ID: 465268
Sample Name: E-Remittance Form_z.TXT.exe
Cookbook: default.jbs
Time: 10:47:11
Date: 14/08/2021
Version: 33.0.0 White Diamond

Table of Contents

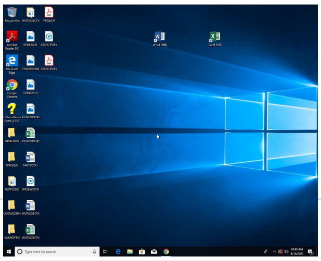
Windows Analysis Report E-Remittance Form_z.TXT.exe

Overview

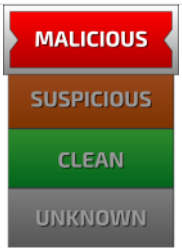
General Information

Sample Name:	E-Remittance Form_z.TXT.exe
Analysis ID:	465268
MD5:	0c3bdc11fd6454b..
SHA1:	1c925518e07576..
SHA256:	bdade907a458b6..
Tags:	exe HawkEye
Infos:	

Most interesting Screenshot:



Detection



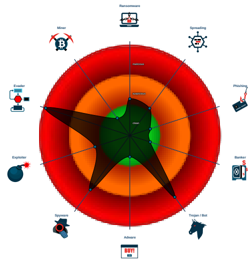
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected AntiVM autoit script
- Yara detected AntiVM3
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code references suspic…
- Allocates memory in foreign process…
- Drops PE files with a suspicious file…

Classification



Process Tree

- System is w10x64
- E-Remittance Form_z.TXT.exe (PID: 5956 cmdline: 'C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe' MD5: 0C3BDC11FD6454BB67DA849864170B44)
  - urdavsa.pif (PID: 3588 cmdline: 'C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif' rpgc.htg MD5: CDBB08D4234736C4A052DC3F181E66F2)
    - wscript.exe (PID: 2520 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\82139548\run.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - urdavsa.pif (PID: 5708 cmdline: 'C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif' rpgc.htg MD5: CDBB08D4234736C4A052DC3F181E66F2)
        - wscript.exe (PID: 5564 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\82139548\run.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
          - urdavsa.pif (PID: 2232 cmdline: 'C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif' rpgc.htg MD5: CDBB08D4234736C4A052DC3F181E66F2)
            - wscript.exe (PID: 1360 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\82139548\run.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
              - urdavsa.pif (PID: 5552 cmdline: 'C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif' rpgc.htg MD5: CDBB08D4234736C4A052DC3F181E66F2)
                - RegSvcs.exe (PID: 4684 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- cleanup

Malware Configuration

Threatname: HawkEye

```
{
  "Modules": [
    "mailpv",
    "WebBrowserPassView",
    "browserpv"
  ],
  "Version": "HawkEye Keylogger - Reborn v9{"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001C.00000002.584515573.0000000000982000.00000040.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87a2e:$s1: HawkEye Keylogger • 0x87a97:$s1: HawkEye Keylogger • 0x80e71:$s2: _ScreenshotLogger • 0x80e3e:$s3: _PasswordStealer
0000001C.00000002.584515573.0000000000982000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0000001C.00000002.586361746.0000000003234000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x77bbc:$s2: _ScreenshotLogger • 0x78108:$s2: _ScreenshotLogger • 0x77b89:$s3: _PasswordStealer • 0x780d5:$s3: _PasswordStealer
0000001C.00000002.586361746.0000000003234000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000019.00000003.580526774.0000000004A10000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87c4e:$s1: HawkEye Keylogger • 0x87cb7:$s1: HawkEye Keylogger • 0x81091:$s2: _ScreenshotLogger • 0x8105e:$s3: _PasswordStealer

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
28.2.RegSvcs.exe.7da834a.4.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x11bb0:$a1: logins.json • 0x11b10:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x12334:$s4: \mozsqlite3.dll • 0x115a4:$s5: SMTP Password
28.2.RegSvcs.exe.7da834a.4.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
28.2.RegSvcs.exe.980000.0.unpack	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87c2e:$s1: HawkEye Keylogger • 0x87c97:$s1: HawkEye Keylogger • 0x81071:$s2: _ScreenshotLogger • 0x8103e:$s3: _PasswordStealer
28.2.RegSvcs.exe.980000.0.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x87601:$name: ConfuserEx • 0x8630e:$compile: AssemblyTitle
28.2.RegSvcs.exe.980000.0.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	

Click to see the 27 entries

Sigma Overview

System Summary:

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: WScript or CScript Dropper

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Drops PE files with a suspicious file extension

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM autoit script

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

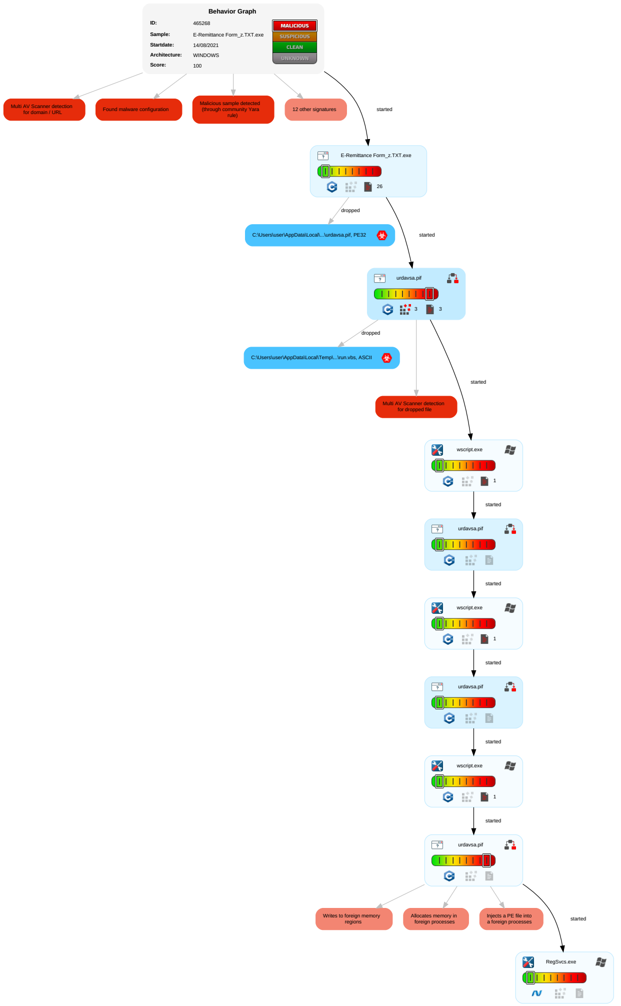
Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Valid Accounts 2	Scripting 1 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	Ingr Trar
Default Accounts	Native API 1 1	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	Enc Cha
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Valid Accounts 2	Scripting 1 1	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Rem Soft

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Local Accounts	At (Windows)	Logon Script (Mac)	Access Token Manipulation 2 1	Obfuscated Files or Information 1 2	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Prot Impe
Cloud Accounts	Cron	Network Logon Script	Process Injection 3 1 2	Software Packing 2	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Falll Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 2 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mult Con
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2	DCSync	Virtualization/Sandbox Evasion 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Con Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 2	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 2	/etc/passwd and /etc/shadow	Application Window Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 2 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 3 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

Behavior Graph



Behavior Graph

ID: 465268
Sample: E-Remittance Form_z.TXT.exe
Startdate: 14/08/2021
Architecture: WINDOWS
Score: 100

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Multi AV Scanner detection for domain / URL
Found malware configuration
Malicious sample detected (through community Yara rule)
12 other signatures
started
E-Remittance Form_z.TXT.exe
26
dropped
C:\Users\user\AppData\Local\...\urdavsa.pif, PE32
started
urdavsa.pif
3
3
dropped
C:\Users\user\AppData\Local\Temp\...\run.vbs, ASCII
Multi AV Scanner detection for dropped file
started
wscript.exe
1
started
urdavsa.pif
started
wscript.exe
1
started
urdavsa.pif
started
wscript.exe
1
started
urdavsa.pif
Writes to foreign memory regions
Allocates memory in foreign processes
Injects a PE file into a foreign processes
started
RegSvcs.exe

Hide Legend

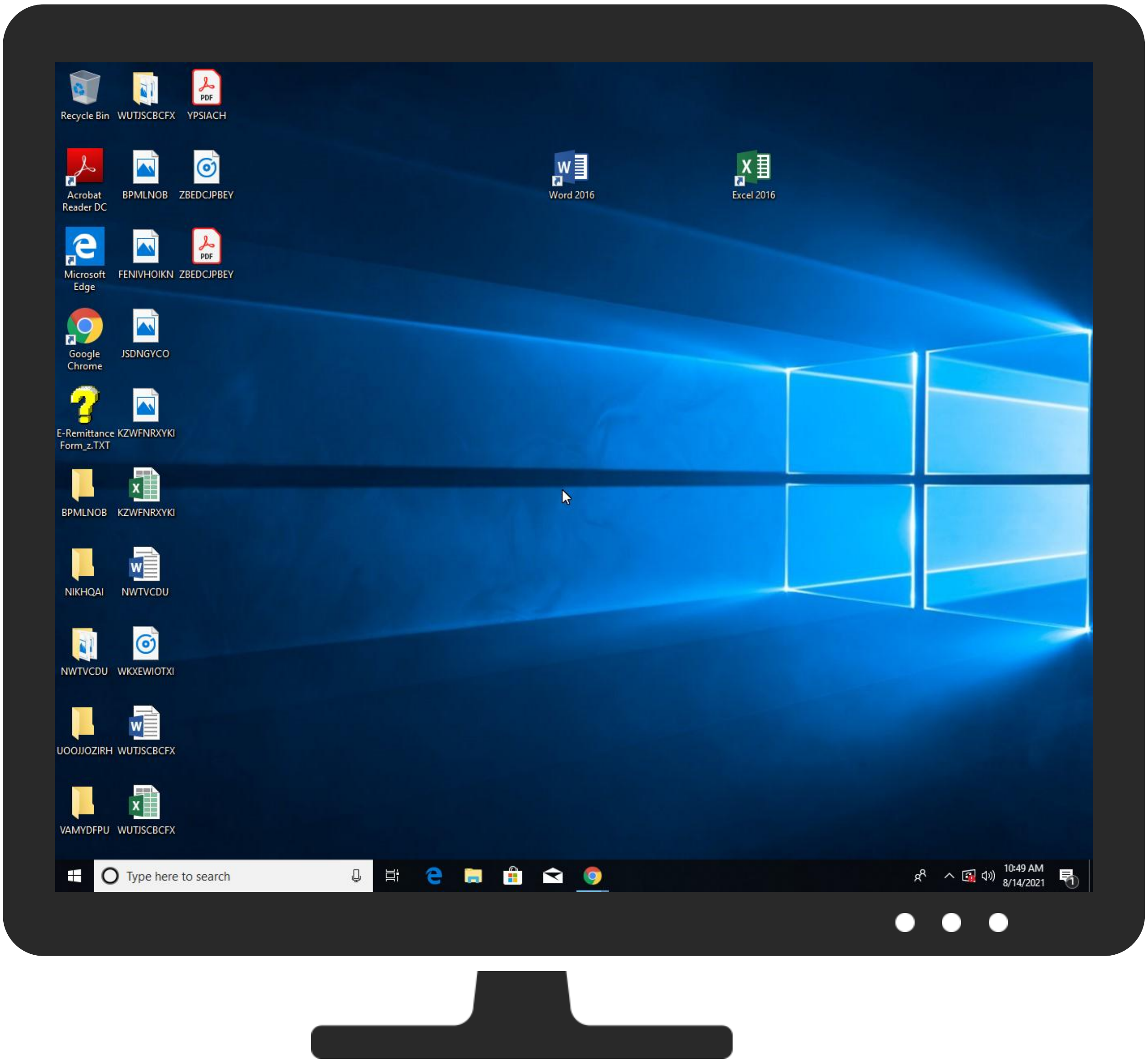
Legend:

- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif	46%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
28.2.RegSvcs.exe.980000.0.unpack	100%	Avira	TR/Dropper.Gen		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://https://a.pomf.cat/	8%	Virustotal		Browse
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository09	0%	URL Reputation	safe	
http://pomf.cat/upload.php&https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.php	9%	Virustotal		Browse
http://pomf.cat/upload.php	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	
http://pomf.cat/upload.phpCContent-Disposition:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	465268
Start date:	14.08.2021
Start time:	10:47:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	E-Remittance Form_z.TXT.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.spyw.evad.winEXE@17/20@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 62.6% (good quality ratio 60%) • Quality average: 80% • Quality standard deviation: 26.9%
HCA Information:	• Successful, ratio: 60% • 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
10:50:02	API Interceptor	1x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif	Notice to submit_pdf.exe	Get hash	malicious	Browse	
	New Order No.0342.exe	Get hash	malicious	Browse	
	Notice_to_submit.exe	Get hash	malicious	Browse	
	Quote AUG_AQ601-LH7019B_Docx.exe	Get hash	malicious	Browse	
	AUG PO-HN512201811,PDF.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\82139548\bsaecqbjx.docx	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	674

C:\Users\user\AppData\Local\Temp\82139548\bsaecqbjx.docx	
Entropy (8bit):	5.540128598208296
Encrypted:	false
SSDEEP:	12:8jKFFAqcUJwSdPU02ikQtSG/pENAJzLRrR4bFy9TcOYXT0JNrBFDQ:8KSUJBT2/PG/pcoogT/+T0JZDQ
MD5:	F0F53FE19A0F58EE77AA2A14F9C1C581
SHA1:	5FD907307B9A05C993E4F1F03A0933977CE9FDAC
SHA-256:	8DFE05B156401A48A206E21B86057AE05529F5F963EBCFFAB763D82B5C43C7E7
SHA-512:	50F08CD830ADB394548D289FD115C0D2A919212009178A10358601B902132FB1D8F7E5D0025516451DF8B6138A974D5D5352AA570DDACC0F320FD030CE351F3D
Malicious:	false
Reputation:	low
Preview:	4vvVKXzLWk06W5qQ2558A8WcwXnYcYzmB79985jTku28tRMDd96crO1mj93JA40L5u835M4..2IRu51JrI8s7638J6SkQw2j24mr377Dn9L5392Q63204T2gR1hnWkoYn257Kq35uGM8izo19EL7O7d0DQ8wEaQ9e7..ll0ph3JAh8P3YJ6d0SWSVKw92TOfs12oX7mkPVzn384SEJ23G1fa7gllQ5UC673L07567McjZ7j6O05TR8..5G8U0d9Q0KYiY4mpWT75H330Ns5FE0646PwR97pI9w63lS202i4757B80L4T97Xy3300RQ4Vm388572IoXLuh1Q57..u43U227454Ld193n67JJA7ZrE1169185019g5jxrIrZ9563s3o5a9UMW1Y9Mm8X611JEn71xwymT58FY28ksb44vpV0j33P2KT6e140O218cN7F0h7pe0z25TA3537W56Ays..YEH7D19428y..z1uDG8fvRbX1337udm44s46A0u0ARZ0Z26R31O8U0mf3rko70635M58w1eIUc4k2724KJAn335N81A7bgM8Hd2403HwMw3e37zH6dgrjjhYn030DYq0319SRcnvqAe5Cf45J7n22T8h342Ix0J392V5W09674638h8sp2ZnY855lz9r579Kf9Y70b6..

C:\Users\user\AppData\Local\Temp\82139548\essmbjocut.ico	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	5.52265483798474
Encrypted:	false
SSDEEP:	12:PGp6do4g1GWuiGzZTKiIoUfGfThmBtmxNrm+JUtgK27hu3Fn:PiDY7iGNKNbfm0BtiPJY0hu3F
MD5:	26FD61702ABAB4B42FF87A064DBACBEA
SHA1:	99F80E74E2A16A5AEC6A7310C42AD7777D44DE17
SHA-256:	543AECFFBDE74DEC8E0D568AB649AAC80E9F42E464395C742D3778D7159173D1
SHA-512:	8A6D42867C425B4BAE7CEA35A8772546BA0823744F90A5D2689CBF356C990BAD2099C5FB10342580FB423D0F2179723FBB54A7DC9F42D5017508F3AB1FE6FB9E
Malicious:	false
Reputation:	low
Preview:	16438L861u45VT60..Ppq3s1Dov26S0P26R3W48YX9V8k10s61fYFwHSz8o27k11L2SmftWB70XN2795470JClr8M5pdj07Ry89J3v0TIr8Qp01D63Q..st7k581q40X0u6396Yf9v48X4P3nc1t7BgT0n5q5Kz6jQ8s9u5P4QY69j4B1322x6k66n3R2j3I6l920xIch951jm17Oj9..7F541mfJuu61BnZM19u5oAG1u3KA4UMGS5L3ka6Y217722zp2iojdTKM56nURfA24680XW29F479v7Z5353d5s7b92vl2R5FbU0tLwQ5m99Ft1I23201T7876G495Q819H1W808033Zxy46x004jch873..yV4kxkYvlo58oZcS1oeB94M5838N8y76C4R1z1AOG5Tk5pFQM64V1ELy9y1zbL908QXfU598VGO326NRDAzfZGL0zr..848O6C9vfu67VYPVu8J75oE0967FC6o960R755bs9rk16nh02W5i62Yi592k60t701NKN1I5GA9211630PGi74M198523hU20Oa1KsbC9N17tw7ogM3i3bIW940a38c042XyEn4CI75LIn..

C:\Users\user\AppData\Local\Temp\82139548\hqlxwejnc.exe	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	598
Entropy (8bit):	5.4952567631528115
Encrypted:	false
SSDEEP:	12:xKxMdia+ETKV5SpyJHWwEVflx5vD/Q1aEb9OLToZui4OJ9bum7a4JOfAUn:4a+EeVMpPLflrQ11xOHA4gRumuqhU
MD5:	358136509F7C05C793B42E886AE6D084
SHA1:	992D2F72C85F9E9745242F6FDCDE071973D224E2
SHA-256:	40B4D24B4FA108163B4D24BAF7CAE02CAFFF9DE0AD75BE9A481006E8ECDB76AB
SHA-512:	65BE9C4A58FD2B57309F3F8D5C1596BA77D00227868B376ED5608B2925B4BE9D7DB38812869F073A9FD0F8366AC21E03FE3EDF7D57E305C1D867E0F6D47EC56
Malicious:	false
Reputation:	low
Preview:	9S50Y3a6FELYQ6458e6IF1krWdeP72RC9yN3FkM721Wk020J563..B73SM054x6P353021KU98s5s1hXLQxD7mWZ21ItncTo8n3WvXPjHOQT4r4yn1jPy9cgc4uo14X2l8J2K436uZC0546181082n6S945j..70ammO64kA9KBJ4K03wj62Yct72702ky..c1pj6878fjrcpZ553ev0q3zY0600600Oso083Q2r3peP13B279zQqlUqL1F1758yQtR3O3a9C98QKJ608Pta5a3w28tG82Y425G1..chx7CqaQ1a61C53NAcq92088i66RHPM389T01J66W5440q4446xn3U1ws6RW85671894MsOonr02JiW9rrDb18017N..Gf1685J5k557pw08I4Kx491642821Le60cE94701N2E095E6948UFy9L4s3pG6ysByHL1B623B6J12fvBb4Wq7x..8c6j..a1426e8R918Ij95W0s3FZ73sm91O4676Hh603LzeFZYwY1S51v37diIW4L330E4Qpn2485Gk71au78K0UnZ517Iv80Q0n5tb03A7rT2Id9JFk7mPHhz..

C:\Users\user\AppData\Local\Temp\82139548\kvfbftnru.mp3	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	609
Entropy (8bit):	5.579508725342047
Encrypted:	false
SSDEEP:	12:7xe5IFyBA/Iv6+TEcR1HIevQIjVCSRh1EivSVmUR:IIF/+D1HILIj5RjNKVR
MD5:	3995C00C683ABAF23AE16274E0E84A2E
SHA1:	0DB8A0E5AD441ABAAE7ABC1BBE6F99B1E05B6D48

C:\Users\user\AppData\Local\Temp\82139548\kvfbftnru.mp3

SHA-256:	E98C5EB50F09EE0551A5032D91953CBF960F957F9C3C653E9E542F43D8B067AB
SHA-512:	0D14D57560CE01E112BE1DB21DFA066F3CC1BC2C1C7F9BC4CE5F6B3F6BAB519F4570C9F03BC1E2F16093C3B006989BF072CE496E91E45D803C232C3C93831CA
Malicious:	false
Reputation:	low
Preview:	600Q663w9e85ZI545fw715Wb5..3zs327583TLd43A8lrMU40P3098pe9Z580raeF7AMjgGKh0Ii9B1Vm2D10391Vq01560I11n2S128rB52j460q301c0W12sHN0m9976 aClWNy8RcP91yKK0Qv281W41lX5526V5da2b4h9lpvbK..128eIK84x45x92542TZ5e4D4ZhxGJYdzMG099KkF9emIV9780FyeLfX8dX0FTX2L9B3RvF58c278kR6SXo7r 48..V32Qq773Lo4t5c6..VC8qaqM9Dd1Wy6XBET3uGNH8KHz29n1K0NQbh503876ly9k6hcT02FA8HXE1742oiJSi7iKG3s8q42rqS77608dh03R5I4..0tni8FA404cd8 ltPoX44Tck57D94YN71qu8e310r4U8Y40r4a6u6mW71Lb9fB09y431K0Bw05E6991YLl1fKoBMg100EMb781MR17cSP0Mf..fKS240YGL57Z8bC33iPnU9uq3rBQ60k9j7 34I25SKd92A23a7SjV76xx643Bn7IDu056J5LK85N56wp6QEaGJ9Fs53VU225UkY8yED56pLG83KfmCb6i1n65U..

C:\Users\user\AppData\Local\Temp\82139548\ledpu.cpl

Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	583
Entropy (8bit):	5.452460739145846
Encrypted:	false
SSDEEP:	12:OAqaKucRSoJDYJlN4UznyA6Rb6srSiT5H:OAqGh4eWwsrSiTx
MD5:	A1563EA76BB076ADE23C8964AD9D8A9F
SHA1:	279087601847BD60F01AAFF79DAAC385649A7807
SHA-256:	E0E570841AC7D8611AE4D04E6D50933A2651041BC3BFE07299C2280EA08FEA2D
SHA-512:	0BF0C2FD38A5C6499BE40649C9289BB47765934268DC412A7FA868B8C4BAD10A1DF6AC9E25B30F095894A1003B1909134FC24AE4B06C6C206AC81DAAB8114FD
Malicious:	false
Reputation:	low
Preview:	r13C3j49..96b24O..Ywg4P0b0N2889CY9a899y7d3835W9D6YZ9bMkZAoO7a86z58bc7L95b23VyRp14Qe1IN98pkq738jPyg0d01hV96516I5I..205l47d9y09368No 4KH0g8Jo4CN8wSJH6eM4xM0Gac12ads6142FW5j2F16FZ920192DiQNygum8VV118W608rPY5C14614th0DP5ys26K213Bfq355C0ea3jaPZrdEnrL6Mywf82KN..OHbEX 29hK2gu9PF0y75I6j016K3gtc4o7K2LsZHN79XnGR..oBF986K1j8Ids4908Cuc1MRW3b2170V35990NA292Gp3c..i5Kj38Bj800Y2641R74T89Y1e0d258Y73511dpRR 5R7..7M6z1783f15F98384oWeD..672QU3e5KSJJPLDC50Fu1FkW8488o9m695415gba54S0nP30Gh7g6T78ZCp392j7494o3P20Y94..mK0349511661sHI4b93Q588W6 2uzASs303r7LLf3P46f5G84q471YV3hM0v2t59GN78z680R841654en9Q9A0j..

C:\Users\user\AppData\Local\Temp\82139548\mibt.ppt

Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.577691894994689
Encrypted:	false
SSDEEP:	12:jbPxuiUCHHWh8g3qRyPXRX0ukC5Hp/C5tMgv543NLOprhVi45weh:HxVH2h8tkX07Pt57rjDlh
MD5:	18BC4D9E0FC1B64E7ECAFCCEBE8FF1B0
SHA1:	E1AAB49B15223B7B28DF4B376C896AF975D60D6E
SHA-256:	1E17E644516D5F59C0BA1C856B6B31C8AECEE8ACC7CE092BE36FFD0637E08E2B
SHA-512:	D29E3780F6B0A73BB1750855FAFDBD278E5524B2A8E73AA9EDA640C355ED7C5183917799201CAA26BDD5021564D87403DCBB9F8CBBF4FA87147D9DBABEEB5C69
Malicious:	false
Preview:	lU1hB8v2121bC55Ut07ekzxM6wX5Ej16G29BK758748Fg7s12Gf9..mQK12SDs9oPOL0IX05617ij79STO7K9PjTv3KEvIb5SE5Jvm025183F922DEsXs84C0o648M73Gq 445v015joQM89cnn04K9Vu64mK0185Z043N26490mw7Tc7543310BM7x6isH2A3TWUz0i992YS1d2KIblr153L0h1t..3Q5MGr6VW8ZYY6pn3q7UKK1934898IYp..yuhR A3oY044W1g3p2320hiU3rd4c9062I7..71Xy12xC8i0t3Rmz17l2wqs85rN10E20TfR0W4467WaahG1Iu37Z51XBfoiI2XB6nZfJXjgt85FQk529t5..iy3YDF55m1G25A stL8fXu1x1dueIC3tx07ZM8hex60M463L9DGs3IZ1NFVqcN8xdI6Y9R29w04801581oZ4l0s755WcQAV1gX1572mrw357QJw46..0V1l1d30WC678I9W8a22em9oR..

C:\Users\user\AppData\Local\Temp\82139548\ncplbfrqpr.txt

Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.509377507232657
Encrypted:	false
SSDEEP:	12:5rEvOmPSPK6dSwh6J2oGvQXxGcRXNU9ZCyLgV2FdI4h4VVANA:lIfOdShJbGqxGcx63rLgsF5WeA
MD5:	0B8AF5DC59BB7CB4FDD0B0F7AF3757DF
SHA1:	C44F230525060FBA3C9ADD285F7801119933A796
SHA-256:	1E46A71EF3CE0502278DC55F187B52F23029FB0B55A948A32D3E28E439A82812
SHA-512:	D6744FAFCBEB11D7D6A6F58E88B9410F4E4A0E18C08362E14F39534E6F553C4E657BC02C476AAF57B6357E5C1E224D4F3AB125028E11564C4B43EEA1700B19F
Malicious:	false

C:\Users\user\AppData\Local\Temp\82139548\ncplbfrqpr.txt	
Preview:	2E8xGXD0fLj1ir0830m1Et6365JK6Nym46h4824o3O0dDZ35TF66775Mjo0rp8fCt6939yD9a54imcJ770x74Mk5M16E289..7Fo9rs6989Hy5v6670I8g3DT9Ftl2868rhF5FgV760806989UnJO0qi43bA1rUoVF9Xh53Dxej76Og11092CYtX7e022bf4CpB893YYXgvyluHa798sr70855OQTnC4zi3Mb34N3j850V086624n5x710h9087Q590d0r9GO39..j39A0Y21ljROV69SHXWn9949bQOZNTPL632j0816270n373002N55eHtgdRZ73lAVVdcA792TzO5422843DI98bD91YrW5133pUw345Btuai5T17zGEQ3C3096u2qa7802L7ZOz8FL02F3suC2OyU7LUT..Xc14XY85AEGTpg74665WL4xqTLrw3ur7854iw72jY375oaOj3N..Bg9jo8XNhvgr2XPVG49A02448lP51qik8T077UZo..

C:\Users\user\AppData\Local\Temp\82139548\pojm.ini	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	545
Entropy (8bit):	5.467162535814078
Encrypted:	false
SSDEEP:	12:M2GC/8WPHJGcXPnupWMDYfvd21KXbawy1HXcD6bbfjDQ7BXVnn:1GCJYSWpWMDB1MadKyfXQN1
MD5:	A4DD3AF5059AEBF0C30F2C56E4CA5164
SHA1:	0728B0DBFF92F39DD62BBA076F840A3CEDDADEB5
SHA-256:	7BAA9365B05C1D1A6FAA2366A8947AA8BEE7F1029B4503A1430C1BF18B10AA34
SHA-512:	2D446B221C47D3CA44D8E55517D83F1A7D38F7C4EBFFB3E270EE46155142B2FAB37813C0CFB0DDFC5E461A64DD775F94E6A725E6733FEB3B80E443CDCF92650
Malicious:	false
Preview:	FS2Zs3f3..m527217xm5Mxp6V9ms29tQXXvA3g8wR26Gf2486l7fZ93hJC2Ac6uYe995XIF26P254IYKS4lzy3767UGthk18Y3Li..0tlR188c3m51nZ4Y4k316t9Hm..17450Z2CN34539dY8036B0M482E604v70eu4G9021n222C3I063K97118qN8Hk3W97R583rxEyeR5kqRyF4PR382f6..8542liv3yz92WZsn9d1gCN73oFG44f3E6AecFZ6lM3zeOk231Mw60I78d5563z7005LHK4P017V2R56R08G7490Wnixm2563Lge6Y7g5V4d58R1QU8D46n85u09OZo844I3cV711f..44101E52W12768690G53qay8DMq9Kp01jY73p47n45jGs3nbKX3417v9O..t23j1ESR4O1u6V66Fajb932d49Wb6Aj8t81..2jVX4150Np1Fr31236KNz51a32mC448cVXXsrHSn5x50V50g39r2z4YpTogfH5iCMCQ559h331z28Ff43olV34V..

C:\Users\user\AppData\Local\Temp\82139548\pqbfmorxw.docx	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1183730
Entropy (8bit):	4.173093630730597
Encrypted:	false
SSDEEP:	12288:U9qJojg1bG1qxYtA3/7Ulx0Q/WNfK5Fwd4TvnreBQPkA/Z5RYN8LN+hcGx2urb:MH2uw7pQ/0fd4TvauPkqzgb
MD5:	545E57CC8251F56FB77DDE769CB11C97
SHA1:	342C79300E6CDF7644EDA1C72FFDBAA46BDE55F2
SHA-256:	7679BAF73789098BC9D5A04C82DE4B5CD2AB209A0B58F9ACE561F50CF1EFDAF8
SHA-512:	5B03F06E530B17035E2D28E8EB2B4CACA30C9ABCCD0C100261B0B5BD51BD8EC3A08A1CC36945DA9E7E7AA408CFA393D0A310E175E07013DDA9ADE2413638D25F
Malicious:	false
Preview:	FC5i133DE..aH0G59ioQ439qgQ8d35q9Dbc1672ceLPLd5..80r686u46..drwd2teq80Lj4mjs9b3Yr3pQ6el63Q98do1D8jI14XE..4Bi939d8ZhJ8u1NneWq1i601g45u771nKtW841il20oHaY8V99cvNuIM1xz1rgSE5T020J8EW468z3LdrX85sYvu66P6..u98sfYg3d6M12ca1Sm25W8Z44a5q18I1p15PYu4eZigX7Zz8UOa3702943g046Jfm11z0078s..U27IICMS5GEA5CU9r2d27j1rE17i9wC5M5Z1m048uf29sI1I1Xz303NlK3L33vf67PNUN8De2SLBA01..Lx7N7s38tbf75th83sR1p1034K7Z1YYpV6q7357b2imX6O1Lrp7338e1O09te3b0z1q2UpS5..7g14Wkbx14u62WrJ2689Oy67L77o7I1W7Ff65658E92..jzZU159633sDkY0ndn4hjt0tDq3R6q7207NU1WR55v7M5840..QcN4Dy0a6o5izZp11Z0S908LU56K41B3zER99Q80jD9tecv..1U185a399feP354Oe1N9Q0YSIjf924160FP956Gx..2I46kS6El695Q577CP95sP09z9744zh8kc8D75zTQ2Aj..dF53A2A48iq7Lf75953sh6NPV3..Ha983iZ740188xj60m3Aj743hU9H9n581v80..U390g61uG0saZwGntV5pviLdE2XQz5z3520z6a4WY6Kl..3Fa7p6PpsnX5az2y6Yg0B194t6Tdsq9WOlb8HPY9IK2h2C5Ul4V0L92uQ3396bVP0TK43T5RWP870RjS9gP8e1Su11H..m74osL906203f338s6cW6aj737gtKWB1g478E9o7P70VMCl4108miy6u788576357v2..F07iMh9h763A8rq8EdWo82F54u1phYFP9376y4548DfIrS435..r2115fmcj3MQ1x3

C:\Users\user\AppData\Local\Temp\82139548\pvvrt.ini	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	606
Entropy (8bit):	5.4640654918354326
Encrypted:	false
SSDEEP:	12:gQ5UVx1yVs3N+VQbL4rTwtW7FATTecTVqTjKeeA/YngJzwJMSPS5krov:V5OzaCN+sLzW7WTDxq3KeeA/Yn+BSPY
MD5:	6A2411B573ECBA959EA1FD48109FD0A6
SHA1:	FCF12012579E72D3E64DA520A0E76676E0B3D493
SHA-256:	249752A301B6EE470D127FCE1684D58AB0546ACAEFC8C9CCCC989E6B49D010AC
SHA-512:	0FCC44D51E520FAAD763D06D93F667E4415B43C90E83CB82CB09C1AEFB88FD8156608A95B602064C1D545FCB52E09E1BB198ACC12AB1481BC7A5E1BDEF986D9B
Malicious:	false
Preview:	y45QD105S35979448QC30..c3016AIX5aY9qC45q29y3T3HN7Ivc5G6Tx3uF93Sa5ZtqNnE7i52o5S..6t61U855r2ir104vDEr0Sjg4LZhmBo2E515mQK97C6aC2HR58157A16v7tdl540XozJ2T552st30y7R48N01cn222Gb4H27GnK60ugB4251d53n06N7tJhD2xH289770sA2Rlh20xkTX8n6J87m64AH54T5033..50ww6Z8Vk37X3M9ghhhe24D12Au769796C54Z2..b1s5VB54fqf261pYPTiKTQyEJH3TX141l8fH8M36531125OH2626yza845UyeZW02230511411V9M66Fa98T0jHAN163..w0Ll7hsB8fne9ur7282kgXXI68263E192GQKT5Ff6Bg5608y8B0y1OE7h3KJVHy493G..4657E4Utcon6029l9TgQFe84..dc24x4294SrJ7582081X7i3L28jrS8z1440vSR8lE21y355GB4m1o33j896U4t3fR1Zx8418zTSkWo799ryBg4V43Fym6R5s16wXAEQm1F1784qZ5C4548G16d54Cjd710GQyz4..

C:\Users\user\AppData\Local\Temp\82139548\rnjidsxil.mp3	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	576
Entropy (8bit):	5.443753737781502
Encrypted:	false
SSDEEP:	12:p2FRxgroJLu3PUWdaFUwsroryyVmCmn5MGbpJAcSaS8SzDtAQUByc4:iwc4iyZroWyVmvSG74aSpDz8yc4
MD5:	398B0A5437BA24AAC3CA3E573360F9B3
SHA1:	097C4D23BC17BB1C670C2D5E91E13E4BCE5B1405
SHA-256:	8AEE1198832808676ADE13F08E17B01D07A91D69C3B88B6967516E7CF9256635
SHA-512:	CA7B9161F63D4BB7939315A4B2A1D2336E604B5E1403EFDBCEFC74A6464090CB874336B9754ADFC25E9370887CBBFFFAABB17C3BD0FE1F87F7ECC9DDF6CCB 937
Malicious:	false
Preview:	3HHI09vuq31zo19XXD9DAT820KvXHJ0431UuV808ywv9257347lH072lg3925k8Xaz1O71M5S14217KdkOGAoF64728R143Mrh5cH7Ln37322v1n247LtcXMb6SRk..I62 4l2wgd926z14192re44ND68829C48R836XBs8200Kv5m8aV1Z36PM9zz86O1iK166368Q424UpKZb2ncC3SMBx2UmE4l19SRf1F60083W4w..3z26610ZUvH U6AMZG8aW6p7W51155M2687cS3a856H0..9i1WKuzb86C1578432fpM99UfF2Esb0k00334bTq246lOy296529o0QNK942aS6s995xe434Ws58dizfI25366480f3C8g38 A0KisTxOs256g89mx91i5QvY4975ZTuZ4q0z3U4E67s0x..w2V612TlQC66..E74KxS5i4T6ml0S3ZUlX36A2rN121Va74eE758sW86yY3n97qdQP3Y44w1h9798kyTd3r s8f9W42SWUoA6r8z8sM3q451o2kG28IP5G820222BE0u0X3Z7VZZr1i05r4I1Z6N..

C:\Users\user\AppData\Local\Temp\82139548\rpgc.htg	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	data
Category:	dropped
Size (bytes):	104576560
Entropy (8bit):	7.097392671031914
Encrypted:	false
SSDEEP:	12288:mGaSGa+Ga+GafGaRGa7GaqGayGaLGaiGaKGaoGa7GaLGaJGanGaDGamGaZGatGai:+
MD5:	5D32075EAAEECB2F209ED24D4676AA39
SHA1:	F0913F914AFB1A9CDAC9FD48552A22376EBD5A25
SHA-256:	AC616BEF1065A0D60C7731DC2AAB0B795D4471239B6ACBA9A301BC1290781214
SHA-512:	5FF5A1B573913974F5E47A7E749C24EB16EABBB58C0D40297CDCF0B6AE3A324772626135E1492815185095964CB5D8826714F01F8F4BC090B6E527A25B4DEB6B
Malicious:	false
Preview:	..;..`$....)4.S.i......#.c.s.&..........9.{v......u'..C.6r.&J..x.mTFXg.....;....{p&..V...F....y.4.1.7.m.2.a.6.i.k.9.7.8.1.w.n.8.O.3.4.0.h.6.6.6.A.4.5.8.n.1.3........g..<.B..n[.!.....-..2.;....X..!!x.. .Z..C..#....f...N..$...A..j..wg:.):.<...0.>..H...._F.TP3R.v........X.V.4.9.L.7.8.b.7.u.y.3.8.T.C.1.7.....r.H.j.q.V.5.A.5.9.B.7..........yJ....-+.L...bX .{S..:....'q..wBM,oIGE.*8..4>...F6..'. ......R...>XrNcZP}.T._.tC..........s.s.Y.I.0.9.4.Q.9.3.3.7.9.2.s.t.7.X.1.x.0.3.Y.6.C.U.l.3.7.L.F.1.n.F.9.J.2.7.7.5.g.D.f.W.....trnB...x....5...16..I#.....RH.)#M........ML.1.+.E..W\........7. .^i.r..-.\g.l.J{.}6..kj...[..Z<..r..j..T..r[.$.#.!y..r>x_.Bh..;...,....?.I....tyT...m>.o.7d...Qs*...8.......-.%.G`.r&....s.P.3.6.9.L.3.7.1.I.3.8.2.3.n.0.Y.e.6.4.6.9.N.Q.p.1.Q.6.3.H.x.6.8.m.W .....ss..g...;.....^M.W.k..b.f...l.Q.}<<...../....\|....-..u...".7.[g.UW..3..XEN..L*v....w....+v...s.cw..H.R...6@..<.u1...qxcqj.H.uR.S..X4..........m......I.....BDp.o....L3 d7-.....%.......X.r....\|$... ?.>

C:\Users\user\AppData\Local\Temp\82139548\run.vbs	
Process:	C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	88
Entropy (8bit):	4.6051756194659905
Encrypted:	false
SSDEEP:	
MD5:	CDB722E39D2AFD726FE91A0D3A540E8B
SHA1:	8EED8DDC0948243039A2286C19317EE58F4DC28D
SHA-256:	B80412F79C971F1E886247CBBD553951793AB8A3388C8A81EDDE54C555ED3666
SHA-512:	E5CF20D6DB82DE3A53D2AF4EF1A917D0922D111BDB5061408EEAB21F31D6F257E2FD0FA8EE1B1D40260489DA7DA34D0558095962DE4FEDA8BA34E6551A426E 6F
Malicious:	**true**
Preview:	Set WshShell = WScript.CreateObject("WScript.Shell")..WshShell.Run"urdavsa.pif rpgc.htg"

C:\Users\user\AppData\Local\Temp\82139548\rwvkj.jpg	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	529
Entropy (8bit):	5.405323351479462
Encrypted:	false
SSDEEP:	
MD5:	0FCF9A109B3EE20CDB79E59015830DFE
SHA1:	C2E1FFD870CC57A61EA2608DD691FCCBF04B46FF

C:\Users\user\AppData\Local\Temp\82139548\rwvkj.jpg

SHA-256:	02B8CB179E2F91F15AD5C1D79F9DD326EAD86A3BE5A8F3ECC53CFB1AA9A2CB43
SHA-512:	89233BD37626B44D53FFA150CB7E377C5A0EE3C5B3AF40CB95BC5DB511A69AFDA54075C264C0B3E5E9B291758D66A9A87BFEE454E105A453B348DE73F6F0281 7
Malicious:	false
Preview:	D2H42r56l925273967OEU34AJ7d6X2yW3583..55d509cH4034DLk5Pj998S4Gq30201U1uNQ94s5z1GAI95nBKs4Yp2080N68DWM3s842OEX6FMnmDX6a19 vK51g02h16lF07qg99..x364P87a6mB7G71hw52z426H21Ij4Q8Ow9bY2lYg..0gKy1u9o232fI25P5BO5802WW8y1T5j8V83rmcZyLSi86v0492RF35801808199169R7 3838dbS47649o8c97W1..8187VP97m0b844n61LXL999MRUQBbj1lw2ymk78..M63676K4M45K6F7V759sT40ddFL3p38RQI8pL1jx7cb5..1A65YS0zW0361f71EW5U48 W2N4yg3n3614Kl1D37Ia58Z27DM2kgf898009nI9QCt1naa9leu9xkd5q395Ij0Ll4FG8A3H854304W63t4wXsMOf60dz94i747Ubt911r0dyxu9p44a0x89848258I240 80b10240phWk4sNkU..

C:\Users\user\AppData\Local\Temp\82139548\sggjqlvp.ico

Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	684
Entropy (8bit):	5.448992123973903
Encrypted:	false
SSDEEP:	
MD5:	3BCFFAB29A55B49F02607D6FCF61139C
SHA1:	E6B260BF6C2219EAC6F0D03428B8B7374E5F7663
SHA-256:	872BEAA2956D41732F6CEFFDA078F288A39B963174C9D4A1EEBDB40047574A01
SHA-512:	2ABA9382FD064A1BCEB6C08D13E73D58700B7F991E9BD576F7C700D801849B29BE2AD82E4CE3654EC35499F89D570E7BB6D561AE0B44FC4E1C0DA35E72FC51 B7
Malicious:	false
Preview:	C97Q6a2y35i9859iwk..Wu313635285R1Zqg7n4ASp75N256taU4gr4LA6SRpf597D427q8aBkCb4z7303Kk0324130iw77qE2R..84403UPc064viG4sf14F19e72B7i4 A45942b14PX0t828jQGa4EC7Q67921XKys7123d32trP59a69SzMk90y9xbY5Wx3M0L1XL2P3rp13LMg59..b2m9EwI279T2v8E66RN0l4G0bpz1w869O9b6E3U8e1Z67C 44gpF6885r0411oUL3472039453YDP5cfWKdn8Kr50k..143H15..2G29R2UC1J8s..dQt9Xido82Ky5Uu6BVi96f557iR722Qo0H0VJz7919Oc31P2257c1767K3o7n5G 6..UXK433H92976q45033rP0zs522C647ZQKmOtvaMZ13j8AgCZa6h1Sbd934nP9u5UqYOB6fC0LZABus8S8o7XS8UQ2599A6H64ac01O7ck..80nJ9A19D1Up3654F3c9 8ZYoV908Sw7A6P7hL693FY404m2PA5263u4dm5934Ld5YW6724010181l6w58u3K56AfGK9h9P82kSRKmDl1kJ801P3D561V15LP0Of4NEcSO75l568j29j691EI566Q0T d5359b307m7817B0j8MT9003PP6982LC..

C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif

Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	662256
Entropy (8bit):	6.573686718539873
Encrypted:	false
SSDEEP:	
MD5:	CDBB08D4234736C4A052DC3F181E66F2
SHA1:	6801A805B6DCB760E8BF399A7D3AD0489FEC7BFB
SHA-256:	07E5F6D7EC7CCBC3D742658E9161D799934C6F7F6A3EBF560F361B4EE1730B6A
SHA-512:	1EBD1A546E64D4B36D4F143FF7211D953F8DB8E74C739DB5E9C0939A6EB010A461FD1368F8A7813A8A2DA804DE6993010075AC21E4917D74D3F9394EAEBAFDF B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 46%
Joe Sandbox View:	• Filename: Notice to submit_pdf.exe, Detection: malicious, Browse • Filename: New Order No.0342.exe, Detection: malicious, Browse • Filename: Notice_to_submit.exe, Detection: malicious, Browse • Filename: Quote AUG_AQ601-LH7019B_Docx.exe, Detection: malicious, Browse • Filename: AUG PO-HN512201811,PDF.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....... ....@.........................p......).....@...@.......@.........................T........2...........D...........c.. ..D............ ....text............................... ..`.rdata....... ....@..@.data...X........h..................@....rsrc....2.......4...R.............@..@.reloc...u.......v..................@..B............... ....

C:\Users\user\AppData\Local\Temp\82139548\uummnexccu.ini

Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	518
Entropy (8bit):	5.421084621909537
Encrypted:	false
SSDEEP:	
MD5:	28632856AB37779B2BE85A9F6482747F
SHA1:	9B473FBDE596F68A6670B3663AE13FDE02F0B8FB

C:\Users\user\AppData\Local\Temp\82139548\uummnexccu.ini	
SHA-256:	AE08F906B87EFC7475D9D9A75B6CB95278A59EC81CC10A40F9E191C99732ABF5
SHA-512:	1DA6835A4B366384851937E246A2F9051F78EE4D94F999290B095FCB9CD4669912D62AECBB51AE42F6D4B1B67E0B74B9FE62BC442C2AB5C08A134C36A30BAE7 F
Malicious:	false
Preview:	EPS4t59X5285j55jyw2381d63W393Z2Y18JM85I73fTio37100H44200Kh520sK3712xk3Xj34451Z1I1x6132beK10q58603hYjijn3L73uCk1B0440fU6M8y381G4611lf4n..7Qf8X94y7107P5W897Ui06Q10..55sObbFkyC8179RDUg3u6tpiQ9x8q09J062Y5o0fP717qHp5B21..vm0s818478E916S67D0k..26OKGyHGMod54WYQ6WT867Cb42135vIUk5yAh8T2g02icE6eE1yOYO78A4rDSlz7JC2x56s30QiGa08I..QDYA37B1J1gH0e95qH4FP3LN74733078PAR3Y15NrKX9I346F4gH4eW3SH12K7x1OItCy..498v444U2vC5h20KWP309935116ofFx36BBobxliuH71671a73d083h9k8O5Z0596435Yy40QF9tsPe074176l19Ci0dLF3612UI7f2E8c85J8Z19oXRCn03z3388..

C:\Users\user\AppData\Local\Temp\82139548\wdav.xml	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	565
Entropy (8bit):	5.618694035615005
Encrypted:	false
SSDEEP:	
MD5:	7188C2DDAC3FE15E2B779A3DF36E0046
SHA1:	C03D1675326D726B14ECB4EFE2D7C9E5B4516242
SHA-256:	F4198D2447BCD0A3C4CE6187A9E879DEF55839C4B78796A179F6E95DAC90F79F
SHA-512:	2FF433C18C27C3D088E6908D77D38F6FDD2CEE325D7D3558256EF7952790516E5426FB99590F50487201D225B9BBB3141BA99F06166994365B6F206C7D0E83D9
Malicious:	false
Preview:	NE15..059g42J7six1S4Oa8t52b2N5tzF066cI5X6..G2fOc2C2mjJ62u8DTyfk084wBco8KHn20FX37R92Vcd90B64KppO95T12P55YX1n940x9JjiP73979RG..XXFo8q6FyPkd3yL9d2zaiO5e1lz83vhW..2R7UB9389be9tK1f79P6CZp7EyR8qHY183z7pd9101h2Y76jzRn882s5iS03m5Vbb546C..5YLURey4b01uAd947Q8nkvz69e55H3yhi0KG26Gei0e3f8zxtzh92lh7108GNAwT151pJFX010w99g22RRIR44RY60cb3W32SH2hgf6..z1ggg0xh745FP7lh28o..71Z0519th197Y3..aJI4DI0c2RSXXpgdso4KAQ54yaU273D248ZiiMH14t74w2679kUusZbM598o5xBsZm7Jl1Z2A70m5ie2xJR778..6C06217oRx8oH8lf6u9fEsGNF789275QKdzYI38hIP2Q3oH773xZ32bXRe6HkD5X8G4qif6t0j8FLzgq2owBZ1Jt39ST5Y2IGv3s1Q7..

C:\Users\user\AppData\Local\Temp\82139548\wvjnbptk.exe	
Process:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.48021842881949
Encrypted:	false
SSDEEP:	
MD5:	52C468E5B63BD119D9D61B097F98001D
SHA1:	10C1D028CB6060644D81C8B1ABE108A093454F18
SHA-256:	0846B83011BC5C400ED8756D5E1CD2E35B33F9B77F3BA403F4A21C956F851D0B
SHA-512:	727D42CB5F98DEACD628D76CBAC7B1A9344224A9B948BB75102367BA24551CC82274FE4F399A853AEB0C90883D3FBEDDE72860F6945C7CB137AA7A6C5DE04E F0
Malicious:	false
Preview:	47110gZ7VL1u2HVtodciI3..Bx465T92fKNVr6lqD41Q384p94M7VV8IIXCw6W2..4p4P7C1Y0632j1y2vU692PPD5DLO1wc2f4j14b1Z9145iyh4T0WNn33o70JfW..6dQ1ROU87D3hnP925374a4g6o3K907Q61h6ug6500969G9608597012F1aKs6f6y24H88OdZfa7hpR9kcWF3b661c3za..t7R3A4MZVE47aIB3rhg28..24PgKQQ60235h1C71V6Ve47j8h0Dq2rZy33428Oc1370Zg4f5u07r21DT854122F337V50q8ff51K4Bt86d..5Mj4u1FYaZD4oe3h0268t4346yGyb8u1186e1O3Zv6UAjp4U306iW86115241AL9vvi0GUs295i4faXB1K024iI59lP15dfl2n18JwltR5TIUv0T8D72q14u065Lj94A0vZ80apPYxX1BLix9..CvI94401hp08sr3kSA91zaGLnu24..

C:\Users\user\temp\pqbfmorxw.docx	
Process:	C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	70
Entropy (8bit):	5.000801324663666
Encrypted:	false
SSDEEP:	
MD5:	E476E6BA62A9C4AE9762F8B817B28136
SHA1:	46C94419E4D7066EEC9463DC636B15817C6E065B
SHA-256:	552015B135E3564DCDDBBDF1DF5BCEF916CD1729352624CE65904877FD19844C
SHA-512:	53B38EB5059C0B0F88B26B6CDC74C33D4C5E4B6B1B409E86640AB6253B612B1AFE3E48D038ABFE703860B1CBC47A8530EEC06B176BE7846E094C28474917B73 4
Malicious:	false
Preview:	[S3tt!ng]..stpth=%temp%..Key=..Dir3ctory=82139548..ExE_c=urdavsa.pif..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.775012373250531
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:	E-Remittance Form_z.TXT.exe
File size:	1441541
MD5:	0c3bdc11fd6454bb67da849864170b44
SHA1:	1c925518e075761758a47f677016c95f5e80c92c
SHA256:	bdade907a458b6c9d2e87af5667c3b8a16aa7804535634ed662b0e07c34f64b1
SHA512:	b75c5e2967976c5df69b7ad438b9dc26b68accd1fe707575f396b3926e16c99dbf7fd4f30815430e5160461793de9f7897bc2660307f94aa8795a01220b7ad9b
SSDEEP:	24576:rAOcZAh8BbGTd6g+HrTWCGMnuce4hXQoVUsywK6ULRrAPWcBfhNQXNmrKb:taRov+LCuug7VU4KVrAPWLIrKb
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:	f1fce4e630f0b0b0

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	0.600210336538	data	6.36873857062	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
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: E-Remittance Form_z.TXT.exe PID: 5956 Parent PID: 5868

General

Start time:	10:47:56
Start date:	14/08/2021
Path:	C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\E-Remittance Form_z.TXT.exe'
Imagebase:	0x9e0000
File size:	1441541 bytes
MD5 hash:	0C3BDC11FD6454BB67DA849864170B44
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: urdavsa.pif PID: 3588 Parent PID: 5956

General

Start time:	10:48:02
Start date:	14/08/2021
Path:	C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif' rpgc.htg
Imagebase:	0xa90000
File size:	662256 bytes
MD5 hash:	CDBB08D4234736C4A052DC3F181E66F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 34%, Metadefender, Browse • Detection: 46%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: wscript.exe PID: 2520 Parent PID: 3588

General

Start time:	10:48:28
Start date:	14/08/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\82139548\run.vbs'
Imagebase:	0x11b0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: urdavsa.pif PID: 5708 Parent PID: 2520

General

Start time:	10:48:32
Start date:	14/08/2021
Path:	C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif' rpgc.htg
Imagebase:	0xa90000
File size:	662256 bytes
MD5 hash:	CDBB08D4234736C4A052DC3F181E66F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: wscript.exe PID: 5564 Parent PID: 5708

General

Start time:	10:49:01
Start date:	14/08/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\82139548\run.vbs'
Imagebase:	0x11b0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: urdavsa.pif PID: 2232 Parent PID: 5564

General

Start time:	10:49:03
Start date:	14/08/2021
Path:	C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif' rpgc.htg
Imagebase:	0xa90000
File size:	662256 bytes
MD5 hash:	CDBB08D4234736C4A052DC3F181E66F2

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: wscript.exe PID: 1360 Parent PID: 2232

General

Start time:	10:49:30
Start date:	14/08/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\82139548\run.vbs'
Imagebase:	0x11b0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: urdavsa.pif PID: 5552 Parent PID: 1360

General

Start time:	10:49:32
Start date:	14/08/2021
Path:	C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\82139548\urdavsa.pif' rpgc.htg
Imagebase:	0xa90000
File size:	662256 bytes
MD5 hash:	CDBB08D4234736C4A052DC3F181E66F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000019.00000003.580526774.0000000004A10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000019.00000003.580526774.0000000004A10000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: RegSvcs.exe PID: 4684 Parent PID: 5552

General

Start time:	10:50:00
Start date:	14/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x5b0000
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: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 0000001C.00000002.584515573.0000000000982000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.584515573.0000000000982000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 0000001C.00000002.586361746.0000000003234000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.586361746.0000000003234000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000001C.00000002.589273699.0000000007D50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.589273699.0000000007D50000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.589273699.0000000007D50000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000003.582261171.0000000004A95000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000003.582261171.0000000004A95000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis