ID: 715068
Sample Name: INV_0893.exe
Cookbook: default.jbs
Time: 15:51:49
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

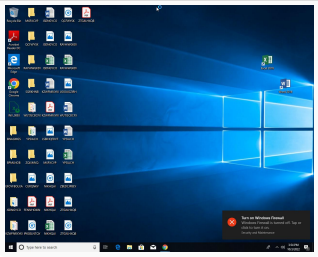
Windows Analysis Report

INV_0893.exe

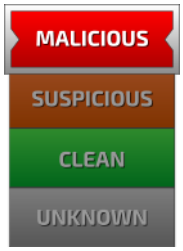
Overview

General Information

Sample Name:	INV_0893.exe
Analysis ID:	715068
MD5:	d23e1e317d6872.
SHA1:	76b58185f5aa82..
SHA256:	8dda840eccb534..
Tags:	exe JustClickAm-com
Infos:	



Detection

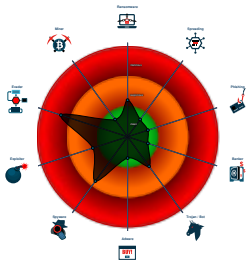


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected AntiVM autoit script
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Drops PE files with a suspicious file…
- Uses 32bit PE files
- Contains functionality to check if a d…
- Contains functionality to query local…
- May sleep (evasive loops) to hinder…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- INV_0893.exe (PID: 1348 cmdline: C:\Users\user\Desktop\INV_0893.exe MD5: D23E1E317D68720216699E1C9E524A78)
  - uvbdlqfvw.pif (PID: 2528 cmdline: "C:\Users\user\1_102\uvbdlqfvw.pif" faeupdrjbw.afr MD5: F28AA08788132E64DB4B8918EE2430B1)
    - wscript.exe (PID: 5360 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - uvbdlqfvw.pif (PID: 1244 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
        - wscript.exe (PID: 1076 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
          - uvbdlqfvw.pif (PID: 4648 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
            - wscript.exe (PID: 5848 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
              - uvbdlqfvw.pif (PID: 5884 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
                - wscript.exe (PID: 2472 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
                  - uvbdlqfvw.pif (PID: 5336 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
  - uvbdlqfvw.pif (PID: 5268 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" C:\Users\user\1_102\FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
    - wscript.exe (PID: 4392 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - uvbdlqfvw.pif (PID: 5328 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
        - wscript.exe (PID: 6060 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
          - uvbdlqfvw.pif (PID: 2148 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
  - uvbdlqfvw.pif (PID: 2180 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" C:\Users\user\1_102\FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
    - wscript.exe (PID: 6072 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - uvbdlqfvw.pif (PID: 1332 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
        - wscript.exe (PID: 4596 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
  - uvbdlqfvw.pif (PID: 5780 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" C:\Users\user\1_102\FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
    - wscript.exe (PID: 4324 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - uvbdlqfvw.pif (PID: 3648 cmdline: "C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR MD5: F28AA08788132E64DB4B8918EE2430B1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: uvbdlqfvw.pif PID: 2528	JoeSecurity_AntiVM_1	Yara detected AntiVM autoit script	Joe Security	
Process Memory Space: uvbdlqfvw.pif PID: 5336	JoeSecurity_AntiVM_1	Yara detected AntiVM autoit script	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Persistence and Installation Behavior

Drops PE files with a suspicious file extension

Malware Analysis System Evasion

Yara detected AntiVM autoit script

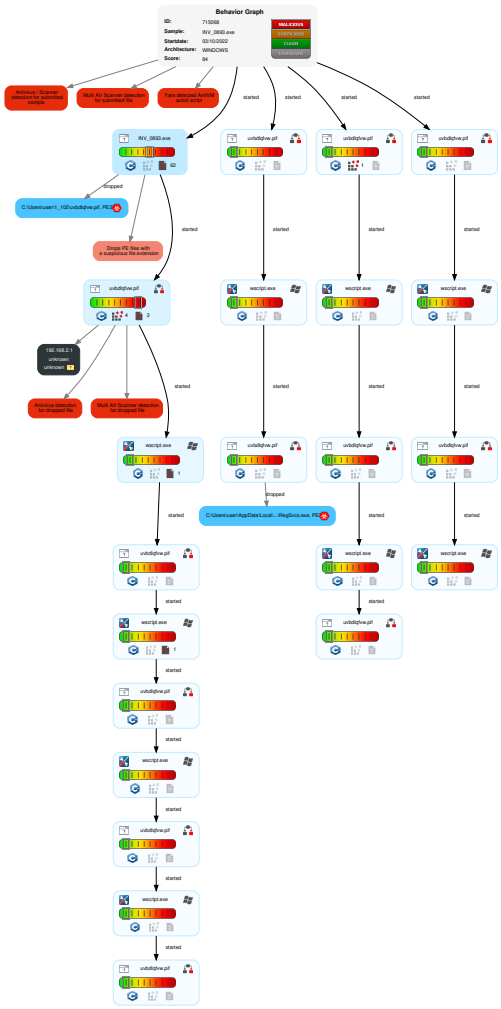
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	1 1 Scripting	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	2 1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	1 Native API	1 Valid Accounts	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 Valid Accounts	1 1 Scripting	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	2 Clipboard Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 Access Token Manipulation	2 Obfuscated Files or Information	NTDS	2 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 2 Process Injection	1 Software Packing	LSA Secrets	1 2 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Masquerading	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Valid Accounts	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 1 Access Token Manipulation	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 2 Process Injection	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

Behavior Graph

Hide Legend



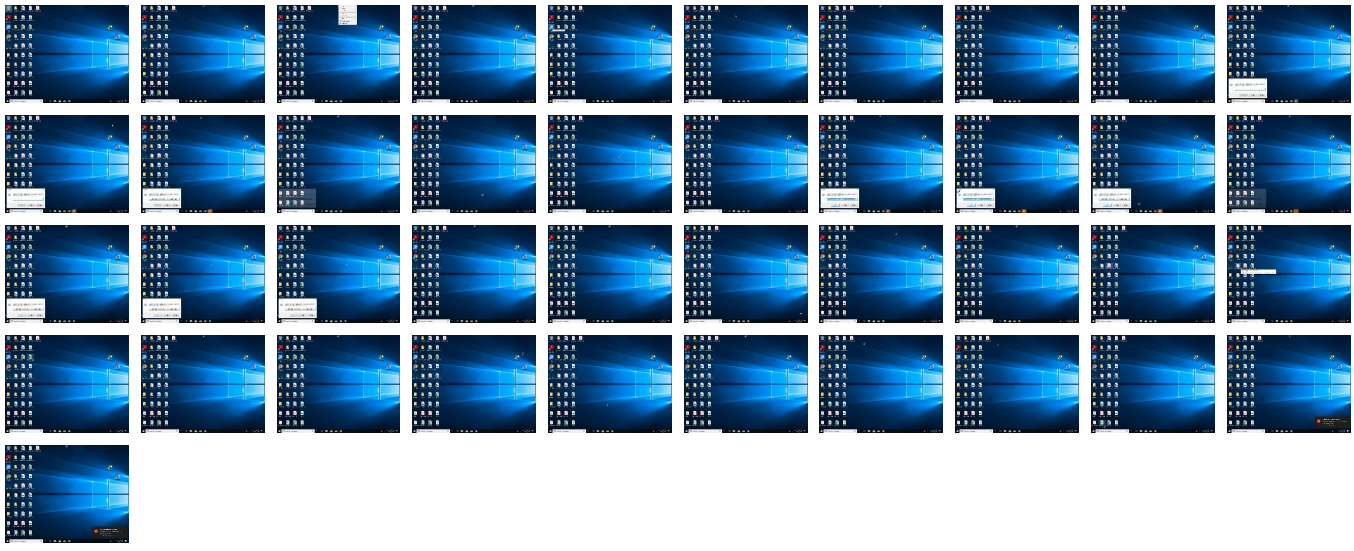
Legend:

- 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

Source	Detection	Scanner	Label	Link
INV_0893.exe	68%	ReversingLabs	Win32.Trojan.Worefflint	
INV_0893.exe	66%	Virustotal		Browse
INV_0893.exe	100%	Avira	TR/AD.Nekark.nyohb	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\1_102\uvbdlqfvw.pif	100%	Avira	TR/Redcap.qnaqq	
C:\Users\user\1_102\uvbdlqfvw.pif	84%	ReversingLabs	Win32.Trojan.Leonem	
C:\Users\user\1_102\uvbdlqfvw.pif	39%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	Metadefender		Browse

Unpacked PE Files

No Antivirus matches

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

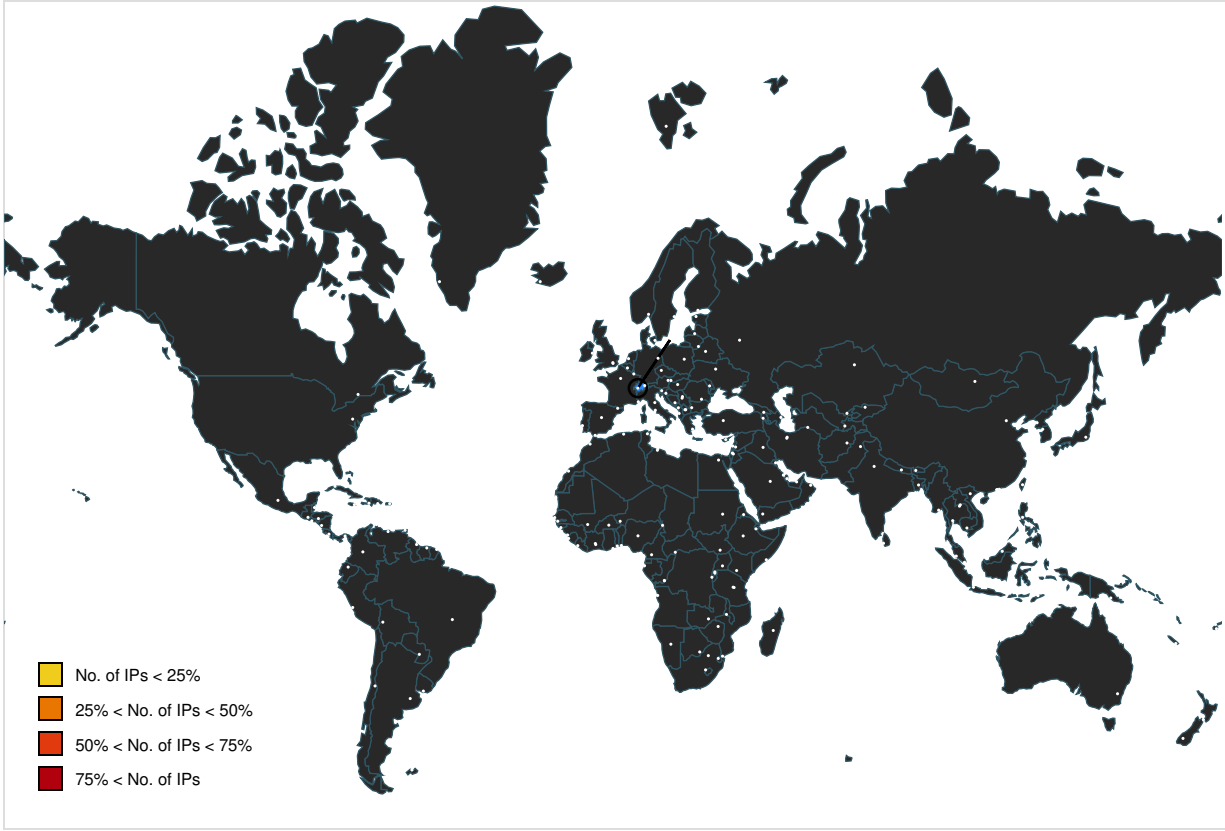
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://secure.globalsign.net/cacert/PrimObject.crt0	INV_0893.exe, 00000000.00000003.33611148 2.000000000499C000.00000004.00000800.000 20000.00000000.sdmp, uvbdlqfvw.pif.0.dr	false	• URL Reputation: safe	unknown
http://secure.globalsign.net/cacert/ObjectSign.crt09	INV_0893.exe, 00000000.00000003.33611148 2.000000000499C000.00000004.00000800.000 20000.00000000.sdmp, uvbdlqfvw.pif.0.dr	false	• URL Reputation: safe	unknown
http://www.globalsign.net/repository09	INV_0893.exe, 00000000.00000003.33611148 2.000000000499C000.00000004.00000800.000 20000.00000000.sdmp, uvbdlqfvw.pif.0.dr	false	• URL Reputation: safe	unknown
http://www.autoitscript.com/autoit3/0	INV_0893.exe, 00000000.00000003.33611148 2.000000000499C000.00000004.00000800.000 20000.00000000.sdmp, uvbdlqfvw.pif.0.dr	false		high
http://www.globalsign.net/repository/0	INV_0893.exe, 00000000.00000003.33611148 2.000000000499C000.00000004.00000800.000 20000.00000000.sdmp, uvbdlqfvw.pif.0.dr	false	• URL Reputation: safe	unknown
http://www.globalsign.net/repository/03	INV_0893.exe, 00000000.00000003.33611148 2.000000000499C000.00000004.00000800.000 20000.00000000.sdmp, uvbdlqfvw.pif.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715068
Start date and time:	2022-10-03 15:51:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV_0893.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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:	mal84.evad.winEXE@40/60@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 99.8% (good quality ratio 95.8%) • Quality average: 80.1% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.126.32.69, 40.126.32.75, 20.190.160.13, 20.190.160.12, 40.126.32.67, 40.126.32.73, 40.126.32.137, 20.190.160.21, 20.40.129.122, 20.82.228.9
- Excluded domains from analysis (whitelisted): rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, prda.aadg.msidentity.com, login.live.com, neus2c-displaycatalog.frontdoor.bigcatalog.commerce.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, iris-de-prod-azsc-frc.francecentral.cloudapp.azure.com, arc.msn.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:53:25	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run WindowsUpdate C:\Users\user\1_102\UVBDLQ~1.PIF C:\Users\user\1_102\FAEUPD~1.AFR
15:53:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run WindowsUpdate C:\Users\user\1_102\UVBDLQ~1.PIF C:\Users\user\1_102\FAEUPD~1.AFR
15:53:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run WindowsUpdate C:\Users\user\1_102\UVBDLQ~1.PIF C:\Users\user\1_102\FAEUPD~1.AFR

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\1_102\ajibht.bin

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.502922789746913
Encrypted:	false
SSDEEP:	12:TZVwp2gd7VaxgD0amKpQf+/eg1zQT52rgAP1CI7r2jtzwzXn9Qre/:TkpBaxgoaOmQTCtr7Cjtz4n9QA
MD5:	02539DFADEB3051CCAE79615BA474DF5
SHA1:	D23B4ADD8523D43EBC55A70309E53070B80D3C9C
SHA-256:	1055A69758449B4167A4F6F109B6A4D71B4C146F9C900C76ABA3F166A5F643C2
SHA-512:	2869400A31CF1FF7E2CFD4EDD5637088395F304BB21AC610D4891F91780906E1A3C2FFC91AFE3D9544C6973B783D3EC81746A8B46F6DA607316957ABDD4F933
Malicious:	false
Preview:	gk2o8kq0640KLfY09Mr87C34VU41U6oJ8491O24g8v910QG98D547015USA06j55D7008j4067HN3Zd8dttH8ar31v0v4L33c96C7129M474rE9484x4c95j8NG385Nk.. W9ztU4k699qAql63mLU5et4n634u0q8o1Y3Y26wc22nZ31..c3Ey54n6p638023p0Ymz11j8a8t81yGH6q9KHh9oP476w76P743P5IWIW34SS9067IHtjd8Ey99131tNO5 997Jx682bT0yB7tsHxv81881fB..L50T70tQL8W5X1HMv5081HuQ36T35cyW3Bd14uXVxg30C311778TamK77A97H3bRam1syr8Sl5Y..2LCdX91Lv0097..6ibG7v9l3O Fp6l93F..J6gc05eA0vbym5c6iVZ0c728wV7mg9eSc95o..82V8de1gQdS1m2U84447d4ta5j66Bn2Fh5k83W32d..TO934770G8fv117xxat54Y84oD7q59284452Khfp E00nMU2F0UE0Db4f2X2l9T3612KGyMD3gKF6o57YE7j69YXzPm6Q4435Xx375Rlz35T39dbz2671326s3RQ151OJ55..

C:\Users\user\1_102\ajjvnqq.mp3

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	546
Entropy (8bit):	5.480449121422421
Encrypted:	false
SSDEEP:	12:OM7QfKMeheVQTm7oL83fwFEd1XJE0b2dRv52JZq1EgFhTTRoqM4nge:bkfvehKk5L7FETXBSEfq1PHHM4ge
MD5:	DF4F286C01DF62AF4C04FCC0E25D04E3
SHA1:	5B8602420FD4CEA89FCF49E585A1A9574181D2B8
SHA-256:	364E95C29108F312DDCAF91D8835CC9D86796C44AE398C31A34C6E70DFB902C2
SHA-512:	9E83819342DF37694575373066FF5EAD5B31CB0C0822C807D19309854BFF9E24367845C6F260EB38C87C7E54F88CF97FD1DF2CBDCA5EFDBCAB633CFF7FF8BE 5
Malicious:	false
Preview:	Q9F3628Iq7Erta5506d69F26mbQO6604l69Mv96Z80OD41X7TM86a82NbV5h9Q26Uy5clINTQgC31Yf091mNzcnO410536fuH847..30N20dts2ob53fh58Vlj5WTji4A7 b179E05oiB3G4483o6P01113lE007827b..P545Q5737ZM8K5891n6DxQ539Zb6R7I47fQxv8FXa5H830b888F6038Sl9RZ7K2LDQHI6m38M0D3hs9ACY8R1 mS533gR8CHP6658316IgOrDQE73cnMgi2DYoI362MXP0249LaLB748FRQp2GhK055nctDA61GQsO04uLhW3..54MV3OUk7XSAOV8fAc8M11nZ71423h993z2 CSqUk4ez2GO3z6Bo3..1mc2q5GCE1e6X1E0Qar74Kwcr584640C5PSU90E7ePN23Kg13387123Su63lE29E330B98l6922uc603387K0xi6bht..G0vH76w3535VX053u4 3T9xS06S8W35R7rW1Hcrr78lvHXO9h7ZLG481X3T8904..

C:\Users\user\1_102\amelelq.xls

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	542
Entropy (8bit):	5.559086402409345
Encrypted:	false
SSDEEP:	12:c83YCpnbO36NustrLVnrInw9kNoIka4Nc9SNSjXx2wc7RqIFsfv:c83YpiuEhMwmQcLjA97R7sfv
MD5:	E20A67DED600A204E27EF18A4BC16C35
SHA1:	D6EB4879297894F160EFB1988FAD032B8B269B39
SHA-256:	C16BBB631264A94077E33D0FC59DA6A493D1F3DA336329C0FA193B58C838E38A
SHA-512:	C409DB31BAF2E333B95D1D8629A997D199D084AD3DEB01DD5160F60ED64D0E35975462BC146F11A473C04C9D804C9E327311C6765A536B8A5B1B143A03DAD0 B
Malicious:	false
Preview:	J4wl386j1aYAj30RYKeB6IKO83r3E1Cu88BV579N1K13400O58559924h9u4G4Jn6zF9WE10..RCsLt48f..9466LDww311FgmxnqJ6JU2OKn6a3rz2Vo6399ab..4X4IA 713eX3V4m4R5I8jQ58c4i4D2e8TNlmu230831BoQ2rlL04RF959379kl41TSx47UdZ03SkmHhZIG101606TKHcEm9D06X989yU7QE4H13283Hv6amrNEc44Tz9o1a6xUFh oWu1g97UVMSu7..y7O4AV262j9O9K77KgT1tJf8IN57q43hN38p088g155lP67A8wP1KxV91g958FCKrJ30sm4J5LXQ76aw9cC457BB3aFvA7h6j213d6m9d4EsY76qV59 wNMM8rHHt4536v..gN0914Ur9jH95w0GR517rvRuvdOmoO4X23Ms844218ozrmSN94255AShjPdp6M018T0394irB1x4D8JFg0C6U7jj265Q0AqJ1u4M15G25B997d0H6R 5c19fuW41fT60TD179nF..

C:\Users\user\1_102\anuhmos.txt

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.538318374250493
Encrypted:	false
SSDEEP:	12:J3JW3xr1R3J/OF0e1VwUcL5WMBNUPS2u58M8hSGiQ3dM52m:JGXVOJ1VhcdWWSju5BP03ds2m
MD5:	7A5A37B1EA05049E306EBB0F426FE5F7
SHA1:	FE60539FD8AAEC467685E7A4756E9EE83577CCE5
SHA-256:	325E5D396689DEA2C9F2BA8EC049403B1A5E2189783F20FEBBBD1165A8335CFC
SHA-512:	9C9D705E6FAA7D6849A75314F4BCD81B643CE4B2495A056BCDA8847DE70EF20804EA79D01B9D44EA6C63F33BB0DCD0BC8D1FE80621722F9CE8AF0ECD4FBF9 5FD
Malicious:	false
Preview:	172b30iKv1X0D0m8E3U83O33x49UqX71l922ZRx32h2w33py1w8622njs96b9A2mN3FSP9kqcm1162Q1tt0jZB05Wkk5s17WLbF7tFvv0uR268c7603j6fv8j8LkQ397EH 6gJ8dbcy..k3y1uc9227e86FD4qBF34C5nN9l602612196IK1899gHtkiVx3LjoAhh16TTAabitg504vjSR6y128P9E36vS8j4107sz7nlk389z6oYxg1904469i1eA1X1 TaUzwrMuv1VsM88U7A63..1943b5V8Q9vy2434Jp1DlOa8h87K78N63957Wux993ViNm0J93z2M70281gO3WK6tTR4IQ05n8Yy2S82321v31D3sf0l12699B8Z2uT8B0Zd 813ofy5gPO946Y4haDZXV9Y0185TCB68aFa0VV3q4racCiE3d9O1rPNz5jfNev0kz3N48VAgN3u2..34289GQN349MngN88Q0RK25r63V4EOuFYY2RA..

C:\Users\user\1_102\aoejxqi.docx

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	502
Entropy (8bit):	5.502422490466258
Encrypted:	false
SSDEEP:	12:r4x10qssK3yPWIXObNHIEewOSPTeqSyyMgn:ru10jW0bu/wQMg
MD5:	4BAABC8BEC0E679A2B308121CFF84B27
SHA1:	318992FAA1404CE761CCBCE068BBCEAD473068D6
SHA-256:	720B60E05186580911EF7FA304C0408601F28539B51499CB1D94FEDC7AFC8500
SHA-512:	FE2AD1B47F83C02D2188CEA7F14C62E9E648490D6AA2C4787F9A7CC5579EA612DB41970DAD59D91E5F4FF8744843175F70ACA570529B4222F6AD804F29318E2
Malicious:	false
Preview:	9mAbWN7AI75z562t66c8ascd8O4n93xVfckvY9T33lWuQ8PJ6H506gY0PtRKP9y9m728Xoc0W675769lRTL57b68Ih797X4V359F1J3Qf84S8G13XhG599G5NU36I0W3vB e01lYRf3l678..a9199BBD04G52Mw237pYp51FOk7n57xRK369HPz00ou0T360d2pg85b2H8Zm1LP5568159mUK6l26m53O80z89w1hl6t1hlOhDXbRA3nNX4T8fElo69d cK5USGj0od..c9J8e47R2lZ4Xu6vs21908OUc8gd5TLro7Q56px7R8C2m203ecPG5uk6405z8pns0lQ2d704745v076o222..7wysY7sY9tF14M0jehP886S92113864Zk 70l5Xsm78B493zb20265936frs9tE399Uz14qw74sF88KlPL77E88jq8605JAW38TgeeJfQDJ601n410WGsnKE6u8X26a8exp958l6455FFT0t..

C:\Users\user\1_102\axniud.jpg

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	517
Entropy (8bit):	5.531074123964247
Encrypted:	false
SSDEEP:	12:NwlPuUaZP0YZXoBwWWMAQC6Cik+ZwQ+3Mb:N4un50YdoyWWMnC6Cikt1E
MD5:	7B7F642ACECCF300072B55D278C47746
SHA1:	B0D921DFB53E1420F75E1AFBABF5F46150E95380
SHA-256:	474B3E56EE960F33B2A61CC790E15DFCF55632678C448118B28F418F8D6BB8A6
SHA-512:	2677C67B581D1B6B10AC76B50B72AACB9748830E6A55A68FD04D31555C98FE36262565CC04BD31382A5BF94DB5615C8511795520C49B175C5511489BF6A0766E
Malicious:	false
Preview:	ZSUP2g9zvUJzpF873H425U7t5WB7vz0u5sJuESdqYm1Y05b8fLTh1S1601l360l01Nsjqu9S8Q1jN5UO1922261w12z8p0Q3x39UcG6D7mid1rW46GTCiHgA70911FYfy1 Mu7fZ0sV..l550n9M61n1769p7BlJ2uA1jg9212493yIE3R0w8sg62z41W8dV5xe7aE04y525159CK027sDf8..3y9y..C429o99U6Z4Ab7u5DQ6tj0t37HG6f79B4p5Lb 9RwJ90H27ACr0N6P82Ah578Cy50RP2z88O6Qq80vEaN4a10048Sb57E5i4wpk75h581469..2CW03c424uJS..5479Kc6C2ro1K57ED254D6534VM49NC96XfYVv37M7nJ 73661SXl9iB9DcOrrz03eGyfnC5A7w31E08H9..5gi6342P6r7DVaM0w3T8242PrYEAx0v5413782luFK1Vs68U91B1Atj13yqw2BlC2f9a204979o42w9kxEF7Mb..

C:\Users\user\1_102\bjnov.bmp

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.461006629355738
Encrypted:	false
SSDEEP:	12:qvm8DEVc33cWpPipvBqUm83UH4MPWqg0jWWnEwsBFF/AeWZxEb:qOD2bpc4U3AsqEwszWzEb
MD5:	FD026243F93E4152C54CD5520B14596A
SHA1:	D0E8BBA3874236618B93BF1AFD625BDF403ADCD6

SHA-256:	459F2E9990F78A4D512E6F40679DBEBC32F89602D16C7A146113A00086EB3C2E
SHA-512:	A9B295F11BD7AE6949906E7E3E165535FDDE42B30A53C3DF4418C376FC470C588F5E167961C656857D445DFFDF0605BD2161E42B9D95779434C1DDB1CDB9CD0
Malicious:	false
Preview:	0ix2D922817vv01CFI418j90UkIBNkLd6Z380h53g80b6D730J194N00oT870S5L3K0hmjk80z297l2Y3Vb31JXl7fT9v34744q0Y3O4ft9485i27..PPGDd3Di0Q4U476 l8ewG38c3324ssc18774HT92u7469q4795cnkoC34548f6f4q432F75WE6808J05I76..E1D60g3U1B283Z5u3Ee5813N8RidtK82124ll554qS9MxXv3083Pqa450s2S1 v2A0iFpQ02jAmW94VBX425lJS192Hw7309MZl430Ao2BtZ98KvLl9V5rD68KxE785i3vi2l4mB6I51690604e9cr012290xF3P9384g7Ni632z8Q9r455Brr71YB5LH09N 6p30D..gF774P30127dbqycWM03lio0Xa7eZcu6Ql3k039B3kh3ORg0Rnua0ZNR7W31HK49id89J0t9Jbd75i1D3de9..32e5Q3r4eh..m0bSK1Ev139n0z5XeA2F6L59V HHe572A32467tmT0582FS2fG3l10g24sC2C5rZQi4Nc1j9ahe3AmHGn7J3998gq3Xxw63N5IjN61909ah60A89ILmaG..

C:\Users\user\1_102\ccqmrdcse.exe

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	552
Entropy (8bit):	5.465694310675173
Encrypted:	false
SSDEEP:	12:0XxEdlcFMg3A0lzOkU98Wtc7/uN5lNvf4OjkiHJUEa/4PTWrF0LqStW9G:Q1c73FbkUtW27H7AMTQ2Lp/
MD5:	2471AD1D47F78C4B5637DED83B703AB2
SHA1:	F5D510788519971288A53978B55C42BC56DC327F
SHA-256:	6C987CA44B52B93FE75A03D33ABFAF5467611BE1E5407EC0CCB3C34D155CD69B
SHA-512:	148540423B893908CBA110B163A58F8ED9B01D8809086C8368BF74E96A5CD72512E81E317A2437924C5A3FC7D414A34C0A8B71AF18A235E2DEEC38B5C9638244
Malicious:	false
Preview:	G917cK4ZM6Oi228k3Q0xk105x772zXV8..G1I5mR..8B462P6vU0HabsG60edwD5F1w63I92vdc1jeJ8Tb..T424kU398p2Qp4T3113Be6wAz8A98ya6r040..d8409z8M P4KWp5xu689y0P7dE894K71A8Z5S1kTJ480ZT76B54Wzs323FsWn7w640v72U08iveE6355Q1Z19BY1OT3987ovJ8C757Eh5gdtU9JE1JG787s9c424SVn725d2i9lm9R6 o3KeK8GR5gq4X2O5yRT74qO079z8Au5pZkh7G5X3..2j4136z7710p64gO17E1u54MT3M9126366949eYD831h01z1TdM4095BEEVdeWG575KF14e334QorB 5b5NJ6L5t2w839..1k19Ls49y97rW39O5C18K..wia2oZF44j6v40T6j4804oCJ7v945320223Da7rAP6VPCc0mT8330As3V8h40gM07I73EY160324Xc8ScT2H3I688JV B5F7s5cU8si28ojlUQ36u64Tl4U1a0R3228FY8H3..

C:\Users\user\1_102\cqlbvl.jpg

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	610
Entropy (8bit):	5.561295700260987
Encrypted:	false
SSDEEP:	12:ObSEJcRWqB+CWxzEwoTrcUms1P81V/ORqxhdU860wbcX:OzJg4xEPTrzi1ROg6bcX
MD5:	E4858AC750880DE003CF18825C5721E3
SHA1:	8A767BDB2C12FA67099508996AAA491A15D0B6C0
SHA-256:	66273F2079650B7558F4E3719829378B2B57BF915E492928DC16E7F08D6C15E3
SHA-512:	30FFFC42B61F6884B57EBBCEDBCE83631F448214E5E204BDEFFFFC78760B38E9A34455D2BF96E917C454C358E522D197A8393D6EEED80606C487BD7372885D10
Malicious:	false
Preview:	3GL9C9CU97AMp01re0895jv31727hK1474Xcfx4fw0z4o0L1hzcT7185..HSexrQl14jvi96e29n94016OYT9..743259IP1DN515PQ53Mr3P2y7O0UhUX..xZg43kvU55 60p7zZv11A1h8937o2U2489m69Nq659XTD92f2XM686113h41UNKW17QqprQd9..pN5vjvL3zy4wbU1g4t9a2FHeR89OQC8189n4MZrotv1hYvE6gL4Yt6jwW43l9rLU21 TvEwW2oGff8S1KmC6..w73f576w5wR90h2iSLfg8A26J5bA1480MgVWOcp4P78rxSI2zF29N8wY65Y964ZU4oLvmml24a94CM8r5QuiwG0o..7lMg185pQ9J8c0nJiw32k v7B27slJ1x5X55O0MvM5..5TgCQFbtT22H8B535R4A5pm3X94vQBu4B7c9jWY72260ajd9P80D8tpS15yLxz1866Y7V..l9Y023C242K7C4a6Nynv1kp08Y6D57H62Ix9d CLa2xp100mrA4Z480C1E804255sY1210e14541r1v6301lgQ4C7pJU1MrKBnPu9432z1n6lr87iD247Gi7z138Xg..

C:\Users\user\1_102\dcbewlcfwo.cpl

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	503
Entropy (8bit):	5.444157356340834
Encrypted:	false
SSDEEP:	12:kK4TdMkOb1rl4wsfByP5HVdJj2E1EIDVUDveUyWT9fv:kKkMkObcxS3d2uwDV9WJv
MD5:	7C4CC21B68DAD67209FAF6503CAF9152
SHA1:	153390D387805338C04BFD5EF6E9808213762197
SHA-256:	FBF55A460DFAA43926174E2CCB66C4AFE1E7044A324000F0522E5306741282B3
SHA-512:	EB719D67D2B320D566380F459EFD17A10DEBEA63713B8EABE344F97D488142986390E156804D46E55F50A1831C10C809EE38770EA51969E449B2CD38C23DEA1
Malicious:	false

Preview:	908s67f712fZL1CFm3407QBZ28t7q0Yov712yBRdj6432L90M55g8t9p3vTU6G6T4v05tDC5it5oaVi4Sn9sCqlp3Nc9538b091422ilTuG3AV0El07595i5A9Ew21Is91 u90..52c3QG68Fe636Kskc7iuH3Il216Z1412Z19RW4rorJ797Vb9gd69aTLn1E65v95tnxF57V9ZzVNHrXH26646695783bfRQ5d1x2p5Yu9f0..Z459c5kM7x697CaP1 65..5DIaf3D3lQHj4602o76zb81K413r1l9556Lly1k4si88526we5w3113U005FMj1m9C224lk41739qY20967Z31mnG42w44vJGD9vBH582t125a14Gsr1..ZL8V9j63 HE8127nF4CUN7re92g6r34L472D505972oxfj8S3tNk8NtoK71A9246Dly55k0bjcJ2021v0617Uw36..OVCh36l00557zx59xJ1..D9sxl7E7p..

C:\Users\user\1_102\djofgadl.xls

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	521
Entropy (8bit):	5.413071314397834
Encrypted:	false
SSDEEP:	12:LYPYJJVS7foKK2ZUZka+9F6DjvIzk6nTqBGzj/yMcSK:LYPiYCqfI11eBY97K
MD5:	3C30E492F470C93CF12BBE7641E9FC69
SHA1:	6F71F33CAE025F41EF020659650F2D73A1FE6A85
SHA-256:	3F9F4A67C9EAEA41556110C790B580648B1A5AC5ED476F1080E1DF1876A2B3AF
SHA-512:	45AA60C878D1FFEBA2C6A944621CE101D9782E1FD29E196D23E917DAB539107763EA4D583C50AC846D7FE7A15D85285A7DC8C006BB99666F47C93454AC4A96 7
Malicious:	false
Preview:	4k60o59813E3GuWl5V243kZ05P2I5gnVfrlGP56513U17cV192p05F26K9eqQb5319xM13564OsO8qk6316P87V05CL6b3J14cM342Pq0QjLO9JgQ5W89AG4LB12naX2k9 pkFX5C964XE32vV8Yl4q7sJkc21rrl691T7d1D7H15ni7O06Ek8u79boe38I2qM8MFh0..9702w6277Ol1E8O04pA4934T92U1k93042417XqfjzSz31iLH1a73r46TEXk V89eD99554N5Aq45O0h88581vm3N5KB01209290Rs14hgX592pzR175E232fuw9K77LmvK0gjJZoSfU3P3774u3Ek99u2478mSD1896W5M6yDnz4WJR0c33r0775Vcs..9 14H82f0B5X95N5ndA9sqo1BoM1200g8326a0084YF4On59kyl13v136OsH62Rg0318k4l164R05iL40Od411cVYrqF0hd2QA9lcM78314362CK64K86DO2y07T33f4K7z..

C:\Users\user\1_102\dnnkbxvv.xml

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	531
Entropy (8bit):	5.456363943562378
Encrypted:	false
SSDEEP:	12:YvdWcr20OHLLPGJ/XxFNL6A1rZcWXlndU8Jjm1:YvdWcJiDe/XxF4A1FdVdvk
MD5:	ACCEFAA385E9A4C129D3D3B1875923A8
SHA1:	33E3CBC286967F500ABD1B6888AC5BCC99EFA183
SHA-256:	CD6459610AC3BE59E9399D9DA63D156503CA1C862B6E80C9ED481E70A6F010B5
SHA-512:	A3C04A5C0511B7EE4454FB110C469BF82934BEE572248382C4C9B75BD86C1F05C319E9EB46213BA6DD66AF72E696C14B236FDFF894611AB07FDEFCF9D24CD6 A
Malicious:	false
Preview:	T292WA3X1W4BmPXToc9P247N28gBfpL057GJ6L6d0973tJspv1ZG13L4506AZam12Y37v90Y86d0Tzv7440L536950NJ4bLn6nsi5561h21m9BiJ6575p51774829..YO8 5N60180S75ds388f570l339139V4WVWJ2BQt7L46JA81P4eM5c5Lj3vk0BL5u4d05RD67TF21Ze7hZx8uM7P52wnE..o7cPf1sw7SEV54Q1Y8x60a4Yhl2L4V6De1RGbTX 21Uw621LOa995A5b524y243RoT0m1c5..o87s27956F7NOCwWk4Hzrhh11521J2J9kDp068M5O01z63698997z2n7Gi9PU2c1ND3Lk795d..vS42886c70lK4ha0744l3. .888mo32aSGo3P92n98V571Mivr43jP326337853Dv69e43G19U6y6pvtgX1U66oCN469vHy6vu298Z77R7Lo4qmogf7UR91mBenu8bKM4v8Fn5o6N4pcKwZe84893949F 0k6ThU9i4..

C:\Users\user\1_102\duhuvcet.mp3

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	582
Entropy (8bit):	5.5299496587239005
Encrypted:	false
SSDEEP:	12:ETkTiVpyT3f8vYoToYd1+z9CsV7wveR4bMeA3eRTlzJNfSwsSum:gQTPQT7hsKWR4bMeAORNQLm
MD5:	E9533480FC3385A0EE3E7956B2E784FC
SHA1:	32BEE8BBABCB0FE7A3B59FEAB3FB23B7BDCE2AB0
SHA-256:	72AEE43C7B2A8E5FBE2616BB9352F86350D394637C97A8F99D1ACEF8D6BBFB85
SHA-512:	6377C12C7A06236FE4FC65E707E45BBF2364F5358BF8D19E5A61061FC9AE570291FC5FF7B1A0A7ACE49BF7FB0CD36B792CD628C25777EBBF60E7E853843FE79 B
Malicious:	false
Preview:	W29q24Fq9D52i9ot95X7uB63918yo4yp895J7pjV5z260QCeni3U25z443lXOE3G9vgge1K4C79oE9676pNa75SO4k14N9M..O1813251Y6558Oi2O52Q72l00zrjS21v6 4u8GmAB85XO4AB5ew3546eZU0xh82x1575..e8h39K923Vwn8tJu3z7ZK0D91243QK6910JDNps1xu6B8qV1i9X5pR83Ni2z68756zOx9440QI054FH8L26E mew1M0vmC6..zo4o7T6143Y335O98c4b96373Vm88Y2wj8s9Ba9B5LD4D7S3L354lCr8u5R4ZC45BY9cBq621tEO23WKX00J33BB6065465w4agpG319580fx3UwqXiZuU K5X29a198Mc38..p5KnK8879lnRa1ehL931Wj1A9FmM1J0rs76982176W7L6aclQE7U7jl6kU9..67kVbvabHJt73189n90FCHA3zl7YJgy2yV7TSTIAB662o9zV5lwfg5 53Ql33DH46k18xS94Q4e79HVAE0Bd220807SG7rMi09p336PK67o7APNKfrt71zBcAh5Q6..

C:\Users\user\1_102\ekqfgt.jpg

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	505
Entropy (8bit):	5.455938783150867
Encrypted:	false
SSDEEP:	12:YVlgIH/hqbeU3/iVa0GRPgjFOH9Sh5Z8n3Onuja0kJvwRE2b9vSnKoyn:bg/h9U08sF0+5C+nJ0rE2xvSnKoy
MD5:	189839DC90D5E63721BD54B9E3F6D42C
SHA1:	2F99961CFC270D43913C301536E797AA4F3C340F
SHA-256:	12441E1570307C465EB74F4F2630386F5EBA2188C3F287955DBEC2EFB99DF63B
SHA-512:	8F8951FC3B826B0F2AD967DE564506D31C005A3A6AB88482E4A0994DD37D40A2F5E20E76CA4CFA726A32FEE5CBA8777C105A1ADFCA4CCE90B52DD9543F715E 5C
Malicious:	false
Preview:	412y2N583DZ2536uqo80155J87bMGdOh9Rdz23z45M6b84Pd4M0u74p669q130A1S146f197O1hP0fPf58N0qf1k5BS310bF216C86..1YD5fDD11Bl12h9Wap23857N0Z 09Q5h921..1qq6Ex8ZAe9I0R83ax7y6o3m4ZQ928MVZn7Y0x8Y05M27372EifjLb6hpl33E69s7FNoQ70o6tpa25..57ZcQ30EY06FhH7X9500YdE2Fb7w7a1..H91gX13 W5jB8..94o2137d677D6SkzN19HS6xy2In15Bj683ySsc8Y931yhkW97OXD59si4591453JT069b87tIu634iUv8QoCiG1..52F95476i5heoBK8cZ87t3q330Gw..1dkc 068ci1J7JQi0xg8..i70U7833014ngOk29d29W93K5661uymT0A..1xDPpdIlZ8i591cDw2Z7998t3aeT6F3x273WB0429Duh9eQQ4482oHI9L0hl..

C:\Users\user\1_102\eqedro.ppt

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	505
Entropy (8bit):	5.521259353437891
Encrypted:	false
SSDEEP:	12:0SdhdYYgt4V6BS3yhMpOZtYgTHV6lX5jhgQLmJ5yy:xlg4KhHtgbJCJp
MD5:	73F367733DDA95390061C717E879F97E
SHA1:	395682B54D6AC4E6C650D9E8654836D2FE3CDF60
SHA-256:	E7482D8536E7CB687BA88B8A96CC4038B011C4F09948A7FEA049FCFFCEA963EA
SHA-512:	F472C1A70DC4ABAB50C8B188A9E1A6189B4D47607DFB039EA63515970A36975CE42CA6936B109CD71C4436FE4B52D3F83C9B73B7979F24B0BD077FDC2CFDC9 C7
Malicious:	false
Preview:	6bwzc7MS10h322Yp1CY894D9M468YT2U9yKqdW..6k7S401JLn4VS4k9k0U96S60Vm956B9083q6vh1L09b3q..1v46W9QiW9L465679G2615X3uu7189847lo0T2P917f VJ142362t806G951m27EChLXa9l6m7A0u8n8d..Z17HU9q3cq97ni6XN1ECZD0pDM2l4m3Y9P5e82uoiRE8cx1423m5bE72U0jxh476038O9165o8i23Dg8vVoy5by0sO8 Lqu56444a6T..3LH7dRX60A8z719j4G71ng90a84z17W40T785FE38A1g4z1AGrDm4B9Go75i0k5u9zgPzdmE54v37uQ4x0gtbU1m4imx7..H5QF41il6JET7W2w16QRzE 52UpL8xQJ9fwsmq597CNV9O6ief1EK9DGWQ01px282VQL0O93eXEp334bRD90HW5OF88o4377mPgl12zK8lK5C863n855w2Wn3HX558jl72U42iLD..

C:\Users\user\1_102\faeupdrjbw.afr

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	179159046
Entropy (8bit):	7.043177293100947
Encrypted:	false
SSDEEP:	196608:yTH/UGgbLwzLZQQ+s4n+aZlUSdBOLijwxDn/8OMzXzenW01t2FARSFcZd2i3uKkf:b
MD5:	EFFBA2D361BF03ECA0D7B874614A995A
SHA1:	DF02FAFBC0864975B8E55CD7FF3EC75BCFBE5212
SHA-256:	CA4EEFBEE52DFB136B739ED8C49265C620E61956ACF85FD6E4735D0347700C01
SHA-512:	B2E35BB21DF6B1362F051AE24F1E8F534E77CA8CCF6CFAA17C54A4137E1547031C3273A117B127B465C04596F8D5EDD47C36BD5532C19F0534DF41EF0FB0010
Malicious:	false
Preview:	..;.Y.....@K..1.X..X....>..Y....MT@.^.a.=D..S[..(."v.>.R...l.T[.q...M.0N.d}...R6...H6.<~D.....<....`#..l.i.w;.9.....OV...T..tV....|u... $.~.....G....!...fw..h.w.\"o8..]......l..D.....# .c.s..fM=.....p..W.g..e.Dk.).!O.....j-...u.s;J.9...H.:....E..AQ.y5.Sa..d...3f.e..WCX.>.D.$=iKX..9...D..L....m.L.K4BF..[...)..D.X.!.L...G..3..{..h....s.L.Y.....h...0.W.....K.....7.9 .j.A.3.w.y.....v9.]U.s.l...C....T./)..6k...F.Dp.=....2.....xX....r.4.0|..@6. .....X.d..s.J..f."....Rc....P...lbR..... ....1.8.7.1.l.4.U.5.1.5.3.S.J...../N.....`....S.....b.%..oT`..lK.....c..... .ce....i.9.5.p.u.w.....A.g.A.m.w.A.7.0.0.0.a.R.6.E.y.q.g.o.A.7.B.T.I.8.p.F.....i.C.0.1.v.x.1.e.g.G.h.1.v.0.9.9.v.8.l.1.K.0.1.x.w.5.K.4.....E.5.6.4.3.1.5.z.9.2.W.L.J.8.2.0.0.P.G.8.0 .....G.3.w.2.h.p.3.Z.....7.6.E.8.5.0.7.o.1.1.L.9.i.9.V.9.I.S.2.j.M.k.9.R.0.1.b.1.8.....?..~."z..1...>7..S....h....MSJV..JZ..d.....M.. 6.t....x....2.a.6.2.4.0.R.t.j.2.O.e.9.L.r.r.N.7.I.9 .2.7.p.5.6.6.p.3...

C:\Users\user\1_102\fcndwufx.exe

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	621
Entropy (8bit):	5.49707199150231
Encrypted:	false
SSDEEP:	
MD5:	B59C5FC427AC149CFA601824C46183D2
SHA1:	8E49397ACE23E77970BD69EFB1C01C398F3D64B3
SHA-256:	5C11D7C6D70D1E656F7448BE82E2920E7674AC193578E4CD9AFFDAF2EB2E6EE2
SHA-512:	572F804EC6FC625EEF8972CA35C14B1C005A80AB6A09B0CECAAB50395CA8EB13F593572ECC2DE35823C3C9539EF4BD0C13ABC0DED8F4A20949E5013A7654E466
Malicious:	false
Preview:	8C3xD4092BU33un943lx0035xL247Ozq7a3qLbPp9tT9w362l33G3141ActLa68Q75a80HG2HFEE5H036C4892w8H6i8s528C2Mw9n8z669RyPg3x73Y21885o4d7..T57aBC4n8621641906Sve63cr1044C36MX19A9872370ThA399802AT606JqwTy03HF59V8k4By3..hUw4v5c75a9M7TDFny07nl2m8z49p33K8D4E2M18568081h3564599DYmdQtu2wR5945z7eD2W8ool28RD1hW08Q2HaM300139CeHkr3y4Q0l54L6Y2D8il8Jn87RF670ngQlt48a3520..04X6Rkdl7hjVLx40..ToKiE7MCr434u5430DGTpnNTT25uQ2043jC17X574C..ltF99O2385lJFop5Pnr8S47PtkrwB7O0yn5W0lT12r460w1Kv2QGz0vUu2iFTdf6Xe06deEaKmf334V59k1U29R..1Okb46lEkF632u725111h5pcl0102rR60r8nT7K78W7zeP3pd2053HmJZwR59S0bv4G91X45W21K85bjYL4TPusbOn8FUh759pAO6LVo38fUC42374M60cP1..

C:\Users\user\1_102\fmdem.docx

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	Clarion Developer (v2 and above) memo data
Category:	dropped
Size (bytes):	645
Entropy (8bit):	5.471968385843521
Encrypted:	false
SSDEEP:	
MD5:	15FD81E2379FEB3AEF0B57330D8956A4
SHA1:	9DCE9EC6588F6D404A1F7D0067519A3291B24D53
SHA-256:	51DBEAC88145CBD4851D83F4AD35EE66728D1D8D4D9860DAF3993EE30B724913
SHA-512:	8C05B486192D73B40B656877973C4DEEE60582740F9ACB63A79014568EFE256B1F42FCF7B8E8EFAECA0740FBA8DC2945C97DAF7BB24F85B4D8828A3FB7F2DC82
Malicious:	false
Preview:	M3K3bt4H7252l4933127q6UQ..3z56nmi0t4m4O37Q9Kh6NRJ3Fy943YshJ19475R807PK8lpL5C3gS035dWH60xW45R757Vg03va71bmC4V0Ou6Ov96Tl3m955NhS234743m711D69slc0M2tULqU8..i12G13B6AA9hs29NVu4q15rn68w1e27J6f4682x8L1ga07Z8xGHI224x91y64979RZD4x42649W1x77R36331U4Aj4A8sW33Z1G0tEZ5C1u12lt143E23wQ9N26d1f30C2fk8DTBrNy2X59D7CRZx1v22P9Ji696l32V5X9m00X47WvZez7855..BMzK6939g4s15CT0g245j0d1gN82Aj3HMEk6S0XUa5QQQgApWwH450DBU5o8XAn38BB31s60037h6C1..9448248e2XmFLCzr0S72wY799qwIqSQ07kLZy1rE5OFV8Rb40B..H8Es394nM59vSoP0b4j6hf7k494473Af8h00a15ie804257m02U7xm5H92053qu77b1d7b9z2P1xu850CAxwA7u60758Nj05A93Zy14f08EW18sf2t336fmp68X1YFk30oB4748kx92D1mte4i6734Fy91hT554160NsN4980OY4y..

C:\Users\user\1_102\gbxurtvclr.msc

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	570
Entropy (8bit):	5.523011187954899
Encrypted:	false
SSDEEP:	
MD5:	F9812BC1DE6DBD1FF19D08FDA1B969E0
SHA1:	4FBAA7DC09C949376A4AD76D28F34C1D8BE7A05A
SHA-256:	6FF8FDFBE2CD2ECC3F9E0AFDDBDEF8C6673012A84B65BB6A73744398D4AF954C
SHA-512:	EAF1A4FB1EB4EF965F120C2F97994EC13C777FF9A0E746D9D386F4EBC4970A1070C21C88730A6EDA4D5145941699538E68BEAFDC2FC54C3E6C64224BED1D59A
Malicious:	false
Preview:	f7l52mp6Cp3l3U9363qiS099YWk3Qaz40J9m6x74SM4l66ZMKR588Chqm2212314H6J310G0y1xtd84aY4727v1PEs4X6TsRo65kF67oy574r2nTPBh5U5005H3032x79It1c9K3b96R0kh9P..KzGmXL2CM6M0GgE585xu72A..J09R7u9Xg34NZ84K0Z4R8oD8oj7M382ck0ubQ775rp8144227787zo093480S424QJvV68M1Mo7M35leL50Fd68t202edpvwL1Pa3AgV78c71y9Y9rqy83Z2mfp0c..O859f9Q60r9h03Gry6J8UVcF835s356gsgNs57ee6H6577992343V60x3bnKxU761RT6e72NFF46X72fm66okA1Y6T8004979M03e595l2z0wfZYNZ9CID489F3S8..187GoNvac80251izJx38ZP30RP90cWLaaPQ0G0551V8qF9G3rJ9B56Z6r57R4y32qc7M3TS82WW6gSJy501U77l52JzkrARRHq1J9LA3X00pH1TqCkBHIcsks1y5840vk18zb8YAO4bhg1..

C:\Users\user\1_102\hbnvn.msc

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	591
Entropy (8bit):	5.467808890344202
Encrypted:	false

SSDEEP:	
MD5:	8302D68CF6B041D730204E06643003A1
SHA1:	A3003E66960CA64B4B42DFAA70EF0CA9FF52EC9E
SHA-256:	902834812255FAED5AA3046942930A60D0BA508D0D46D978EF866DAB57539098
SHA-512:	277E04DAFEA317A4A392EC0EA94CD162FC48EE27A83CB523040FB754F5D45F861A59FF1032CA5AF53F5C24EAE89DAE6A6C38EC46E2E0958050085B955C8F6AD3
Malicious:	false
Preview:	77yRJ3i3U738RF83242oP50eM55H8043936k12E77266Q5Gm48h3FM993k3877F79L20y30962qu6waR5QJ8u6y951W4x0M4557culDE..0h494sJDmF7WP36H324j148K24Q6hK5xK35S754N9K3b1PFVsEf56T6e7pcA0450XyKRf78N3OT0N1R5r0abOEWuiM46f4p3xQldG3iXfd034hAb7b53XwbV120ST529O3Nbv7QJc842J3E11n0b87BQ8UV465usV91g6ngi..7g1a6DXdR9YV8Kk9834PG4x1R1xw05rC173kbq36282EBMgv924j4iq6J7je2Xp6z5K8qKPO7e0kR7V2qEp3WwXx314f780TMv227ZW9200B87W5e0q..Rin6a90W5806nE2H656195eS06tl712v88UW2004i5r7JW267Bx96tzOOd9ZkN9A9cJ54Fi36katB041..5W65g6..0c8am9a7J68VEaW5024O6M52Uz5Ed51st5O7roc0cPe01136Cg4J3rZ9eQ5RbK65S9c20J4HzN0g0803y71402eX1322sWL5EX4P5qvw18..

C:\Users\user\1_102\hedweucwot.mp3

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	529
Entropy (8bit):	5.4438129030545515
Encrypted:	false
SSDEEP:	
MD5:	A0B601DB16CE6D535BE352965468FE07
SHA1:	F57EDE679AABD57889674E1B2ED808CEA75C5E40
SHA-256:	0EE33B459F5009DBD2F7826D2C830CFC1CF7DCA179FFFC6CA219668209BE23B3
SHA-512:	3F8D7FDBE720D3848AA4F1EFC9F36CC934D110396DC20DF56245F9538DAAB4986D799C8E291E3F7A48F29A78A541B473356C0DAE73201FE69278C6DF06B0E2D7
Malicious:	false
Preview:	59AWu47rOEN720Tq3L4X6264635c1G45NZWzwYN42753f1M0Jd9y752y964F6xz3017..27CS2D6m00QV7H115U7y8vq3y221d781yy7au32O3Blb6P..pxI5W4iY14603CF17199213A0Hb05R19av66NWdN35880l7JD6b443l7nvVf8k9aN687fds0SWYY4oU8ZV82OxV4thXSUfIDM..n3hHD691C7845oRh67sa6jXZz10R283a17sYN12F14c2..aiE5258xQ0o054Z153p0350fe540669P77202hNxpKye8146VU5sE4A8m2f..3x3t7SLI74101Ae78pqBd40oP17582K4ciCt98n1432gU8H4UV70D767yGK95L3r352f2py108x42L2b9Z2nI1886K3N93Eb5vF1GFOjD630uu60vzb2641..X4j6E2WRp7hY1d97N753OlVmX64G1353M186xWlp89L430e3HcXO41g8183Daf9DE4B1k1aD75G80tA53Iv..

C:\Users\user\1_102\hrccfoi.mp3

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	630
Entropy (8bit):	5.516598658841613
Encrypted:	false
SSDEEP:	
MD5:	8383E1870B90DDB0DBBC6C17C1096E25
SHA1:	374B2DAA67C01248F594E6175F8AC85842D3A0B0
SHA-256:	0A72779DE21DCF99924DD8358E3070527FF556AF082C7A71C8C130142211F9E7
SHA-512:	DB40537B5AA9585F2EDBD8853CCA991F3CFB66A6F231BF7ECDA8923B3A470858E71E462AE22BC1904914098982726366281A44A13DA50FA7FD540FC970D0DA47
Malicious:	false
Preview:	78c5nOA0o11A99oW4t6mgM5b1q6K3759Kqk5na9Ar3EI..OHg85SB3co7rg94FKVc931A4VO8FV744U3Fz4v3Cg2fEacHT3BA528NI3c2Zr9953..Wmh4Vn88S8Hg275656F8U59q76V9Q949xxX47xs1p6Q74Q9W9652hN84f96qe06Qt6514D57j25vP754P91PyC6bwK9fTJNI7H4vF39zQhSle86UE961k..1qXF8bjTFY515DP59z5552e12Wqwj7m41arza78x9kw5A23443ZpqU5iojAm6x6HI03T8zK577dS77Ag6kyV39phq9nX000ZIK74F94lR6SQwQL78886154l886mf..9D793e06sB4eJ4T827oe536z752V..JV0cZ5w021P35751d6Sne35v42f828fy6kak8USQeN02rj05U3553K1UI1yA643E18aX91AKqV3MmMsQL..M4O0N9CK6ox5V9V75Hn3tS8t05Tr2142JkRR229G8l6Fx35pM2FT1prf675B514Cd8b435C3Tc4EE9lfWp14T6N96qNv6Wa014xs4M9807uV0Sr3Ta3gjk1116g7fMK8YM1364gwX6yL2EE776384G0fyY69..

C:\Users\user\1_102\iqdsniwt.xl

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	513
Entropy (8bit):	5.3949891433134
Encrypted:	false
SSDEEP:	
MD5:	7167BD2FB9AFEE2660965BFFD1B6C115
SHA1:	B031FCC4531667FB87DAC87EBAD83C70443D032A

SHA-256:	24A778A073E03FB4C263022D8B68557C57FF63EF1D85B0DCF115B5EAC04EF4FD
SHA-512:	7D4060DC0E34182DE1367C1808DF78C874179DF8FD920483FD5388F2D008AB48609BF753629A1850FFDCBC1AAF6D7D0E176B7BA570449F8331443C44FC0E074
Malicious:	false
Preview:	P0h1C97556e6suv68r3a76jb87Y187472bCf9W201l30z5rM61Y1leTH0fhj159r49069i9zCl66KdL86QB4Oj..53nw8020D83332U3337pATI100G8i6lxfAb75665u9fh09h62eSI 2P..Y7ViN4Y88q5j2Y8K2H04427lLpp76g227y9g8L3Qbt4N8c00f9375h7J..39PEd84i5d8Do9N96n047456llr9Q0s1A3PCA01Er54oRu4DM084n6X6AX3p1N0f..0I 2z48gDupaPq0t9286U68366MDkp5964dG707v..XzbFk5CPk2..6B253XW5106x547w714698vf4VZUuE3tv3r52W4b3462EWZ70YS34y9c5xM66x196Jhf7Q76O972t85 e6D6h0D3GKyZJ4H61bJj16m9F4q1l62O2c86a48281y07ijn1746o26M08z1fG6T6566932..6s09v76y71Vy7zxW7S1119Z8e972j0Gg5r7hb5..

C:\Users\user\1_102\iwtbbrn.pdf

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	540
Entropy (8bit):	5.494341517091222
Encrypted:	false
SSDEEP:	
MD5:	A1E8D95728AAF329A8247673EC1DA164
SHA1:	2AF3CBFF97B65B42E09DA2F456708E2189477431
SHA-256:	F18068DDB07529F55EB73EDCCEF5178E2F7302C8D0DC2DEA8E6DCE85B1D39D26
SHA-512:	AB43150EE98F290A35AABA5A2BCDBD0A971106777EC828B32F6FFB2D519BDD50DFF49C330909F94B081461CE765BF800D82C7FC03827EE557790A72F9BD98A9 0
Malicious:	false
Preview:	7DEy13Euo0775D7WZ4C7Bs0ukQVZ9N7Jis06QsY854df9l0rTh9Q4lC3q8c96yyK7h6SJ10cMb61vQBs7t704mJ11A735plROv06sCu40CUg1v93H0476T5r65xmquRe.. O1t5jbU17y04X180g42Rjsp..h15923P722K1C6645tW1v23Kp6Nt0rDc71U14Ay71948..fE56t64M4clOdxt6OGs1ai340327Csr0TOpv5qrp1A834y7c061c53o5133 0Fh2l4n57Awut655v0S1R3kf99..347n52hW077M1N333868BoEiMRlOk82209ifuvVKz35a3S015864168Z69HVl3T252u9Q4w307497hvf83pFO91nOO6d6Q1c0ux8u. .R530S6G8lN1q845Ol23e45306Ru931P4W0KEh7SoQdb695hP6OIH2iLq30w6XwgnN68pG10h659jsBQ9WXh99PH7687Mp6s2B..D2sB4Tac34m09F54756U7f64kf769y e69q77ll8hYGXzc5W8..

C:\Users\user\1_102\jpfhdaeg.xml

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	513
Entropy (8bit):	5.3992262540886085
Encrypted:	false
SSDEEP:	
MD5:	F17324F85594EA54B29A63E5D18702B5
SHA1:	16F2756633366DF146C03BE44D0182B3710D37F0
SHA-256:	6B7477159BB3C972D9F534B150FE184B2761C427437421FCE5AC33D14F2CB61C
SHA-512:	E0500926519ABE6F79B93F6C51127F4221F23E6D1913366A076B860C19669F0C07C945FF368F2DAAD3F76887E4A5F680C45BCD449DD9C8A70824B0CBF27768D6
Malicious:	false
Preview:	Xo089e9787z86283890x71Eikq3x9WVsG8E3034HZ6Bi4f0f1V5e0zO1F37053K6U82Q32q92y1xB6YN80816168F89Q6006R69jeN99a85TUs3L3BpgiW..543w03Kfvu r17d76L8U60Jao5jna203X3FXJGB972F8L3C588f7u65GR865224ZO2x7D235s9425L0i560YM2rhu1v968833219hDut4H53X566i75RM8l254682C6t9530Yg2..8EUB Cwe113t16x7XkP553c05HN0l934d27y7oq78150Z0jH60p68cDxMO1r5we4gcU28x6Ob55yUX3DHxud4L4MDP07Hoox6031845088wz7F65b3hn0375q8S7SH148L97N42 69gY0405Rwy9ZpJ1C3W4wTwkEBd22kOO8q..6N5H5ai6602260ItJiJs8fS07911k80i3y5PpuX4..VM40ckhzNyRq7z242R9b2933R8Sjwf089qW6cqA5f4Z..

C:\Users\user\1_102\junnhus.tbg

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	330770
Entropy (8bit):	4.000017803033723
Encrypted:	false
SSDEEP:	
MD5:	EB1CCD9AD7C05D6F77E14F488A7ECD7B
SHA1:	2D3B3D67FC34052680419279308E93ECABC2F0F5
SHA-256:	9C6BE7508C3DE7D4502F32F167129AC5ECDAA2A8A83825CD1826110B5551CF2E
SHA-512:	6F37DCEFAA02D82ED509A441486DFFB3FD148A8958B97C405B13075577774AF8678BE07A8BF86D38B6C9268B6337BF773D84D80C244348CC90538BD196C302D
Malicious:	false

Preview:	DC38868D7CD9F6D262F504B2D3E0C93FD9C4E9CDC46D871E7A7FCBD8FA00DCFDA16674AF8B71D50EEAE3602ADC5FEE76A8F0FAD84F51ECA0AD81457C F814AAB6061CD92032E124583D410581C5B90A523B7045216758A4A06C022A649EC14479DBCF6F203F06F318CA4B2357EF588A6C98D9CE8EAB77C272 7CB861EFCC4E6085366795D9B74DDD9FC974B28F769A4FE7AF2336B07B8995CE5902031FFE6B88A2F6AC33397D694682AA68BD5FE92BC5F8C0725BA3 4DDD8FE06A1EA10ABA96556F2CEBE766EB13AA74837BBC28EBD1D9AC4C412EAE94CE2EDCDE6E7B02EF301366551CE661786F50D323C6C6D638956645 19C3097280C12E940563F780CF7BF00F27FA49B6D7CA1EB8ACF0D67C36C5F83810E1849373E7C994ADF4D05B4710D65BE176771F3EAB5B1C2430AAB8 45310CA7BDE5B8434561F46876FB935209F53567DFE3D3D1FCB4A6B5292EE1E36D63745FE979D44709429DC0170D72BB5B7EB5EE4421268A5A7FDDB0 FBD404736AD4C1B50A4E044D63679B8407EC2214B9370E5538F897323108B2207B829F3A3B7CE376F582618C1DF73C3C8D1214F35051336CD2A01DCA A9DFB4F0668A77D7AE60C87893C1D8D04B8FA270B7440EBC1102E37493B40D401C116F1ED0D72F9DBF18907C9F7DF5CB52F902E9DB8FC3ECD240643A 48A594C08A6C0D380501109C4EF97E43C6439A5A

C:\Users\user\1_102\jwtc.docx

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	587
Entropy (8bit):	5.4990229248664155
Encrypted:	false
SSDEEP:	
MD5:	EB738A10368F4F49DCDD4E1A9A51BC24
SHA1:	A950FE99E9D5FF86C415117AB7C05960BBBB945F
SHA-256:	31C72EEEE3A3C534AEED8A6512289CA5A2B80276AF8D142119D3DB3D5CD4FD9B
SHA-512:	83A208834CA3053DEFB1D0397907745EC6327F9C669791759C5900871E3881AA7A8EA337EBC81EDDC292AE74CE02BE15D0080E129A4125C219803CB0F703D7F
Malicious:	false
Preview:	89WzDmr4MD071iyg8G0KH4r01HM4A68MWAUP9Vp449545J2vq43rEQiX4A21h68l6iv1L2u4C8N08TV31OfEXU6657zPWJ8487A2c64E158IHB9w27t2E3b. .Ap6NEE6756P7k10OXG713UfW8zX1D07C0u5z3..7i204O5Y1v7mr019d34G7G9usSJD5F4E14z1O4o1ihAsX34tbG7il61vsxsl3Z7X729DEeDS5D499E1P57V6F43O22 5XD5..5XBAZ58j62CB8Zgo6c5G8g66g4777dE0W51B913k6cq86o05MFL67zJJ2620wukT4ag00820c9cKnG815E5..K961m8B45n7X20zS818FNx2k368k78P7Wd4S6A4 3K220z9CERZEgHVAfQi2Mn99vJj764jI545yT8344G25BFUQ0057h..3m5Ft44275o7I3672322..Y209Z0a8R7Bs6JKq3Om6hv6V37rn8Gs4Gn27Ewv62..vY766CbWEy lQQY6323s3Te070X1DJ30PR7kT5512582A5cBq7LK9m1T19699b975djZ2yie9jxB7uz511zN55..

C:\Users\user\1_102\lqiblshv.cpl

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	511
Entropy (8bit):	5.551437262542175
Encrypted:	false
SSDEEP:	
MD5:	D66EC3875C44189C7A7889D164B9D8AA
SHA1:	3C1B4F21FBF4B93625982A476DA521EB61597629
SHA-256:	9E97B4914A4557CBB8F090C101E9B4451E24F9CFF386E638E3F260F86A4F12B0
SHA-512:	9226482F69B518F22C43FC829BAB39ED932BB770B827929E626A5EE5A604CD99FCC9A79D10C6C5414C2DB97819FD2C34BF63A09F60579271009CDA58231BDF9
Malicious:	false
Preview:	86sS9a6Kl96OK26F7WHMro081bskFiAt018w702p79RzkQLYjo52u240NiXM6JW722E6HsMJ5258OXBns09649q729478..t5Ub0vb0MF124k0349HWAg738fXWw1k07XJ 617p12z061W9fYokyqYow51DM71dUK8bcCl0pQHVg0j8a2J3Xn26me0545FIAk..43DXf6Xo..C6RO23jG60yZ1GlexZx40UK4sQA455CjTkZwmxDn6m149O4C1fEOn49p 7l3GKBOaEU00u7w7J5..e2wj2853M96..Uj65W3F2x0V3f96m3zR1y5615d0p3Ue0s8vHU85t9dG62y718Fx1P59KwkHy97U063tQ5092Ks1Gc19Z9E0GGkbW6bN96lOuk 30pl..645Ty9BJXK63Ne2b..0k2a2xfz32l996489zw5y266E32qhrJK94U88y19D5Gl6..78Bw9b857r9404Up8769au4j42J33u0lO8mzeDKOP9pBmEG7..

C:\Users\user\1_102\mjmxve.bin

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	590
Entropy (8bit):	5.499505296046658
Encrypted:	false
SSDEEP:	
MD5:	4FC1CB5F5F68ACD1DB8818BA85D8BAFD
SHA1:	BF5A0DEAA92ADC8B0BFCAB46DD97B77632B355FC
SHA-256:	63F203567456D6108DCF4A804081BD88EBE1143BC4FDEA315CCA8E4E85234E41
SHA-512:	4E4B5DA72DC88A3FDDD230D61020D82DC0C47764986CECE6F41CB2AF68A5FADAADA1C47670709D4961725D5569A57DC4FF9715025D7613D664F9B63512AB92 A
Malicious:	false

Preview:	74251WFe08069soNk6alcpkKj23hzrU300U64f81a985xp8gU83t0bUn1710Z1oSuQdLj5R8FP11XQgC62U8822Xdep54..tb636vS0VX4820Uygj554Gq14145SLMLa13 AW3XN8961673tfuB1994v4Bm71bHs8fbE33272Z9671408E79DzU7636EA9zE50L2V260d0J0L2t82740ofy9aUg10G9ID1PE2Cm9CM412SUX32qe8W39hA9 k11T083qHXJ9H55..g820Q646g5cDrsYY1Mx6836OL5bEI0GyPoztbk6k5Z45t7A51Ec23S0v1XZuv79Ov9630CBbXjo53D7p7d6A..T98kd18i20R4V1Q6mt71U9S19gm BU0l8Vbnj61557835531r9MT481odGfz5a60eZW9OGa81SiC..0OYj9At6ewe2H3N4JdG9n23b86v5F87265tO7i64Z770DCE08240diW..6g8Vp29Em63u54sg121t209 iZB27g2NsfvQ2BQ71FG1Iyf352958r43dBcD7wAx225Dd0xwb7Qb0r11i83n54Z9W88319Fi73S0Ye..

C:\Users\user\1_102\msvvkner.docx	
Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	519
Entropy (8bit):	5.464354090838085
Encrypted:	false
SSDEEP:	
MD5:	0F4A302BAF9CA3CC0F0CD108483FC1DC
SHA1:	94ACB95E7B751632DA37671C71CAD883744208B0
SHA-256:	FE09D2D2BF542E29B0B40C840B5221521796E2AB6CC40B68D867DD306386D01F
SHA-512:	E37F56603CDE4D653CD38D512388FD20A64571F7DA95B715B103876B797C6DA14D83241A3D81EA563EC2F17ADA20C89D25979930742FE128C2894C3CE3906ED
Malicious:	false
Preview:	94VYj6..55r6C7m5w3J75172p5aRKzN77la00FI5pE70713U2fbZ2AAR26AH65hmmxn7P45u9y1oPU4H5hYdt4A8G6509Yj5C1808N515..53kfgW3S19Qu329tj888QIq Cv093zM46nn7t600oY7x7l9uz1T4H409xAp8Z50BLFxe0Q3977Y9Dc77754T67e0f83e93lUG3Rt6pvgXEho1CR59pTxP506r171r9Gq408Q1yR9rY30U8b04cJ1W8K25W 1431x6779x..MoY3BB54741gq780270j7999IgzY7953Um4..290316814284040R3uG5489Z4ieJyoNGs7xGDODFyc3K2bqD7l3cwYdQsP5tVtWL905065T98HsPq7TMI XA40R5e67s4qo0nc2t1Ni8AgE4RtrZ2AUKf5..O7336g..3b7gCO1554K95KZgl96r618957A08N99XDhh390wt414b5W5z353P4g9F6n3l2pvZy46e04u57Hy9385Y..

C:\Users\user\1_102\ngbjex.exe	
Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.512930856432887
Encrypted:	false
SSDEEP:	
MD5:	A294011042563ED9764DCBD194CAD2F4
SHA1:	03299BFA63362BE22818B23C43685250182009FE
SHA-256:	3D08DD97FB80CDCBCD322F4AE15D50E07BD3A4A380D4EE22E94299CC5D2BC44F
SHA-512:	DF9D762BAE3256ACCB8BA17B845A362BC41B677AD4025277C184058B4550E8041534A21A02F49A29D52275A33A9F0BCE4290DD7A7D9D4E1513F889FDF0E7C13 E
Malicious:	false
Preview:	52ZZg07z3eKT5E28g455u70At27VkC5rMc716M012M947IC9v46e588..3CMha..533l8rgXVOh9Qo0W7P4..880mWn175Ej848N216o6gS0r55FjO8L40RBGLtJ63B4zA hM56q97d..1P1L3b288F0UT122dXpAp6TWT50D732v..5037urEn8yZ9A00shru75V9C561R1Gl2Phl4x14099O0d6wX44gxf5F7rUU1P9aP2yBDcB7780..o54bQ4qL7u 43241d2H31wjD22Rp4928TC3b49094819feXuu09K905c2Rl4qy47PmR2RoMm..kMw8GtWZ66xG6V569S62KtP9na7qq90j941Ev69iy84217d1g0Dq5hyq048W394F5p9 r95Yw1Ck3Hm5JDE3O130n201h8q063WWpM3623d504G3OOk46g5lII7xy9hB4230j830l3UA4p3tTj9Qnq..khDo3442i8z1Rz781Ld..trS39u5180n3SJCp85vW2e5G9 4djsN9C0n3x8n69R96487o6HU5n7HUYx223189..

C:\Users\user\1_102\njcbgjubnt.docx	
Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	538
Entropy (8bit):	5.50879030771399
Encrypted:	false
SSDEEP:	
MD5:	920BB470AECB569C31D2E6324CD6D2E1
SHA1:	DFE128D5EED8ABE883198E83F13F43DBA43AE9D3
SHA-256:	BCA1F286EBC2F0212648CD1D8DCE3C6ED9384B09081E55DB81B348CEBDA7CCA2
SHA-512:	C4A3BFC15B203C8823D45EFCD55E52B3AB7DED462A7D3163613F439F0C4E70BF9F81442DA9B9BD706FAEC30AA627D854A1F272BF098706A8267CCC1BD3FFB AA
Malicious:	false
Preview:	157C695834lZ7stt39Z9zFPmU6naU9B4VEOWV85XQ774V83u5072v3ma88158B5G9005g716k20wb332v3vRG27k99J92KW5u3YxM66XZe7467Sj74kWz084Y4i3379f11 L7a55H0196v5Slzb80..GDc2lrP3OlJ602O18..959cimtP4uF..8oH6Dx621yVGm7hjIL940..T65yl99nRU7L9..c011h085..b8w2tQuhI22b11jyOfo20073c61Io125m6R9HX3m 990nAR6KElpZQc8Ljd19AM84jl..5T390j74V14hr3609944r9j9Y50wjMZ26oOj..39MXBO03U4DlZ3fh74xW6cSF44D8qdc474as54L30w0eo40ap7i2ehNs5jn03sgc j62689qrGz3ymxuS018L7y59t19b1DLg5q4oaG0s330XR13Y0..70mA9RYa0qH33Cts0029l8Z657u115R4J22E47j7PCv50lAjT33aH17d8q528U3O975xN7DKy6yX097 5yJ8Zq..

C:\Users\user\1_102\nkgm.ini

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	563
Entropy (8bit):	5.461447205398388
Encrypted:	false
SSDEEP:	
MD5:	E8468600EA9B5C6072F0F1379F09A640
SHA1:	14144AC9B74F784CDC2E42958A43210F973E13BB
SHA-256:	90A3C32AE9371A5C6E4354BD44E07C80F75712F59B4064C6AC85D1853B3C0D91
SHA-512:	57DDF63146FDA91F01A14FCB27C6D1BDAF45D352B4A6F690DBCC60529754173E3B8CA725F2DD7DDC3E342A2306516C724D7258648906A08B319ED5F70E8094
Malicious:	false
Preview:	lrTw20FrRkb9Tx452460..20W4dyTDR87420oa4F0628H0NEK7ne4Gl9vg5K7bNOdp1J74PZ43y71Z3FzNjo0R947r9p2OL9pnb828cndOfjjB6J3kQ8180486OJblMv9M 9z874hnM8Gh46TK5fuNd3H506s1OB31z933Glr2068r24799ZKfPT6305JnO..92L2ef1kF766706M0uf8RAB9079tMl049019Y72MVV408aN16VsZRK4K1f24897h6yb3 pW6L2D952724245nuQdj5V3UhZ7147l8m0G7X2BaR4X3w528Dmq4etaoFw4q054vJYo317S8B89j921z5220h12z70i0UP2l5qZ1510zw5n7cN6ECBRQ9M..5n8r6v3N9M 4apY4J96j2e1V3zI17gM5dV76n824p5Yi7136d65bVOQc7rE30IBE9Q92L6A5M4ZNM51c979Hp7M5KL0113SscdVe73427y4nM0..wPUQ1663o9976Ko8w36 9XQRC98QG67mD6499606M1411473Q7dVIQ6I3989c9gH3Pw9uJ6..

C:\Users\user\1_102\oemfj.pdf

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	560
Entropy (8bit):	5.542858141978373
Encrypted:	false
SSDEEP:	
MD5:	6AC56C71D7588D956D50E68CBBB0661C
SHA1:	9EEAB4A85FA0E46CE1DA5EF4DDDBF7E07C89E64C
SHA-256:	59C9FB1704367C93874A8A79E7929C70DEB6DAE92E13C09ACF1DC2B26B33DEB0
SHA-512:	5A5567688A2306209726848AFF21D3430A528478459A44FF0DC42AC1B0F9F1C67A034EA1EA54162468E10996882EACB0AFFA3CF43AA1C2E26EF9FCC8568E64C1
Malicious:	false
Preview:	91581T89s74k..mTTO6V2IBB..Ac2392VPb3dZ92v87av0NC37033f40OB46tmSF21Wc9wF0Lwio0mvZ7z9bZe6o8b30YC8ppmu54DFgO95CnD9T6e37Gmsw XD54U29y423olqPydh02O73HGa..cj9z03j9w49UR04s925eFGvDlybbwfJST11y51DH3z4f8J310Q3y75NtXvil24FOT3040lffY89M87P3x6e372165iJ9n26au00FW3 UqP3gZj47S6..64ZN8695sWNgUped0bFu2r494ac82X3U3f37fEBT78997p216IC334p8UdF97h916eCkl2aQ05iWf2k3t2k60Y823p6c3Zpw38tn6FwYD892F3bdWNhW8 Z26v8e115316H320n849C97Hh1m..46764SV275rh49aUzqZx9d7t8px6C89c..rBC2C689pWECFr82pbAQ8GG64h62a317333gcAS541k8maM81q19R5G4Qkb5oNB38qF 124958YF0nH1Z8qH4w4S4JF0y8q4K8Hy47YQ02k7Bln4y5E4..

C:\Users\user\1_102\offgxmvkni.dat

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.471748006315979
Encrypted:	false
SSDEEP:	
MD5:	B4D03A71ACED9EB3CFAE708352173AC3
SHA1:	2FC8C380F7F985C1B46D3DC6E598E7C594627848
SHA-256:	B6431A1FAEE9F142CB8909479F9FA40520E68017525DE5A35BEE6DBD76AD17A9
SHA-512:	B07EAF5A9A990CA5B34705700098118789 70F1528160DDCE8C0B1C48F85C3DDC8747D77B5840E19C412A185D76569689547D2F9C713D2A25E1DBD958F84648A1
Malicious:	false
Preview:	5ab3615p4nb2r58g616h5l90uoIdtpY0J96HNe194TmnPK8i7G4pfzT177w7tC3yMr3pN4B7rW79z689961Nm696CEjmu3GO25lZ88H8b07D0CaneAklE352UAi4551F95 2415KgRidr2E2272VB4s9WdDF11a40gk6V833356QDSqYm7d953N47hM14..28036e93t881XhT0bh33Q5mQ569s28fnpVdl7U9528MDO308380oC0RTI082F945fY4202 rvHh7VLslyA98Zq61g18j0P3lXAs61M8l5s3gon0E2nq5Kw53s2yy2w343if1m..54vDm7b4G1l0o3xbb9pL7P79y22350E58..594l9P0R68r0d..7aR56Cd6C808lke8 NQX40XLTL3zu14Y06h8142wFts12b9310sX9z36US48Po0i1x09X9XBzb82..m79u8l6UP4m565e609ocz520E9C353VDt9S3095e09IK193S0207Hc3232236Ranqwm05 udh29T0Ur9C6I29l5323172xBcOA4..

C:\Users\user\1_102\qdmmn.ppt

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	53037

Entropy (8bit):	5.577567030073151
Encrypted:	false
SSDEEP:	
MD5:	B7A0A87BBCC941BEC34FD8ACDCDD077A
SHA1:	8C0C9ADB7B9E1806AA4C49811FA4A2794490C645
SHA-256:	650E29AD1C2A6B951EE4868A5B1D350C8938E942E1796D7A48E52E8F93CABFDA
SHA-512:	830604C84B91DC9012E094F20BF76EBF81ACD6E85825C4481290E81DEF2D18B281C132A4BA817D9CF3FD43A5F5C62A0B40A557B176E8E94A2DCA146C0651F2C3
Malicious:	false
Preview:	t7118845658x93532z993RQ857msPV6kV3l76..EMVO21J8456d33499diU4D0Ti039o7Y84A3440j461Arl355656..E7ccY3tja60dxKg5R50v72Ju7kFt97cvh1g6Mj92e95IgrToRk25..Du604d9f7k1EYI7R6Dkk6H1f600ITN95M7SELG0PJ747890580K8E7n886Dh3Oq47W9..Vh56F0L82Y2ja8039vIkC89hd21424716..Mj5cQzBdp25v8DMU8b06X31x69465G1DY45hB09n0B1HuP2136VH005HW4T5J5..STg3w34154B3G50Rsz208l568B1nT8m7M8by892Lwj7Z6fd71x66R05Y61i24I3..B4QZ1F378565x8D1Yt94750SzuPN6MWL9E502A1lz96TGH0f90ZRn7j1256q27A906e77voM0yA8O1h922L..7C1t03MN8YP6t481mg97L4331j7bPPor3W3AbOl40fO5DiDB2lqpM1H..1WZNYD1e30k087063M873iK..Og4H50i069ah7Bt8s71FF401Iffi8sIL9e84K6..B8948ogP339UO6thklqD991OAalv2z..3h35e73B51tC8dDf5C737j56i79Ov86l8X56K9yiE7659287ARNR0..7cE6Y4816PG2iV605o4cUXz5Q76ee7b7..9E612IlWcvUF372H3Uy05P01yB7Ri4..88ds3R17PT2hW0bo75284AHBbBmDM..0N08g5apfslt602tEf7W33YXe252xq3k3O4y8G0F57258adznu876..mmC0D8zR0Ca7237w9l07l55684e29806q1Jw534Hn4..C794843e1xQ58213a0Eg820iU62Z7m..62572VqK3OM63ii5aB26E4f524V513l6..c0NPk3Gk9Kkv1P91E607P51aP775O10oMC7v90D1T3XR9tS16kp4M034B..007667

C:\Users\user\1_102\qhojj.cpl

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	548
Entropy (8bit):	5.469459668817943
Encrypted:	false
SSDEEP:	
MD5:	D9C884DE03C4D546BEE4CC592CEC9788
SHA1:	92982BD68473826B54D1F2EB792E8B29BFA0D83A
SHA-256:	E251E26441113CBE6C03287CF99118407E74151396EE1DE0AC9B47B7175AE9DD
SHA-512:	4E804471F323B1B4579C7DB36099B1210E968BED406AE09F735AF30C0321AE2F5C88D946001A635560B7A208C3A46201E1BD202660F046637AA75923494EAE26
Malicious:	false
Preview:	73GI05T90A45T6ov95D5k4P3mvV9ZH8ngo4n77deK87r814h92C793z824w31t731dMk6B9L9TBY0Fxof27748U79..S34hSP6xS7nH01L5735R98765Dp2ThhlPmOPp5h74cm5Z56s177wP4y93X5wF0310C9O819juB18oE32x1S2ut2mf4N16n6mcZ6M5oq3sL5A7x703..z683m616B4jS049Yf875rM63xL2Jf95d1v6z7urN8qC6VXi4bhg011g3t07a1858H0155Eo7oc80O4768914812yBi5tnP0IDe14yTI20MWxP5..y0S7U48c5491u3E38587jT4bq0x37P81o29778aL9Teia3b6Gjg15sqg18701814h1Olh780P..804CSDy33w4GYQsmv21nWPV8Kx93uC3s2x1588X713x30a81F60a2i8p8TiH3ZDZ230tj5578lBo4UI91L66v5m7eqzf0JG24n52tc1hWQabrAV111qGJittgkF91tL1uaKf3Q41o397o69SQ3n0V22Zk..

C:\Users\user\1_102\rcigee.msc

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	519
Entropy (8bit):	5.469785608960364
Encrypted:	false
SSDEEP:	
MD5:	542DCA4C1E92E62858A00A97C1CE787A
SHA1:	D7C307B124633D0434C71BF2DF39B9A44548B95F
SHA-256:	CFCDB6F0FDC559161D291688EC7B8E9D5A6CB6A27A781074822E313C6E5A93DC
SHA-512:	F2607B9E0294F097BB1C4DA99B6A6D6E7F8D27A60DA44EE75ED01F19676EC3F22E3F9E8F147A40FE93C6CF06C576593D00655A3DAF86C5534FDAC64215CC14B
Malicious:	false
Preview:	8940SN80Qsm0QdBARX3226E7Vj52dMA2c61474CrE6g14r1x5252B14TxaIp99WWY9MZ..f98FK..64HP7Dai8C1tr1rL740v3SrG05Z3jJK3S9F774..Iy8P4G3X3f6g6MrYzy1x26RN3d8d0653..1ia4FVg10a1h41Me71y94PG3J80388Z0mX4o6yHV4Iq4fDgx98504891XhSAUgUg3364..2k1Stg79q7OjYfl..0j9h1s2q1LwQ27o53M82jD45N3M8zp0OW2CT19hrY511Kc03526m199FePd7g0L05HMlu2Xg9c13OzFVV2M..839M3z8TA898497y737A401H28Yz8Gtr00f6795M6s0U..4zRzY3z8cnmO3s800R12z7dk1bA570bB02bt68D505R294768Ka2o..244S8Hl5d1O0a98J8i41H29lPS148g1aGf48N5W06o35K445eFM493HRW..aq949EEG3L163M1L4mQ770JQX2644M4x4c..

C:\Users\user\1_102\rspcco.icm

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	602
Entropy (8bit):	5.480265808755474
Encrypted:	false

SSDEEP:	
MD5:	E12EC310ED295A4E7BAD30E37424DE67
SHA1:	76BC9E4487D023E72F12E1741D5BF877FCB3A051
SHA-256:	C129B7D0794C62012D7A1AE74EA31EBB231F56FC5BDA43EB3885AB1019DD6DF9
SHA-512:	8512074C6AAC3FD69D677A699D698EB1CFA084B1A75C7138D8B4F65FBAAC9C489A1DDA20259ADE42BB3E4FFA7CDA3F10F426D8046031B4072D0B67B76EFCCDB8
Malicious:	false
Preview:	4K0S6pttGE71Hc7jMWG6JZBx2Wka561UgDS9e00i..806J2qW39N30i16z47J55B8891mJnY951507FA6Y956E3FCw7L8e99TV370w0HWCt3RwS6V20aMY7s 42wBMF7C5jDFW662J23z6t8S11Euf2NHj6T844e3A7..765F6xrH3wM4zi4Q83428Xy778N24w0qs0UX9Df72..Ozuk25IXjb58k822J0p8hR33if0907ns4Ea1488ZV0E 8q0e5Zlxh275J60h0g1F0VnK3Uf2l04d7AD3nhkAh4TgN8D23v1WdrP8W56i87P60A6K3..DDW80Ca07Q730gwb49204My8785Z14cLk8DHH73v2M23P93370601124z27 n2t3mdkwh0d439H68I70LQA7otJ01rGLJK8F203zfzEw3406U97Qx538006r4LJ846q09nQNs5KkQ037z2D2C6J1tgau73815432H6h8Y..1Fcq0s8V819yJ5T0kv9Fc3B B2zZU01Ut7rfhb6J779ht7757O0ejP1618f1XE92M6pKZ3PYGs95096g6e2905PuKYWSv1oe65604OUz42882892xs..

C:\Users\user\1_102\ruiorm.dat

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	514
Entropy (8bit):	5.471533588025103
Encrypted:	false
SSDEEP:	
MD5:	051A53AAEFC80A51743842F3627B9D0A
SHA1:	89BA9967DEC44BB305356F4D62551A728A6562EB
SHA-256:	3F435A192DEDEAFE627BCB9CB074798C1A5092B97BEE366E8D1C1309687EA21A
SHA-512:	2AD726B1AA0D379F655C41C7E74A238B2D54383620B5BB4DD731878869129AA3D53625E1A1D0F7FB9B61BE96CBF15304021EADB8C1F370D518FF6CC3CB7294D
Malicious:	false
Preview:	y0B6KpW5zmub2eHr766x9OaW9J55D34jC728365h26X8724tE5f384F70ILB1ovibo7p5..04530w6di325x1Z120tEq612299a5Hlh7q6jh391MZKUn456u6M88m175Tz 7pPd0T5iRayo53rloM58xQDN..88cgsR85u0lXWw7W63FI1..aH1NlMl5864N9hI18AS0L077sth68bQoEs690i724G9fjS6617oVl4erOZ4CtFEP3sE61170UB6B89k6N 2m895b95rRU..jvX611270Z8KyB6E1134m07Glwr6dI069R5xl263sh1379HU78u92u94..0n74wDL205Qjf1783u4E9yz6n7D06my1b2fm17413lp691n47Gv83a7v02p SV5f9896bK0m3G4698l2KX4P86cy6wwy7wO83vu7321Tiw1Yab9cTq2C799f0G5771u5sZ70e3k36l37X8l552fvl7YQ5hO19Nl2y6O2ND3F3550i0ojm76V0T..

C:\Users\user\1_102\run.vbs

Process:	C:\Users\user\1_102\uvbdlqfvw.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	115
Entropy (8bit):	5.211885843440307
Encrypted:	false
SSDEEP:	
MD5:	474CF0E5CF7589E604811B5B5EFC5435
SHA1:	1D5D718947F211636DAEAD898F5A656EDF490271
SHA-256:	FCB503CE8CF4874FCA9F3205ACB01952FB5759B1D784040E87C5954F6E3C18F6
SHA-512:	F314E084DA5C29896B720ADC2D1B229143E4A14B92E03A12FEBE7DD1316F238F6F11FED8BA6D064C39B74BCE545D3401D5F718945DECFA10FDEB90186431D1B
Malicious:	false
Preview:	Set WshShell = WScript.CreateObject("WScript.Shell")..WshShell.Run"C:\Users\user\1_102\UVBDLQ~1.PIF FAEUPD~1.AFR"

C:\Users\user\1_102\sbuloo.pdf

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	577
Entropy (8bit):	5.54461833354177
Encrypted:	false
SSDEEP:	
MD5:	46E90298A3B143A9272F79E44E90CBD8
SHA1:	97C88D6CC00ABAEEF52B628DA53F5BF069E27068
SHA-256:	D3D09EB1054AFC8217BC13195F5011B2B1E264118A03DD84EBC3FD5903B610B2
SHA-512:	58CCE89E28C2DAE797AE8CC905C29F89F5F2808265EEF966C48D959AE91377F960C171125915ABC936F3444D67D9D31D7B7FBA1BE743DF1B0A6EA050962BFFE
Malicious:	false

Preview:	53v8kt209e3aKW3A365B55311or1Xf578yEA6546s2c9my85296310aOo2Mj90u8Z6se243E8r432XY55878a8IxR4220XV8M3jU1a4w4170CH4zkR0G..L77sFkRT7fg5 aO3aE8H728sL40U666xSvTQ7530liR97Jd6U4Y1RU1Kcig40Ch40R40oVc1Wi41LvNAbD4IInujJwzND189wc0PD4629s..x1uE..2VCI3914YK3V0708w9uaKEA6Vn41A w597d6s55eFa863mLqL65Ly1TNtEQ3W2976iD5dt9Y4Cb4K9ws49g357u95350..Oeu1D51E6S8IFzx6w..5h266t1dn7SmrS4i53a598l6w4q3CR31S26y3RZn..cJhT8 XI74tv5f08qx3Smsm6nK4txi9LjtORliC..HYPt8937279Q819m7f315uL4af7..517jIRD80AHM4u6iF..8CQ434DWe2K95..9k95wCI2l103R50qgYP4QX4F6QdFXeOR 04kd7w6N2lU4Z1048375U8z33r2M3oum53ad3XZ7TWj2t22838x12N4..

C:\Users\user\1_102\skqrmlsxv.pdf

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	586
Entropy (8bit):	5.537777702994396
Encrypted:	false
SSDEEP:	
MD5:	9810605BECED17A2312F2E939E0BFB51
SHA1:	E04B796FA0DDF143A35C1B4E84E246FACB83B72F
SHA-256:	CEE68A3BD433AA3FE26FB204D81527A4DA672767E3D7E9017A2B4EE3F92A46BE
SHA-512:	99A91F76AF8169FB2FD7B53B10D9AD07B345AA5D637F403808CA628629948B94520DE53E63DACE090054179A2F76919D8B4BE0DAF865E3AD8A58742383033B17
Malicious:	false
Preview:	38Bpsg8ALhVk34AMy971P077I7ks3ZtcwG88ya4b953Pwr4l5zHKp538aBW72u8jC0T7ZQ17N1DA1d64BiBYF71Z928O8i9D3620K..631a37gpOFSF4XY2afU2S2l6f9l x6CcQ5idC17w2967HAQup8y8jELUSm53IL96d542Y6N9j5hfD8Tz78299L1hwc753rT05O8B607D4216Wm2I0MnL1RrD0693Ogz2140k..h33p4uE1744m..T788901H75 sTnA091B2776QLhx54l2bRybXIE4vt4Qp7X9Lj68dNNsF1lmuonU7n56L18m860M9z09X8y55uS404sbO78w6n8I19RNT750W6O31SAPARypEFV60MP2n7I0Y..41aFnbk 7..bB650756iQ41hNn06..247L2zIW239S4OGi2tla397709yF2QFrE362..usWOXh1e0DG2mT053s0VX9NBD92Ty6b09i07vI400711Fn43Wb82zN3W2856whpb53QRBF 08H46851lL4Ct12C2u45WhJ19RE7Rf5f8598113pzkY501oVU5MV0wzkXpi2p33j..

C:\Users\user\1_102\sqvp.mp3

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.515848859026026
Encrypted:	false
SSDEEP:	
MD5:	8CE0FA72C43E404C5F6D4BF3106F4518
SHA1:	DB03B8A3EB2A17425D74AED5AC07FBA176FDEB7C
SHA-256:	515C9F1F69E56762CFC38FFA1DD31484E877238BE26DDD44778F2D67F50D7B31
SHA-512:	8DDE62093469F7DD20FCDBE1CD990790C0B0A22CB4AFE26967F18B86F83353F1A72F792B9D7A9209A4A55044A518757AEC3F5C7E0C5307C8506E479F125DBA0
Malicious:	false
Preview:	xHE11R82KE8II0081OL12s6supH047OY26j0cT722w08tt7S102q6692B807rO1kRH1L41jeb9ZOO2642759xC54DWgxW52CINnp7wF45oOWC1iDk2mSM9W2 4h7Z525C7fz11KG2H06KiBY86Xv5Ty9m345p6x9..W9937nUgvC5mp78tg7motz8eeB4wGRNX12aL193jsS7860e3wWT3G607vUsJ4138VY9GETl458ku3G3h8OypS1tPm b3hK21Hf0HPg61glc57ny9JB7T74g81zD40o3441Y33F5g5h8U6e893W9QLR744V2Y7Q5uY65I57..504k6qc9q4G046tMdTQ2xm9WH7Of2FfkQ3LG71T2Q5To2708T8CU 70fFYF769WC4irFBZ56D68kL525732PV65Z0ct961686v10690CMI7xk66LnA0t5a..K5NRL24tNDwH7J82288i6jET08X46508337Gi7PyxoA6OY0F23722w4..

C:\Users\user\1_102\srcruart.pdf

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	5.4832973740986315
Encrypted:	false
SSDEEP:	
MD5:	F055CC8B562B94D84E01CC6C65970123
SHA1:	6A32979F2463A67324902B871EBCEC62178B719A
SHA-256:	B7C44B9465F77711131E2C27BA66CC80107FE2935B36A70CC91B72A7A17701C9
SHA-512:	549FC1827DBCA11720EA663C36E6D316D002F906A97E2C5D8D5E1BB012357FF31E72D0F96CE97FAAD9AC2B9B5077215A6B9A87BFC1B6083EB5F1BA90A7B0F1 C4
Malicious:	false
Preview:	PU4t9pw5YcdI3TbXr2Q9w13N..927oq3n5963C5007GB4pQ7v1dF2zUMj5nI9XHRA7eEyc01MRn603GYsb53n4sgw02uvnXjWlc5w8y3563u0S04007b9M56Ux56j4yAJy 63I1..K29mS3Z46za9OCbO1Q6376lhki56CL4nk5qGP9..16571S2241NNm7XZ1E74z92Oa82G4220BH3h..2URB5r31043g29W7X04CbR90N8K957L163325zsce25749 p4fg48cj24LeZGZabs326t59tjb829XC8Vy23N4QG0vDJ7R..8Frjm7k61EtxT4kx44d32w36z4Qp2ABcx823tHp2bh2V7z1R9D0HGnmV1W73a6MJ13v791..n199N1r4H nP2G1Vv61I0l87s9G46iurk665qYi9227P7049D1L6YC9K577l0194h6n9v4W86fk423wN4J60791M28H71f75N58b223N559..J3zSD12Nb461OB19K565uq86o6yDYR4 EM9fhN3o70YP34j9Qn49Z42682C7K4uE570cP698Zg6sWfh4L9EL12074223Jt2K9DDR01RvyM2NV46z1XxjSa04977rVf9a36350073o45T096annQo032..

C:\Users\user\1_102\tmmcqtvmur.xml

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.431556026528404
Encrypted:	false
SSDEEP:	
MD5:	1BDEF3CFD528AFC04DDC98AC98EAE3B8
SHA1:	BDA3FC0E607ABFCFB2D5C74CC92DA17A995BEE92
SHA-256:	F80D89FF101198A19BE29443483138A42D4815E64BAFDDB2C73E214B469BF82C
SHA-512:	30BC78B46926C77C9B0E6D1D9D65AEC25731E2D4FE58C09187E11F01A54A110C13BDC2F640CA2D02653C47428416027A9C4FE6D6D3913B7B28CB7A9D3999F4
Malicious:	false
Preview:	4F0825G224nOWD1V22712367TtA147sKtdr51577j5e49..krUZ01b7W864tw7B96A0Wx6Pe3g0X2v03R4218201w9e17C4q616693R9WMW34nb9K00234D3vJHU8578k4l581gw18Z4Q8dB8c..VO11qZpa5M4MeY41W4Ch2gXNieBCpFK124cBU9y9768Hk24uW1U0Dg6TetW5p7Rb239l3yyo1Yo605q1K470gV4F8357grL6105Kr317KNH4KkHId9230A5Sn37Ua8Y3R5982YnRh84..di8nCDh71481W62j9IjLp5umSI16U0IR58St2Ae36BmwiLPQ87L40B486aW70D499uPX2p63Pnh1g47e8y832E5v3..8400vB2mVO22706Ep487C2t8Tnse2oiv4fd1Lp67k9gi63RO17075Pb439MvF3nRNaRc7YG1b0g4983F95..r75y7L1M5n1828u1lp9un8k426761v70l37O39Hy0Y4im462N1pis6655Ql0h8..

C:\Users\user\1_102\tmmrvkkjm.pdf

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.542112900656481
Encrypted:	false
SSDEEP:	
MD5:	0AA75B6B4CE7811A2CADEE8B5ADE5A76
SHA1:	4810CFA42889E6CABC76A68D8BBAD1146C5E9B66
SHA-256:	CF1C05D66F55D68F850DAC4168554675C1467AA35733767DE931009D00C51D24
SHA-512:	318059FC961A4755446E1CB96B590B23548AA83C52C7B122493438ACD8E6CEF974CC42B511EFAFDF9073A7B8B11A7B0FF76E7F543233AA50BE06FD4F892BD876
Malicious:	false
Preview:	v4799gKptNW21OspK6p98JQP1l8Mvs6195..9700o83hXU24nWh697721R4ZIP98018VJFUP1rA06E6HG4CH01tp886Ywf9v4c99fq19zI3071uT157Sw2fp98405GYC8z6h8K96267k..29riA352F4vr03L0H81e535m5c6cXd2I361L528F0A3094866eR8..15lnTfiDO..a6A8840RY..PIn2241020Qo9oQzvU0KI256Z83eQ7xhg3Qi..3264ki2n6T50Z5Hq652Td27uq5x3bWA5t5qG666d0fJf2em713OH6vz21I2rRLw4..aQF0985N2p61E4I7h66598lun25BFI78eU..0Y468S1pgBo22ZsUG00K66D4J7zQPH0b4A2b31P2gv1L232a3sui843iV7GEw0lgY6J50b91B60999EVH1F5m29R86m126h7WKJ8GrjEm3V08W5v02664Rxu57Oho1cZqP1sW7R86xo..1kctY6pKm1iYW3I5UB8dHn55fymTIhUEKt0h5tI84a3Vjt72UZ0Ull717D1686V120q3VZd9bDg500k7y1uApr79875JSe53e4eMt44f0coA58Lo63f3o18EW045T9xt0CD88N1JQSK990lb96Y..

C:\Users\user\1_102\tpwck.bmp

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	557
Entropy (8bit):	5.445468719172305
Encrypted:	false
SSDEEP:	
MD5:	A0198613689D2323530B2E097D8BBDC7
SHA1:	A1AF0DB92392C2D2D7295DF27E7B0BE28F09C32E
SHA-256:	3470739646B3824D82F517B7D3E421756C4B9C3442137CB2348DEAE6983AE820
SHA-512:	1435AF86F728C790BD700E4E6FD6E93DCFC6E9528DCE69A32DC669B43E5ABED271FC476DF7FAB3D97E0F2A9C4233F87BCE382AD93A8E7A272897028519E81E5F
Malicious:	false
Preview:	7yeW3TZyl282UX9125sc8a6z25AcV3yZ12QR8w4oXh1ps0o7801a8489pa95bP5a3zr8UN6..56U6oe5m5t0n4s99q31608ri56J898PNMt856J2GU3z8M6PD6BP1Ivu246Ft752E354XhYN9N..77z0006j625Uwv606K6T1TbL75M14bF190Qm2474xR1X8PgA87a848p..29DYa4YL84HS9BF0T3NH2asjkL6T3Z6H2W2hy9F4y11hH183BbL9flf8315KZct1JENVc6QY28569z50M1a7nG91..D1J98Nb9Z..AWoFEj9tY265X4Fff1vD5H7K07lAmT3l91..Y01FT5ma739085157uiZN10f14E749Y153jTsL1H6g4D004vT49u803NU8aaACc3YB257Z0d077ugr132G8yz82D20DL827zNgN..3478483l8h84304UjdD4U50951KbT46bF919ryysQ4MG0r44lN4KFliK61bK9l5z574fH0U9D6dR5h8NPCH9zN68l86O70Y3053ADRM29254Jw76..

C:\Users\user\1_102\upfisl.msc

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	591
Entropy (8bit):	5.5483197473241335
Encrypted:	false
SSDEEP:	
MD5:	F1AAD64ABA9607D2504A3026D913C6A3
SHA1:	A00CC9ECBEA5B656E4BE8FFB72D0C0329DEB3AEB
SHA-256:	D1CB18F142195B0C7DE8B58A1A133DAC507D8F624C0441759E3D308051F53E12
SHA-512:	E838562F314A6CAA5042C4F4CC7FC4901FB6AF554161ED22B036A00DE665F017D68810DF4678FE7E05B902B4B57D18DC54D9726AE398895C70EEDBF916CE4F7B
Malicious:	false
Preview:	Xbs28pH8s29k88cQyB1nB0a4x5J75L7I7l..482A49Z9G410P4H38272F0df1RPCRu20qkH63A16F7u115u9i6Q6pYdu16q3129e5uX25hHu5131o70B2W5..6kuoT1FT6WC84hjYiv407Gm331p4z3x50w3g49n5c835JEb7..5Q0Vb0u046fn5Vri8X431htj501V92g44Xo31yRs4EV2LIm6sG6l83F6sl0vq49h3sMxG2..3LdQY55WwKC4q759j8O6..3Hdw9tVL83ol0s7X3TbkjkEVG39O7B5Cvk1D9Nc4C6Kf4h1F64h1r7331W076g350jvGoCA4q88x4TXqM7yS6IAZE0dsms051iY5d9A7XcLM214Je1k822DboS4gl2Jn7O7G5U0..4Q43EVj8799j1ie84W956ae..4euw98uji34l7076w6L401B6sTG2Xbf8a9Dj194K9J7qkk89u18l99K..WW3NZ58NT5E0474722a14Bt4r6ur2p78xq679o63PiS730fr4k18eA41l0Di7qi2l6a6n61Z969FP76828QpZfz8sEFgsg9p64paQ3Y52..

C:\Users\user\1_102\uuolclj.docx

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	5.515924164934417
Encrypted:	false
SSDEEP:	
MD5:	02020CE3D5A7EA8C68F7B36696C528BF
SHA1:	3E603A3710079AD149DD5EA8BB2469AF627ADC44
SHA-256:	8C313E12003927FCB58AD878D023C48AE2C2C9540214474BCCF08F3EA69F5CC6
SHA-512:	04DC4BEEF6C21A9C6160CAFA39221BE5B5F389A672C576E4B3B414BE7255965A3DE1ECE11B570C450034ED542FC252ADBEF1F0B5B424727AA44E40610BBC1245
Malicious:	false
Preview:	8XJ5O78p43jD6w54Y3C8narYA32uNDR2OO8l9LC3M46Ew49993219698jZ4104X69Pz1i0gX6599es92QqRrbk..0a44Z1q875111n748440l7m7WKgf4VL06qV7x87kP4Se301V5rsKH0Y4JyAWOKQuD9y0Tl2bCp5h07A19hWz6908xLH05329FL2N8Dw6lovo2L6e5Uh6s93sGEY37htz4Bi8l0d3L13u6301ZOk9IF84XRNpes6zG..3eLFE8nsT1tsi43t0m2a3q4l9A4285U8054pu8a46GNp6539VM7w3s55dHd34e9jK4942z773bC88..O1392wc6z05608x19lA5Zr41gm6J0X83xsNWb7n6o84yB18brJO59L3..A1VSG9HPf297X62p8GR7uzLV9y339z72D1db5802UV9u9928fws9uQX00qco72o126ir3ZC9z277J10HQ074hXuwY271..7b902ma70p6ST8uR7952QD33456TNrf17pQRwuVJI09jHJ00YV783h074Xjxm8mNI4..

C:\Users\user\1_102\uvbdlqfvw.pif

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	927984
Entropy (8bit):	6.972227782935505
Encrypted:	false
SSDEEP:	
MD5:	F28AA08788132E64DB4B8918EE2430B1
SHA1:	EF32B1023A89DC36D7C5E98E22845FE87C5EFEF2
SHA-256:	F99B9FC041C177F0BEE2C82D09F451EF0833696111B1B37CBFFF8C975232ECE2
SHA-512:	689CF6118061AA9E7D4B78118DB99338AA767433DF511610D471A989825A84A53119310248ED3870B10E48E77B47C429EF5A276DBC9C4EC53A7588E16093B50F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 84% • Antivirus: Metadefender, Detection: 39%, 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..... ....@.....c.....@...@.....@.....T.....A.....4.....c..... ..D... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc....A.....B...R.....@..@.reloc...u.....v.....@..B.....

C:\Users\user\1_102\uwxfpkwog.ini

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	573

Entropy (8bit):	5.466909554517946
Encrypted:	false
SSDEEP:	
MD5:	9D81DD0B5D9FE79559721E884F78492B
SHA1:	D063DACC1CF447688DB2C41A39A6FABC49DE153D
SHA-256:	3CA9B80D0B2EDBD1D3607FBFE7248DE87D709A501ED65BDFDE9135344C6A8241
SHA-512:	84494455F5A3FF0EDE6CC363B1D58DB26506DF30E4B97BA1009F5D9E1F85107C0CC3DD2C3EADBD927A35D70735DD47AA41A29433A89F080A9326261FCEA2B3 1
Malicious:	false
Preview:	7oP478p4LEq2A20Yt6395Ku56U876HFv795w7Ye73428iA6Ox4589Us0EgQ..nCC3a9j0G2j6NO8rmO8y8591Z5y60Ah0kPNVz97WUki50K05o889IGy4QHbY016G8f0L8 1IGLfZs4M086Z853586s468580du7Rr2Uk726p70Yzg177TO405ZX8D15zDPM28jSnA92..0QxQ4H9cRa171VT0xi1k318xGVo01NEa1iBo31f170ds24ItTWc4d75B37S 6KTL5RVdQ3JtO39h7f7VUw06390218pT48vG91oX8101139L3338sY63RlGBW0KzgkPu3Ys82Z9Adi5f5k2vR01s9cg9t7999744..22305075i2WPO596et3j3ZK4Ts41 6FO9122OHWT..ljo04994p91T57A020ep499Nb4fd16j2U..1sliIL9X2va315D0F..98k7dG0g556E420..g7n4h..LO17DE968A50MEQ54ZeG70tU2482w9OfL5uE686 g0u64ckFw21v840Oo1P8j7909Kz7V4LYzU88F7M9HAGO5jd1g56..

C:\Users\user\1_102\vhojmceu.bin

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	5.493985188967033
Encrypted:	false
SSDEEP:	
MD5:	821E805D08EDD873377FC0CA32729010
SHA1:	1E2EC4347F8DC312A3CD311C884289822BE1EA24
SHA-256:	418C1CDC6E4C4390C40553C1BE9F3538E66FFD0A4A07E9C68189EDC236435A8F
SHA-512:	DCAB63301840FCCF3E976BF04FD2088B758C73D0CC48C416266E97C551F23C5B6055B6AB2D7D1049F3F66745995AC0D093614E4F848815886E4741BD122458DA
Malicious:	false
Preview:	190AE9Th7r63TcE04ehH6940t057O8e50Xj82STOyg2y39H5xB7CnmO3362ZcZvbj45110v9N48V888pL5V9Q7j23pSWe625ga2fW7dN0X1Osl32L37307x2r8r539x3n6 azkMI1b84W56IF4u7963M137q..D4J2QK4I14Z86TWD0b9E8Pz4G1Czx1I7v5sl19P..Kl82J1b95l1vue46Hi5RVBW6..0Bz34U2rhyhG..8q4p81299h603l3OJKU77x ioe1L806hUDuCuG43w0927riqz1852123S5ccjE7unM3Nix6l7687Z9E9k70R0N75z04Lq9CyR6L84lfQ12iF302AC19vx4nWMevz170BxC0ZG2qs7sdF45Y596j155ldO 72w..7l58N0Es0659l95V2s5002493x180e28t8y776w8x900f37865718Y029n89ag90a3i408L084..K7794dxrpO3O4366g4HtWh5Ryj88Rr29Sa6j24JlnP2BWz31z 48sD9Y19duk3RC8n27Lryr31IOQA3T34FF495AL5927CPdS6F0u1T4r67Hy74Sd3j6S51V6oB9sN8L188f308AGD40i8Gp5f..

C:\Users\user\1_102\vmsrlgffxa.msc

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.430646057607747
Encrypted:	false
SSDEEP:	
MD5:	122051DD2E0709DC66CF96C06A5842FA
SHA1:	A442F847EA150CAF49539C76C786DE0B9CB35C43
SHA-256:	47D0C9B11F85B53747D72294B05FAF190C3AE828A44AE5AE389395957DC23755
SHA-512:	4EC2607B9486D8006033FA3CA605DB342DA6B9A1555AB454CCCA884C79D21D56DF64D57485038F67C0F740A3872D6F233EFF8EB58BD7DCE9E90F25345E273DA 7
Malicious:	false
Preview:	9ffWkZjddr2y4j636CPfmrM9Bk41Q59Mk2K4..L4Z8K1t5tm7BDyz7Z207a635b35031cqxT783iCLfkF0391X6121516B2V2s5IT46MuA39..f9C7R2e6V149286266W2 9g91ooe72rA48xH2gg5JeJP48Ps8480k8Sz04kVm1357y2KI5g38Jsg9Wo5D4ykhQI5rcIa0h7920by64t952tK7cJmH51i19yd6e8Y2s9MyT489eT47u3747pLs8STK4O 7918a7W92K82Yn3OiU57Pn7D4w0y1Z6E..27J579o51Crj2B0Q2U2xY1B38s40L8N8qzDt29K7M474215wmr3mv83Nd30E801H..6Z5iw87Gb8k3214209T37Q4zrf7G0p b53N124nwP..5Q9a6230dZ29z5fp5q0804277nz67VU81D90H623jf231Dyr6JKmK2005KjnT2hd5J95id5VKYi0v2s0M7m111f64qhV72931I431BX..

C:\Users\user\1_102\wnjllkkup.msc

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	527
Entropy (8bit):	5.550077693568007
Encrypted:	false
SSDEEP:	
MD5:	84FBE889CAEF2425B70B508FC31B2D89
SHA1:	8542F061AF96F7AC536A8BE0D957945156331510

SHA-256:	14E3669B2D1F19D34FA4FA768FD2C46EA6143FDE7E7088837CFCCEC634876C94
SHA-512:	985485E821E2B65BDA07606CE45CE795B1B83188360A87B48BAEBEF3A1E4888B6C690E1BE76606475CA23D1FC011284E10747A54E9EC9383B7F41BC36EC1D6B6
Malicious:	false
Preview:	0thA2176D8R0DOy2FbR5931v1u9Uq..v0c96V1aA0O516RgL..gHfH3SDy1s5Gu7567H3Upc71rC991g36fx1RW25909K..Y1wP047vTg4358Y35P5787Rdp2Koe47q07z yW70809O6o6iZnRlOVLL4621Ks48229N2g3933u43..h6DJ296K163897s77GT12M43770138s65GjW8Y350JQB5858KdctJE3D46j91e33WSWB205Ygy3O8A802J3238N 10126ly604q4U2r7ce2X2d511VU6N3e5Ln4lL7VX9eo50UA55jP61Lpu1El3rDQlnB0..Ew92fzwwv1J13KpGq6MBH8AUL80OIF6k1cV907C99u217z0R2167073o75tq2 8mS7MYnnO9La0A3l9EBuds2p6j162..l7klok70HJeSH3eYvM772rv4IbV88484pKZcc8G9K3bH3394r3TOuLjNi4AUScJK..Vi9xj8h249F2ij24zMCjj45MTuyaOC27WH7sVg..

C:\Users\user\1_102\wrtwnmt.xml

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.541188358855593
Encrypted:	false
SSDEEP:	
MD5:	45F310DB4E5882B96E167BC0A0CFB404
SHA1:	2F52ED1C21B6DD37B8305F2E233695052CE66F75
SHA-256:	26B6BE317995E8D8F8EDB7A5850D82E84A1BC0A86933F5D036045785E911A416
SHA-512:	AE94E612F044178DED03908B786E535EC24B96945A1585C0F9B25E3BA4847A9C6C5DFCDAB46ADF7C12F61EA2BD7690A87D181ABD88693EA50099F688BA2058 7
Malicious:	false
Preview:	NHeAM74Sc90zlf16B11595U429T943gV884BqtzV4fmI9yK2tg91IWPmS84a6w6Jc5CRRMVS8O6U50lit11slk817b..7y1zhW1725abc8o93R0m7rVYRnE75L553o44St Y9W204H1349dG9258..S8Yo739X4A7752Omn5S0H4Y7524y4W9O806Hz5eBK6508imiD2JiYm4X579DGaTK841y49yRB1An13m9OS52..DD614l0RQ5b0vX 49d5bru2gh875EO53X007z32x86IL6b975JuakZrCsx49Kom40g0U9Q9H2456j0pcxzxq14XDp3aaM1759020l1RudT6eNt9R2004G9Vl1Csv4sj68KVs67DT5F5cCTgTV ctYFv603PML487miAV8N782U9r10jMKjm9hYLH541546zm8..76M60z6aAGMlM99Vb67Pufa835Z..0848bZ9q2hN894701yiec72e9gH50371620990TkBk9zN5761B5U l93dn0BhYnm5QB574Epy2jY9N586w2U2522WijnS45n5Nv19om72Gp4Mg4Z5057Pf5c3Z2zX9L37ytx668F105w4w9z5UY7Xca3b..

C:\Users\user\1_102\xfsxuexxqf.ini

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	545
Entropy (8bit):	5.451214138570856
Encrypted:	false
SSDEEP:	
MD5:	7D14C20D5F7769CB1134A5B93ED86C4D
SHA1:	36B085BC62578C2C131A51909660904D581EAA7E
SHA-256:	21401D62AF960094F327F17339FC728FABF55D2D6CEE7DB83EF347841B3803F3
SHA-512:	435E1FA348D789B4D28E8145290E79A5AC202F910CA44F3D7631CCD239DD255BD4C339CD13FB27353EB322BB8078F60533D69DCA339114FDF8618CCB6F1557A
Malicious:	false
Preview:	064Pq9M40984K4eV7K1g5lxI8J6210Eub9k8AtF87159781E83e2bc77998C48pa2e8Ur75dzFS1n88z80g7Lr3P369N33U6uh1798X142pYt63m531ey4701A9862av12 705P9pjb17L12C825JY2jU001WM4yb26PnWV1U5u59Q8K16Br7T8..4tn01..k4cZuD..8xzV8WXnl0YpGow2uA9J87632jZ6nXoXh676H67jAFAvSr25432O0yBdiBiM9 FH3TD5j79Lx174mxEP0ws05152b974..kqY9HJw72gdk0sM1W108OGAdv113d1c85068SY6SM7tV6n02pUOL946m3flYCj8d10..G7300qb1Z0X84a2xn168o6w3q79p0H 7U570jm42k6XO415Z5M7811qJC7s8220E5973n28chlz145E3lO2K24up0..559956B667E..bD4K541o54vXt20V3YTo43v60306P6KNF22580c523NjIlnX1462KEqQ5 U3X4IG7k6cy1K8815wqbK7I..

C:\Users\user\1_102\xgenwdravq.dat

Process:	C:\Users\user\Desktop\INV_0893.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	569
Entropy (8bit):	5.50884636043805
Encrypted:	false
SSDEEP:	
MD5:	D235504FAD5543813D8F6085000405C8
SHA1:	065CCD6D02D3C84D3B1ED80181EE7A4D520D890E
SHA-256:	3E0CAA187BD0AAB3E0C655816A962FC2DD62D8B3FD8B89C16C445EC7AB1E0B24
SHA-512:	FB7C4E94F6B6B5158DC2B569DC195917F944DFC51B04D1E823848502CC49CE846264E62168E1B6019984EA51BF4B97C331C1CB5FA7AC7857FAB9B69440A32EE 5
Malicious:	false

Preview:	hI1LZ34..72SivYae84vl2LWn95ejm9r151A7uH..35tlzxB68AYQ9K1BNM797X2E4552163..aAHwGT86Bfui6f5122ri1D316x73poiw7FM2cu30H8992218l9aG3hdp 1hO1Fp10BhG2257l569sL3s1NaMpAG2N4EsB2v25277tD7CU6P2Nz143bZ0ZsVQcT61Pm06gV40op86t326FL8G36229PxLC4318wo3kR548Y21qw6249732 2i08T3J2YD..sR9563F9122wDhL86b4AG2t7JlGoJvA1377f..1i144Jp68R4N8a8q8IerZ66UHHy4C0XVU83ay1wK4wHTc9li46K8qp431v..Dpx32u77TL1011J0V05S F7d0954917421j41t334LiG6pcG701yHgm8..6Ag25l06T4TL87ZN4HRx019289x8597KNVOFN135..ok8KslZ9GqB456b2SL7wo4l688YZE3MoJ0xP3EM59da8tle59uq 243770O28898rjnoZ4nX4KV9DZ47b61405FD19X11gn6TLuT48u3Eb5a2..

C:\Users\user\AppData\Local\Temp\RegSvcs.exe

Process:	C:\Users\user\1_102\uvbdlqfvw.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
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(.... s.....o.....r\|..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,(....~....o....9]...

C:\Users\user\temp\qdmmn.ppt

Process:	C:\Users\user\1_102\uvbdlqfvw.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	5.107771566226461
Encrypted:	false
SSDEEP:	
MD5:	92B11A1569E08C09D65D6E1F5B520085
SHA1:	280E847DA1277BE574B80FC019DFEBFABFD44A26
SHA-256:	710CEA5D25746C27EA4213656B0EB48E624BB9DE488164CF966CC9A7F02DA2E4
SHA-512:	61D605F70A11CBD76B54A51796D734A26BEF182CDAB2414D93534A561A72AE0CFC3B6837195106D1A89460E47B2A0DE962081BAC4AA8855C366D52DC42BB6AF
Malicious:	false
Preview:	[S3tt!ng]..stpth=%userprofile%..Key=WindowsUpdate..Dir3ctory=1_102..ExE_c=uvbdlqfvw.pif..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.67310941416459
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:	INV_0893.exe
File size:	1248871
MD5:	d23e1e317d68720216699e1c9e524a78
SHA1:	76b58185f5aa824e5bafc589aaa6c228b341b239
SHA256:	8dda840eccb53427037b3a06dd5f886c78e6e55fe69d96b256b05176e85172db
SHA512:	38a7d77645a9b2eb2bb9ec05c0f0c561a23aecadc7b5206f30bb98aa6bd97722af6a7174e371576deb389f53d58836b501e5ef1acf35da285ff5469784b5b021
SSDEEP:	24576:5AOcZgAgB9ZE+UDuAWGyrb1pUVgfMgLAWDXxo8FVCaWXZWcbISNY:zTAgBLUDqZ1+O3VokCp7U+Y
TLSH:	78451242BB9D88B1F06319355A35AA315A7D3C204EE0A7DFB3D03B6DDB305D15227BA2

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:	324383b393434b96

Static PE Info

General

Entrypoint:	0x41e1f9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
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

Instruction
call 00007FD3284996DFh
jmp 00007FD3284990D3h
cmp ecx, dword ptr [0043D668h]
jne 00007FD328499245h
ret
jmp 00007FD328499855h
ret
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00433068h
mov dword ptr [ecx], 00434284h
ret
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007FD32848C651h
mov dword ptr [esi], 00434290h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00434298h

Instruction
mov dword ptr [ecx], 00434290h
ret
lea eax, dword ptr [ecx+04h]
mov dword ptr [ecx], 00434278h
push eax
call 00007FD32849C3EDh
pop ecx
ret
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 00434278h
push eax
call 00007FD32849C3D6h
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007FD32849924Ch
push 0000000Ch
push esi
call 00007FD32849880Fh
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FD3284991AEh
push 0043A410h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FD32849BAD5h
int3
push ebp
mov ebp, esp
sub esp, 0Ch

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [C++] VS2015 UPD3.1 build 24215 • [EXP] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213 • [LNK] VS2015 UPD3.1 build 24215

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3b540	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3b574	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x15168	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x78000	0x210c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x397d0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x34218	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x32000	0x260	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3aaec	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30581	0x30600	False	0.5892684108527132	data	6.70021125824862	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x32000	0xa332	0xa400	False	0.45503048780487804	data	5.23888424127282	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3d000	0x238b0	0x1200	False	0.3682725694444444	data	3.8399352693886706	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.gfids	0x61000	0xe8	0x200	False	0.333984375	data	2.121663815328785	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x15168	0x15200	False	0.17386279585798817	data	2.7738427471969187	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	0x210c	0x2200	False	0.7865349264705882	data	6.610385193776529	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x62524	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6306c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x64618	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584		
RT_DIALOG	0x74e40	0x286	data	English	United States
RT_DIALOG	0x750c8	0x13a	data	English	United States
RT_DIALOG	0x75204	0xec	data	English	United States
RT_DIALOG	0x752f0	0x12e	data	English	United States
RT_DIALOG	0x75420	0x338	data	English	United States
RT_DIALOG	0x75758	0x252	data	English	United States
RT_STRING	0x759ac	0x1e2	data	English	United States
RT_STRING	0x75b90	0x1cc	data	English	United States
RT_STRING	0x75d5c	0x1b8	data	English	United States
RT_STRING	0x75f14	0x146	data	English	United States
RT_STRING	0x7605c	0x446	data	English	United States
RT_STRING	0x764a4	0x166	data	English	United States
RT_STRING	0x7660c	0x152	data	English	United States
RT_STRING	0x76760	0x10a	data	English	United States
RT_STRING	0x7686c	0xbc	data	English	United States
RT_STRING	0x76928	0xd6	data	English	United States
RT_GROUP_ICON	0x76a00	0x14	data		
RT_MANIFEST	0x76a14	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetOEMCP, GetCommandLineA, GetEnvironmentStringsW, FreeEnvironmentStringsW, DecodePointer
gdiplus.dll	GdiplusShutdown, GdiplusStartup, GdipCreateHBITMAPFromBitmap, GdipCreateBitmapFromStreamICM, GdipCreateBitmapFromStream, GdipDisposeImage, GdipCloneImage, GdipFree, GdipAlloc

Possible Origin

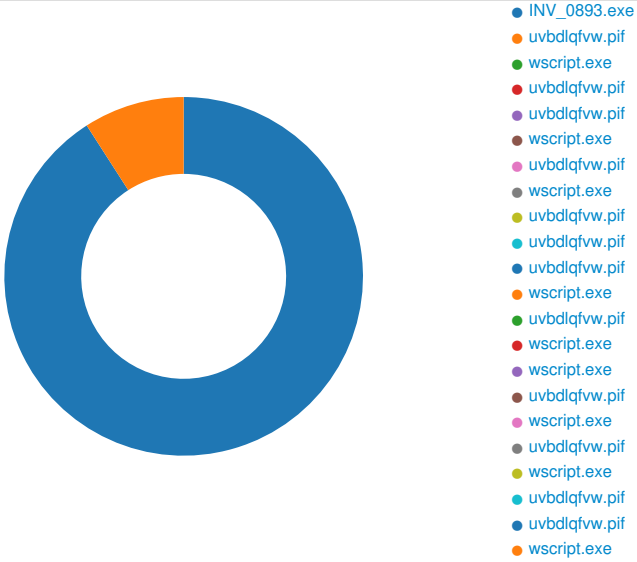
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: INV_0893.exe PID: 1348, Parent PID: 3324

General

Target ID:	0
Start time:	15:52:44
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\INV_0893.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INV_0893.exe
Imagebase:	0x1120000
File size:	1248871 bytes
MD5 hash:	D23E1E317D68720216699E1C9E524A78
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: uvbdlqfvw.pif PID: 2528, Parent PID: 1348

General

Target ID:	3
Start time:	15:53:13
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\uvbdlqfvw.pif" faeupdrjbw.afr
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 84%, ReversingLabs • Detection: 39%, Metadefender, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	112362A	CreateDirectoryW
C:\Users\user\1_102\run.vbs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	111629C	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\1_102\run.vbs	0	115	53 65 74 20 57 73 68 53 68 65 6c 6c 20 3d 20 57 53 63 72 69 70 74 2e 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a 57 73 68 53 68 65 6c 6c 2e 52 75 6e 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6e 73 5c 31 5f 31 30 32 5c 55 56 42 44 4c 51 7e 31 2e 50 49 46 20 46 41 45 55 50 44 7e 31 2e 41 46 52 22	Set WshShell = Wscr ipt.CreateObject("Wscr< wbr>i pt.Shell")WshShell.Run"C :\User s\user\1_102\UVBDLQ~1 .PIF FAEUPD~1.AFR"	success or wait	1	1133D5E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\1_102\faeupdrjbw.afr	unknown	65536	success or wait	2735	110DB2F	ReadFile
C:\Users\user\1_102\faeupdrjbw.afr	unknown	24576	end of file	2	110DB2F	ReadFile
C:\Users\user\1_102\faeupdrjbw.afr	unknown	65536	success or wait	1	10F3B98	ReadFile
C:\Users\user\1_102\faeupdrjbw.afr	unknown	65536	success or wait	2655	10F3B98	ReadFile
C:\Users\user\1_102\faeupdrjbw.afr	unknown	65536	end of file	1	10F3B98	ReadFile
C:\Users\user\1_102\junnhus.tbg	unknown	65536	success or wait	1	10F3B98	ReadFile
C:\Users\user\1_102\junnhus.tbg	unknown	65536	success or wait	6	10F3B98	ReadFile
C:\Users\user\1_102\run.vbs	unknown	65536	end of file	1	10F3B98	ReadFile

Registry Activities

Analysis Process: wscript.exe PID: 5360, Parent PID: 2528

General

Target ID:	4
Start time:	15:53:28
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: uvbdlqfvw.pif PID: 1244, Parent PID: 5360

General

Target ID:	5
Start time:	15:53:29
Start date:	03/10/2022

Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: uvbdlqfvw.pif PID: **5268**, Parent PID: **3324**

General

Target ID:	6
Start time:	15:53:33
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" C:\Users\user\1_102\FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **1076**, Parent PID: **1244**

General

Target ID:	9
Start time:	15:53:43
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: uvbdlqfvw.pif PID: **4648**, Parent PID: **1076**

General

Target ID:	10
Start time:	15:53:46
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **4392**, Parent PID: **5268**

General

Target ID:	11
Start time:	15:53:47
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: uvbdlqfvw.pif PID: **5328**, Parent PID: **4392**

General	
Target ID:	12
Start time:	15:53:52
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: uvbdlqfvw.pif PID: **2180**, Parent PID: **3324**

General	
Target ID:	13
Start time:	15:53:52
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" C:\Users\user\1_102\FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: uvbdlqfvw.pif PID: **5780**, Parent PID: **3324**

General	
Target ID:	14
Start time:	15:54:05
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" C:\Users\user\1_102\FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **5848**, Parent PID: **4648**

General	
Target ID:	15
Start time:	15:54:07
Start date:	03/10/2022

Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: uvbdlqfvw.pif PID: **5884**, Parent PID: **5848**

General

Target ID:	16
Start time:	15:54:11
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **6072**, Parent PID: **2180**

General

Target ID:	17
Start time:	15:54:13
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **6060**, Parent PID: **5328**

General

Target ID:	18
Start time:	15:54:15
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: uvbdlqfvw.pif PID: **1332**, Parent PID: **6072**

General	
Target ID:	19
Start time:	15:54:22
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **4324**, Parent PID: **5780**

General	
Target ID:	20
Start time:	15:54:23
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: uvbdlqfvw.pif PID: **2148**, Parent PID: **6060**

General	
Target ID:	21
Start time:	15:54:23
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **2472**, Parent PID: **5884**

General	
Target ID:	22

Start time:	15:54:32
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: uvbdlqfvw.pif PID: **3648**, Parent PID: **4324**

General

Target ID:	23
Start time:	15:54:32
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: uvbdlqfvw.pif PID: **5336**, Parent PID: **2472**

General

Target ID:	25
Start time:	15:54:41
Start date:	03/10/2022
Path:	C:\Users\user\1_102\uvbdlqfvw.pif
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\1_102\UVBDLQ~1.PIF" FAEUPD~1.AFR
Imagebase:	0x10f0000
File size:	927984 bytes
MD5 hash:	F28AA08788132E64DB4B8918EE2430B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **4596**, Parent PID: **1332**

General

Target ID:	26
Start time:	15:54:47
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\1_102\run.vbs"
Imagebase:	0xf80000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly