bit):	5.615843821595651
Encrypted:	false
SSDEEP:	
MD5:	950FDC6495BAD979136AAF02E62D9FB3
SHA1:	E0AB0FA6EA977D9DC0A73FA87275F21910571A08
SHA-256:	D154E915DF0E35A56F19058B133FF310AF2A724220553D11255FEC759FE24C8C
SHA-512:	9730DF726E4AEEADBCE3523D509B2292C9FD1E5C5BFACF87D8F586390B6E0077A30B93DBAD2D98DACB5BD60FC7170E778F86D17A536598ABB7991DBF2CFEF 44B
Malicious:	false
Reputation:	unknown
Preview:	36J8o3G4IshX027xN48WdEr50..953022Hc34j63bOaDm24nV85x11288Ou52Dq0GADv0e008h11itQ5532827FQ5924u1LHRBi828P..687ExD2Z10EhMS150z5S2..pY 61Lir6Z9Xj8H6Gz17t2k8C43932N8BRS75gv0TY92s5nIn6E11J559R2gZ6uw2u1wOL58705zzJrkm8i4738f2kiENjCz6ujeedYwX7HWX951wg70V7R1W4RjhQOJlZ043 43KhC4WD1SEM92T609QST..4r1d7l912QbQWq087zoQ483kKyRjs27lUn7jV63lECD056L7eA7hEa4897NFVBlze9V00j55y6ryE52fPLp2Ttfjuo3G46eb14hnMlZs66J HY7vV64DAdB..067P86MXv9582fy2A53O43j5j38K31xd2V207OrQSVS7rSF7FP43A75yPqQ5X4h0mtAM1934a..33B6nU686NVMpNk8BZ7Y4IvDJ..

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
Reputation:	unknown
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\68821130\plfiqbrm.pif
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	
MD5:	2867A3817C9245F7CF518524DFD18F28

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D B42
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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\tmpD317.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):	1309
Entropy (8bit):	5.0990514427386
Encrypted:	false
SSDEEP:	
MD5:	77AF6D1744407EBD7E0CEC16F3C7168D
SHA1:	FF4E58917D1AB719E40C68542F663121299DAE67
SHA-256:	A519EB5414D05AC7565B5399D9F1EF717D6846695221B21B51820AA69120EDDC
SHA-512:	529FD47B0605315DDD60D10A99A4830C234C5046C9EE575524C3FC85105C701DCD8EEA4F2A1D8AE444D2E42A2CEF37CE23FB9A2BAF4CB0BAA91B590FB555E 91
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <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:	B1483611495213 39CF680A67610CAB73
SHA1:	D03541402101682147BE62D35E28ABADFC0B9DD9
SHA-256:	14B1A28480719D1ECBFEAE91305D8537B4F8201D3B4FB9D3D5E81961073DB591
SHA-512:	62E9C28E3F3D3098AD9242D9BC2D861CBF5D0C1A3C22B7B50B78DE83EC1425C50E1A7DF867ED433AB5380B1CB745A264AEB1CB44D1529834612995AB2BF3FC 5F
Malicious:	**true**
Reputation:	unknown
Preview:	.o.3..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):	46
Entropy (8bit):	4.3523814564716385
Encrypted:	false
SSDEEP:	
MD5:	E01C7B4BFFC4D8966DFDD6831E4904F7
SHA1:	FE638E970FB82742E2C4D7EA3AE7E043589304FB
SHA-256:	ECFA3D73848685C232F4B352A5E24F4995B7D55FF4130A26B7BAEB3839280300

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SHA-512:	FD9C41391E076E66F9A65DF18CA790EF06518B8033A5D24BF631E6E7F5EACECF34AD2AA7197FEB8B8FC7ED571A3BEFA0C8C940631F6EE5C0F5996D703B6AC50A
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\palnmuffs.msc	
Process:	C:\Users\user\68821130\plfiqbrm.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	93
Entropy (8bit):	5.076928306598549
Encrypted:	false
SSDEEP:	
MD5:	A66DA5ECDDF5D800F67A0BC26FB9BE6B
SHA1:	7BFE01322CA2F3EAAC90C8CEACA4F0DCDA25E6A3
SHA-256:	F80A7E64AD5BCEBC831C491C4D2B884ADFC9F6C56BB83CBBEB3A4FE4D9904BEE
SHA-512:	52BF78ECD8895F565A826F193551EF792D2FD9522D0A945A7CC59554B76ABBB851382CE35178EC2DECC202FDC413B82D796A0086B70C491A85D3AD8E4B931AD4
Malicious:	false
Reputation:	unknown
Preview:	[S3tt!ng]..stpth=%userprofile%..Key=Windows element..Dir3ctory=68821130..ExE_c=plfiqbrm.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
Reputation:	unknown
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):	7.81968496708789
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:	XnQ8NBKkhW.exe
File size:	1023642
MD5:	c2f9ae069b620080b761d9280473e7aa
SHA1:	3df08169a1cb6ec49b4359e5b580c56da2740945
SHA256:	1ff5df8d27ee5989ad0e7c7270bf3c6d711a4ea6141043dedf2ce7028ae1bf42
SHA512:	595750cb3da3b5c3ead6fbed97d10fec791fff13e38221df6b55abb751e179153bf900858afcea2872b66e6d80bb24e9586444205ae8807ec4e539690931ac24
SSDEEP:	24576:rAOcZEhMGI1altq82FLLZcMdxwI1sDx52gWbh9dlW:tmUh2BVdx/1sDxIrtw

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
10/13/21-21:15:13.025684	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59596	8.8.8.8	192.168.2.5
10/13/21-21:15:23.951576	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56969	8.8.8.8	192.168.2.5
10/13/21-21:15:45.544092	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60075	8.8.8.8	192.168.2.5
10/13/21-21:15:56.081768	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54791	8.8.8.8	192.168.2.5
10/13/21-21:16:22.709861	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59261	8.8.8.8	192.168.2.5
10/13/21-21:16:28.073936	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59413	8.8.8.8	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 21:15:12.912091970 CEST	192.168.2.5	8.8.8.8	0xd12c	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:18.438546896 CEST	192.168.2.5	8.8.8.8	0x268f	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:23.839901924 CEST	192.168.2.5	8.8.8.8	0x88df	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:45.430105925 CEST	192.168.2.5	8.8.8.8	0x1d87	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:50.745449066 CEST	192.168.2.5	8.8.8.8	0x57b3	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:55.969116926 CEST	192.168.2.5	8.8.8.8	0x58de	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:16:17.388024092 CEST	192.168.2.5	8.8.8.8	0x2dc3	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:16:22.595729113 CEST	192.168.2.5	8.8.8.8	0xe566	Standard query (0)	ezeani.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:16:27.958744049 CEST	192.168.2.5	8.8.8.8	0x7166	Standard query (0)	ezeani.duckdns.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 21:15:13.025684118 CEST	8.8.8.8	192.168.2.5	0xd12c	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:18.456738949 CEST	8.8.8.8	192.168.2.5	0x268f	No error (0)	ezeani.duckdns.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 21:15:23.951575994 CEST	8.8.8.8	192.168.2.5	0x88df	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:45.544091940 CEST	8.8.8.8	192.168.2.5	0x1d87	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:50.763768911 CEST	8.8.8.8	192.168.2.5	0x57b3	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 21:15:56.081768036 CEST	8.8.8.8	192.168.2.5	0x58de	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 21:16:17.406179905 CEST	8.8.8.8	192.168.2.5	0x2dc3	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 21:16:22.709861040 CEST	8.8.8.8	192.168.2.5	0xe566	No error (0)	ezeani.duckdns.org		194.5.98.48	A (IP address)	IN (0x0001)
Oct 13, 2021 21:16:28.073935986 CEST	8.8.8.8	192.168.2.5	0x7166	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: XnQ8NBKkhW.exe PID: 1500 Parent PID: 2896

General

Start time:	21:14:33
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\XnQ8NBKkhW.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\XnQ8NBKkhW.exe'
Imagebase:	0x1370000
File size:	1023642 bytes
MD5 hash:	C2F9AE069B620080B761D9280473E7AA
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: plfiqbrm.pif PID: 1700 Parent PID: 1500

General

Start time:	21:14:51
Start date:	13/10/2021
Path:	C:\Users\user\68821130\plfiqbrm.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\68821130\plfiqbrm.pif' mofcxpne.aan
Imagebase:	0x7ff797770000
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: 00000008.00000003.296707219.0000000004E99000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.296707219.0000000004E99000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.296707219.0000000004E99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.301043034.0000000005039000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.301043034.0000000005039000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.301043034.0000000005039000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.296677101.0000000005007000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.296677101.0000000005007000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.296677101.0000000005007000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.301207556.0000000004E99000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.301207556.0000000004E99000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.301207556.0000000004E99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.300915708.0000000005007000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.300915708.0000000005007000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.300915708.0000000005007000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.296824143.0000000004FA1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.296824143.0000000004FA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.296824143.0000000004FA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.297562836.000000000506D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.297562836.000000000506D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.297562836.000000000506D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.300876890.000000000506D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.300876890.000000000506D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.300876890.000000000506D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.296554307.0000000004FA1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.296554307.0000000004FA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.296554307.0000000004FA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.296735581.0000000004FD4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.296735581.0000000004FD4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.296735581.0000000004FD4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.300970543.0000000004FD4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.300970543.0000000004FD4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.300970543.0000000004FD4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.301072228.0000000004FA1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.301072228.0000000004FA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.301072228.0000000004FA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000003.301008313.0000000005039000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000003.301008313.0000000005039000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000003.301008313.0000000005039000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 32%, 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: 3620 Parent PID: 1700

General

Start time:	21:14:58
Start date:	13/10/2021

Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xc20000
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: 0000000D.00000002.520986840.0000000006110000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.520986840.0000000006110000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.514761470.0000000001002000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.514761470.0000000001002000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.514761470.0000000001002000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.521202620.0000000006310000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.521202620.0000000006310000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.521202620.0000000006310000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.519934811.0000000004819000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.519934811.0000000004819000.00000004.00000001.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: plfiqbrm.pif PID: 6416 Parent PID: 3472

General

Start time:	21:15:07
Start date:	13/10/2021
Path:	C:\Users\user\68821130\plfiqbrm.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\68821130\plfiqbrm.pif' C:\Users\user\68821130\mofcxpne.aan
Imagebase:	0xbe0000
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: 0000000F.00000003.333450416.0000000004171000.00000004.00000001.sdmp, Author:

Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.333450416.0000000004171000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.333450416.0000000004171000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.333548197.00000000041A4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.333548197.00000000041A4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.333548197.00000000041A4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.333693617.000000000423D000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.333693617.000000000423D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.333693617.000000000423D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.335726585.0000000004171000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.335726585.0000000004171000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.335726585.0000000004171000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.333596902.0000000004171000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.333596902.0000000004171000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.333596902.0000000004171000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.335236446.00000000041D7000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.335236446.00000000041D7000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.335236446.00000000041D7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.333520703.00000000040A8000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.333520703.00000000040A8000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.333520703.00000000040A8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.333495903.00000000041D7000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.333495903.00000000041D7000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.333495903.00000000041D7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.335366291.00000000041A4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.335366291.00000000041A4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.335366291.00000000041A4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.335950135.00000000040A8000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.335950135.00000000040A8000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.335950135.00000000040A8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.335477883.0000000004209000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.335477883.0000000004209000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.335477883.0000000004209000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.335598417.0000000004209000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.335598417.0000000004209000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.335598417.0000000004209000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.335160851.000000000423D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.335160851.000000000423D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.335160851.000000000423D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Deleted

File Read

Analysis Process: schtasks.exe PID: 6436 Parent PID: 3620

General

Start time:	21:15:08
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\tmpD317.tmp'
Imagebase:	0x280000
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: 6464 Parent PID: 6436

General

Start time:	21:15:08
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6576 Parent PID: 904

General

Start time:	21:15:10
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0x2e0000
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: 6596 Parent PID: 6576

General

Start time:	21:15:10
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: 6684 Parent PID: 6416

General

Start time:	21:15:14
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xf20000

File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.358798925.00000000048C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.358798925.00000000048C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.358078886.0000000001302000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.358078886.0000000001302000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.358078886.0000000001302000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.358703813.00000000038C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.358703813.00000000038C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis